Financial Action Task Force
Groupe d'action financière

THIRD MUTUAL EVALUATION ON ANTI-MONEY LAUNDERING AND COMBATING THE FINANCING OF TERRORISM

CANADA

29 FEBRUARY 2008

TABLE OF CONTENTS

1. GENERAL 16

1.1 General Information on Canada 16
1.2 General Situation of Money Laundering and Financing of Terrorism 20
1.3 Overview of the Financial Sector and DNFBP 24
1.4 Overview of commercial laws and mechanisms governing legal persons and arrangements 32
1.5 Overview of strategy to prevent money laundering and terrorist financing 33

2 LEGAL SYSTEM AND RELATED INSTITUTIONAL MEASURES 39

2.1 Criminalisation of Money Laundering (R.1 & R.2) 39
2.2 Criminalisation of Terrorist Financing (SR.II) 49
2.3 Confiscation, freezing and seizing of proceeds (R.3) 54
2.4 Freezing of funds used for terrorist financing (SR.III) 65
2.5 The Financial Intelligence Unit and its functions (R.26 & 30) 73
2.6 Law enforcement, prosecution/ other competent authorities 90
2.7 Cross Border Declaration or Disclosure (SR.IX) 105

3. PREVENTIVE MEASURES - FINANCIAL INSTITUTIONS 114

3.1 Risk of money laundering or terrorist financing (R.5 – 8) 120
3.2 Customer due diligence, including enhanced or reduced measures (R.5-8) 123
3.3 Third parties and introduced business (R.9) 144
3.4 Financial institution secrecy or confidentiality (R.4) 146
3.5 Record keeping and wire transfer rules (R.10 & SR.VII) 149
3.6 Monitoring of transactions and relationships (R.11 & 21) 154
3.7 Suspicious transaction and other reporting (R.13-14, 19, 25, 32 & SR.IV) 159
3.8 Internal controls, compliance, audit and foreign branches (R.15 & 22) 166
3.9 Shell banks (R.18) 175
3.10 Supervision and oversight (R. 23, 30, 29, 17, 32, & 25) 176
3.11 Money or value transfer services (SR. VI) 211

4. PREVENTIVE MEASURES – DESIGNATED NON-FINANCIAL BUSINESSES AND PROFESSIONS 214

4.1 Customer due diligence and record-keeping (R.12) (applying R.5, 6 & 8-11) 214
4.2 Monitoring transactions and other issues (R.16) (applying R.13-15, 17 & 21) 225
4.3 Regulation, supervision and monitoring (R. 24-25) 229
4.4 Other non-financial businesses and professions – Modern secure transaction techniques (R.20) 244

5. LEGAL PERSONS AND ARRANGEMENTS & NON-PROFIT ORGANISATIONS 247

5.1 Legal Persons – Access to beneficial ownership and control information (R.33) 247
5.2 Legal Arrangements – Access to beneficial ownership and control information (R.34) 251
5.3 Non-profit organisations (SR.VIII) 254

6. NATIONAL AND INTERNATIONAL CO-OPERATION 259

6.1 National co-operation and coordination (R.31 & 32) 259
6.2 The Conventions and UN Special Resolutions (R.35 & SR.I) 264
6.3 Mutual Legal Assistance (R.36-38, SR.V, R.30 & 32) 265
6.4 Extradition (R.39, 37 & SR.V) 275
6.5 Other Forms of International Co-operation (R.40, SR.V & R.32) 279

7. RESOURCES AND STATISTICS 288
7.1 Resources and Statistics (R. 30 & 32) 288
7.2 Other relevant AML/CFT measures or issues 289
7.3 General framework for AML/CFT system 289

Tables

Table 1. Ratings of Compliance with FATF Recommendations 290
Table 2: Recommended Action Plan to Improve the AML/CFT System 301
Table 3: Authorities' Response to the Evaluation 308

PREFACE - INFORMATION AND METHODOLOGY USED FOR THE EVALUATION[1]

1. The evaluation of the anti-money laundering (AML) and combating the financing of terrorism (CFT) regime of Canada was based on the Forty Recommendations 2003 and the Eight Special Recommendations on Terrorist Financing 2001 of the Financial Action Task Force (FATF), and was prepared using the AML/CFT Methodology 2004[2]. The evaluation was based on the laws, regulations and other materials supplied by Canada, and information obtained by the evaluation team during its on-site visit to Canada from 19 to 30 March 2007, and subsequently. During the on-site visit, the evaluation team met with officials and representatives of all relevant Canadian government agencies and the private sector. A list of the bodies met is set out in Annex II to the mutual evaluation report.

2. The evaluation was conducted by an assessment team which consisted of members of the FATF Secretariat, APG Secretariat and FATF and APG experts in criminal law, law enforcement and regulatory issues: Mr. John Carlson and Ms. Catherine Marty from the FATF Secretariat, Dr. Gordon Hook from the APG Secretariat, Ms. Anne Juniel, financial expert, Bank of France (France), Mr. Jack de Kluiver, legal expert, Department of Justice (United States), Mr. Marc Penna, law enforcement expert, Cellule de Traitement des Informations Financières (Belgium), Mr. Bill Peoples, law enforcement expert, New Zealand Police (New Zealand) and Mr. Jeremy Platts, financial expert, Hong Kong Monetary Authority (Hong Kong). Mr. Robin Sykes, Central Bank of Jamaica participated as an observer. The assessment team reviewed the institutional framework, the relevant AML/CFT laws, regulations, guidelines and other requirements, and the regulatory and other systems in place to deter money laundering (ML) and the financing of terrorism (FT) through financial institutions and Designated Non-Financial Businesses and Professions (DNFBP), as well as examining the capacity, the implementation and the effectiveness of all these systems.[3]

3. This report provides a summary of the AML/CFT measures in place in Canada as at the date of the on-site visit or immediately thereafter. It describes and analyses those measures, and provides recommendations on how certain aspects of the system could be strengthened (see Table 2). It also sets out Canada's levels of compliance with the FATF 40+9 Recommendations (see Table 1).[4]

---

1 Generally, FATF reports are written in United Kingdom English; however, this report is written in Canadian English to avoid any confusion that may be caused by the spelling of Canadian agencies or citations from Canadian laws, regulations and other sources.

2 As updated in February 2007.

3 The list of all bodies met during the on-site mission, the copies of the key laws, regulations and other measures and the list of all laws, regulations and other materials received and reviewed by the assessors are available in the Annexes of this report.

4 Also see Table 1 for an explanation of the compliance ratings (C, LC, PC and NC).

EXECUTIVE SUMMARY

1. Background Information

4. This report provides a summary of the AML/CFT measures in place in Canada as of June 2007. The report describes and analyses those measures and provides recommendations on how certain aspects of the system could be strengthened. It also sets out Canada's levels of compliance with the FATF 40 + 9 Recommendations (see attached table on the Ratings of Compliance with the FATF Recommendations).

5. Canada has strengthened its overall AML/CFT regime since its last FATF mutual evaluation (1997) by implementing a number of changes both in terms of statutory amendments and structural changes. The most important developments were the enactment of the Proceeds of Crime (Money Laundering) and Terrorist Financing Act and the creation of the Canadian Financial Intelligence Unit (FINTRAC) in 2000. With regard to the legal measures (ML and TF offences, confiscation, freezing mechanisms), the legal framework is generally in line with the FATF standards however further steps could be taken to enhance effective implementation. The Canadian FIU has been provided with extensive powers and responsibilities. Since it became operationally effective in November 2001, FINTRAC has undertaken extensive outreach and assistance to reporting entities and has developed close relationships with government partners. There are concerns about its effectiveness in disclosing money laundering and terrorist financing cases to law enforcement authorities.

6. Canada has recently introduced a significant set of new requirements for financial institutions that aim at implementing the FATF standards. A large number of these new requirements will only be in force in June 2008, and these, together with further amendments applicable to DNFBPs due to come into force in December 2008, have not been analysed in the context of this evaluation. As it currently stands however, the preventive system is generally insufficient to meet the FATF Recommendations. In addition, certain financial institutions that undertake financial activities, as defined by the FATF Recommendations, are not currently covered by the AML/CFT regime. Moreover, both the scope of coverage and the AML/CFT requirements for the designated non-financial businesses and professions (DNFBPs) are insufficient to meet the FATF standards. Although FINTRAC and the Office of the Superintendent of Financial Institutions (OSFI) are involved in comprehensive supervisory actions, there are varying degrees of supervision for AML/CFT purposes in the financial sector.

7. Illicit proceeds from a variety of criminal activities contribute to the ongoing money laundering situation in Canada with drug trafficking as the source of much of the money laundered. Other sources of proceeds of crime include, but are not limited to, prostitution rings, contraband smuggling, illegal arms sales, migrant smuggling, and white-collar crime such as securities offences, real estate fraud, credit card fraud and telemarketing fraud. While there is no estimate for the total annual proceeds of crime, drug sales are estimated to amount to several billion dollars.

8. The money laundering methods used in Canada have remained relatively consistent in recent years. They essentially consist of: smuggling; money service businesses and currency exchanges; casinos; purchase of real estate; wire transfers; establishment of offshore corporations; credit cards, stored value cards and new payment methods; use of nominees; use of foreign bank accounts; use of professional services (lawyers, accountants, etc.); and reinvestment and distribution in illicit drugs. At the placement stage, criminals are using money service businesses or casinos. Electronic funds transfers are being used for layering and at the integration stage, criminal proceeds are used to purchase high-value assets in attempts to conceal the origin of the funds. Most recently, there have been signs that criminals are turning to such methods as Internet payments or cross-border movement of gold bullion.

9. Canadian law enforcement authorities have identified a number of terrorist organisations operating in Canada. Investigations have shown that terrorist cells have a tendency to remain self-sufficient by generating funds locally. In some instances, they may do so by committing petty crimes, such as welfare fraud or credit card fraud. In other instances, cell members have started businesses to glean financial information from unsuspecting customers in order to clone credit cards and commit identity thefts. Law enforcement authorities have intelligence indicating that suspected terrorist entities in Canada are raising funds through drug trafficking.

10. The financial sector in Canada is diverse, mature, well developed and includes many service providers. The sector is significantly integrated, as many players offer similar services and a small group of "financial groups" or conglomerates offer a large variety of financial products directly or through subsidiaries. A wide range of financial institutions exist in Canada and are subject to AML/CFT requirements: banks; credit unions and *caisses populaires*; life insurance companies; trust companies (that offer services similar to those provided by banks but can also administer estates, personal and institutional trusts, trustee pension plans and agency contracts); securities firms and money service businesses (MSBs). Financial leasing, factoring, finance companies (*i.e.* entities specialised in consumer lending, credit cards, equipment financing and small business loans that are not loan companies), providers of e-money, Internet payment providers and cheque cashers are also engaged in financial activities as defined by the FATF.

11. The following DNFBPs are currently subject to AML/CFT requirements: casinos, real estate agents and accountants. In addition, the Government of Canada has recently enacted regulations to cover the following DNFBPs as of December 2008: lawyers, notaries (relevant in Québec and British Columbia only) and dealers in precious metals and stones. Trust and company service providers are not separately recognised nor regulated as a discrete category of entity in Canada and do not fall under the AML/CFT regime. Trust companies, accountants, lawyers and other independent legal professions provide most services of this nature, though it appears that some other businesses exist that engage in TCSP activity.

2. Legal System and Related Institutional Measures

12. The anti-money laundering offences are comprehensive and Canada generally meets the requirements under Recommendations 1 and 2. The money laundering offence (section 462.31 Criminal Code (CC)) is part of a broader proceeds of crime regime designed to cover all obligations in the 1988 Vienna Convention and the 2000 Palermo Convention. Section 462.31 encompasses acts of using, transferring the possession of, sending or delivering to any person or place, transporting, transmitting, altering, disposing of or otherwise dealings with, in any manner and by any means, any property or any proceeds of any property. The Section 462.31 offence is however technically inconsistent with the relevant UN Conventions in that it has a specific intent mental element that is not consistent with those Conventions. Designated offence refers to virtually all indictable offences and also covers all ancillary offences.

13. There is also a second offence of possession of proceeds of crime (s.354(1), CC), whereby it is an offence to knowingly possess money or property derived directly or indirectly from any indictable Canadian criminal offence or any foreign offence, that had it been committed in Canada would have been an indictable offence in Canada. The two offences cover almost all of the requirements of R.1 & 2, with only some minor technical deficiencies (see comments above). Despite this, the emphasis on and preference for pursuing the predicate crimes and the offence of possession of property obtained by crime, and the low number of s.462.31 convictions indicates that the statutes available for countering ML are not being used as effectively as they could be. Canada should develop a more proactive approach to prosecuting the specific money laundering charge under s.462.31.

14. Canada has three criminal offences related to the financing of terrorism (s. 83.02-83.04, CC). The offences are broadly defined and wide-reaching in effect. These offences cover the provision or collection of property intending or knowing that it will be used, in whole or in part, to carry out or

facilitate a "terrorist activity", to possess or use property for that purpose, or to benefit a terrorist group. The offences and related provisions cover all types of property; include ancillary offences; and generally meet all the requirements of the FATF standards. The offences have been in existence for several years and there have been a large number of investigations, but only three persons have been charged with terrorist financing and these charges have not been heard yet. There have been no convictions. Given these facts, the authorities should consider how the TF offence could be more effectively implemented. The overall effectiveness of the TF offence and regime is an issue that the authorities will need to pay close attention to going forward.

15. The CC and the Controlled Drugs and Substances Act (CDSA) contain extensive provisions that authorise the forfeiture of proceeds of crime and instrumentalities used in or intended for use in offences. Forfeiture is available for all money laundering and terrorist financing offences, as well as all predicate offences. Conviction for any indictable offence or a conspiracy or attempt to commit an indictable offence is a prerequisite to forfeiture. There are also discretionary provisions for a fine in lieu of forfeiture, which is the action that Canada has taken to seek to deprive criminals of property of equivalent value. If there are no assets to which such a fine can be applied the court must impose a jail sentence, otherwise the fine is enforced as a civil judgement against any other property of the offender, but cannot be applied against third party property in such cases.

16. Other legislative provisions are broad and allow the authorities to restrain or seize and search for proceeds of crime or instrumentalities. The definition of "property" is broad, and includes any benefit or advantage obtained or "derived directly or indirectly" as a result of the offence. The available data on seizure/restraint and forfeiture is not comprehensive and suggests that it could be more effective.

17. Canada's United Nations Act and its related regulations enable the Canadian government to implement the decisions contained in the resolutions of the United Nations Security Council. The United Nations Al-Qaida and Taliban Regulations (UNAQTR), and the Regulations Implementing the United Nations Resolutions on the Suppression of Terrorism (RIUNRST), were enacted under the authority of Canada's United Nations Act. These regulations allow Canada to list a terrorist individual or entity for the purpose of freezing the funds or assets owned or controlled by that individual or entity or its associates. A third listing mechanism exists under the Criminal Code for threats to Canada's domestic security. Canada has laws and regulations to freeze terrorist funds or other assets of persons designated in the context of S/RES/1267(1999) and S/RES/1373(2001) that are in line with the legal international requirements. However, although the lists are published in the Canada Gazette, there needs to be more communication on listed persons provided to certain categories of financial institutions and other potential asset holders as well as more clear and practical guidance to reporting entities (including DNFBPs and MSBs) that may be holding targeted funds or other assets concerning their obligations in taking action under freezing mechanisms. Canada should also enhance the existing measures to monitor the compliance with the legislation governing the obligations under SRIII (except for federally regulated financial institutions supervised by OSFI).

18. In 2000, Canada established the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC) as a national centre for receiving, analyzing and disseminating information concerning suspected money laundering or terrorist financing. In addition to mandatory reporting by financial institutions and DNFBPs, FINTRAC can receive voluntary information concerning suspicions of money laundering or terrorist financing from the general public and various other sources, including information about cases being investigated by law enforcement agencies and foreign FIUs. FINTRAC has a high level of operational independence and information held by FINTRAC is securely protected.

19. Under the PCMLTFA, FINTRAC is authorized to disseminate financial information to domestic authorities for further action when it has reasonable grounds to suspect that the information would be relevant and useful to the investigation or prosecution of a money laundering or terrorist activity offence. FINTRAC provides comprehensive guidance to reporting entities regarding the manner of reporting and the procedures that should be followed when reporting. In February 2006, FINTRAC

launched an updated secure online report capture system that provides reporting entities with a reliable mechanism to file reports through the Internet. However, the format of reporting forms is perceived by certain reporting entities as being too rigid and reduces the capacity to communicate a maximum level of information. FINTRAC develops very few typologies and is not allowed by the PCMLTFA to ask (directly or indirectly) for additional financial information from reporting entities in line with the FATF requirements.

20. The information that FINTRAC can provide to a disclosure recipient is referred to as "designated information" and includes key details that identify individuals or entities and their financial transactions. Under the PCMLTFA, FINTRAC has the authority to collect information from databases maintained for law enforcement or national security purposes and in respect of which an agreement is entered into. FINTRAC currently has access to two major national police databases. However, FINTRAC has limited access to intelligence information from certain administrative authorities (such as the Canada Revenue Agency (CRA)).

21. There are serious issues in relation to effectiveness with respect to FINTRAC. Although Canada decided to establish a FIU that would make maximum use of advanced technologies in its analytical work, the number of staff dedicated to the analysis of potential ML/FT cases is low, especially in light of the number of reports FINTRAC receives, and FINTRAC has decided to concentrate its efforts on large or significant ML/TF cases. At the time of the on-site visit, the feedback provided by some organizations that receive FINTRAC disclosures was generally negative (unsatisfactory timelines for disclosures, relatively limited added value of FINTRAC disclosures in law enforcement investigations, FINTRAC disclosures positively contributed to existing investigations but rarely generated new ones). It seems that since March 2007, more positive feedback has been received from law enforcement authorities, especially with regard to the timeliness of disclosures. Another important issue is that, FINTRAC disclosures are largely based on voluntary information reports made by law enforcement authorities (80% of cases). This raises serious concerns with respect to the capability of FINTRAC to generate new ML/TF cases independent from existing investigations. Finally, until 2007, no conviction for ML or TF had directly resulted from a FINTRAC disclosure.

22. While all Canadian police forces can investigate money laundering and terrorist financing offences, the Royal Canadian Mounted Police (RCMP), and in particular its Integrated Proceeds of Crime Initiative, IPOC, Units, and, to a lesser extent, the provincial law enforcement authorities in Ontario (the Ontario Provincial Police) and Québec (*Sûreté du Québec*) undertake virtually all money laundering and terrorist financing investigations. The powers and capacity of the law enforcement services are sound and they have appropriate investigative techniques at their disposal. The RCMP acknowledges that, due to resources constraints, it essentially focuses its resources on large, complex ML investigations related to organised crime groups. The RCMP could undertake a larger number of investigations and tackle a larger spectrum of ML/TF cases with additional resources. In addition, consideration should be given to improving the educational and training programmes provided for judges and courts concerning ML and TF offences.

23. Canada has implemented comprehensive measures to detect the physical cross-border transportation of currency and bearer negotiable instruments that are related to ML or FT. These measures are fully in line with the FATF requirements and are effectively implemented.

3. Preventive Measures - Financial Institutions

24. To combat money laundering, the Canadian Parliament enacted the Proceeds of Crime (Money Laundering) Act which received Royal Assent on 29 June 2000. To help fight terrorism, it amended and renamed the legislation the Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA). The PCMLTF Regulations and the PCMLTF Suspicious Transaction Reporting Regulations implement the provisions of the Act. In October 2006, a Bill proposing to further strengthen the PCMLTFA was introduced in Parliament to expand the scope of preventive measures. The Bill received Royal Assent in December 2006. Some new provisions of the PCMLTFA came into

force on 10 February 2007 and on 27 June 2007, the *Regulations Amending Certain Regulations Made Under the PCMLTFA* were enacted and published in the Canada Gazette. Some of these provisions came into force on 30 June 2007; others will take effect on 23 June 2008. A second package of regulatory amendments, the *Proceeds of Crime (Money Laundering) and Terrorist Financing Registration Regulations* setting out a framework for the registration of MSBs will come into force on 30 June 2008. Further regulations were enacted on 26 December 2007 that will come into force in December 2008. However, for the purpose of this report, none of the changes coming into force after June 2007 were considered.

25. FINTRAC (for all reporting parties), OSFI (for Federally Regulated Financial Institutions) and IDA (for securities dealers) have developed guidelines to assist persons and entities subject to the PCMLTFA and the Regulations to understand their obligations. IDA By-laws, Policies and Regulations are legally enforceable and can be considered as "other enforceable means". OSFI and FINTRAC Guidance are considered as non-binding guidance for the purpose of this report.

26. In Canada, certain entities that undertake financial activities, as defined by the FATF Recommendations, are not currently covered by the AML/CFT regime (except for entities that are caught because they also engage in financial activities which are captured under the regime). These include: financial leasing entities; factoring entities; finance companies (*i.e.* mostly entities specialized in consumer lending, issuing certain types of credit cards, equipment financing and unregulated small business lending entities); providers of e-money; Internet payment providers[5]; and cheque cashers[6] when their only activity is cashing cheques issued to denominated persons. Canada considers that these entities pose little or no threat of money laundering/terrorist financing. Canada's approach to risk is not in line with the FATF approach as defined in the Methodology where a list of activities and operations must be covered by the AML/CFT regime unless there is a proven low risk of ML/TF. Canada has applied the opposite approach and has extended coverage of the PCMLTFA only to activities for which there is a proven ML/TF risk. Moreover, the risk assessment process carried out by Canada to reach conclusions on the exposure of certain sectors to ML/TF risks is either non-existent or very fragmented and ad-hoc.

27. Customer identification measures in Canada are currently insufficient to meet the FATF standards[7]. Current legislation does not impose a requirement for financial institutions to conduct CDD in all cases covered by the FATF standards, including when there is a suspicion of ML or TF or when financial institutions have doubts about the veracity or adequacy of previously obtained CDD data. The current customer identification measures for natural persons are insufficient and, except for IDA supervised entities, financial institutions are not required to understand the ownership and control structure of the customer nor obliged to determine the natural persons that ultimately own or control the customer. There are currently no requirements (except for IDA supervised entities) to obtain information on the purpose and intended nature of the business relationship. There is no obligation to perform enhanced due diligence for higher risk categories of customer, business relationship or transaction and the current approach is not in line with the FATF standards regarding situations of lower risk. Finally, the timing of verification of customer identity is inadequate for certain financial entities vis-à-vis certain customers. Financial institutions (except IDA supervised entities in some circumstances) are not prohibited from opening an account or commencing a business relationship or performing a transaction and they are not required to make a suspicious transaction report where they are unable to identify the customer.

---

5 Internet payment and e-money providers are only subject to the Act if they also offer funds remittance or transmission services and, as such, would be considered money services businesses.

6 Cheque cashing businesses that also offer money remittance services are included in the definition of MSBs under the PCMLTFA and are therefore subject to the requirements of the PCMLTFA.

7 New provisions will enter into force in June 2008 and December 2008. These provisions will impose a number of additional requirements including in the following areas: CDD, politically exposed persons, SR VII, record keeping, reporting of suspicious transactions, requirements for DNFBPs, and beneficial ownership information in company legislation. These changes were not assessed as the changes fall outside the period of the evaluation.

28. At the time of the on-site visit, there were no specific legislative or other enforceable requirements in relation to PEPs and limited requirements in relation to correspondent banking relationships. Provisions in relation to the prevention of misuse of technological developments in ML/TF schemes and the mitigation of risks associated with non-face to face business were not in compliance with the FATF requirements. New provisions entered into force in June 2007 for correspondent banking, and will enter into force in June 2008 in relation to PEPs. Although introduced business arrangements exist in Canada, Canada has not implemented adequate requirements in relation to third party introduced business.

29. There is no financial institution secrecy law that inhibits the implementation of AML/CFT requirements. Canada's record-keeping requirements are generally satisfactory. At the time of the on-site visit, Canada had not implemented SRVII on wire transfers.

30. Under the PCMLTFA, there is currently no explicit provision requiring financial institutions to pay special attention to all complex, unusual large transactions. Such a requirement may only be indirectly deduced from (a) the requirement to report to FINTRAC suspicious transactions that may be related to money laundering or terrorist financing, and (b) the obligation to report large international electronic funds transfers and large cash transactions. Canada should ensure that the new provisions coming into force in June 2008 will fully and effectively address these issues. The obligation to give special attention to business relationships and transactions with persons from countries which do not or insufficiently apply the FATF Recommendations is also not fully met.

31. All financial institutions subject to the PCMLTFA are required to report to FINTRAC transactions of any amount for which there are reasonable grounds to suspect are related to the commission of a money laundering offence or a terrorist financing offence. However, certain categories of financial institution (see comments above) are not subject to the PCMLTFA and, consequently, to any mandatory reporting requirement to FINTRAC. Under the current legislation, reporting entities are only required to report completed transactions to FINTRAC. As from June 2008, the reporting requirement will be broadened to the reporting of any suspicious attempted transactions related to money laundering or terrorist financing. The total number of STRs sent by the financial sector appears satisfactory (an average of 20 000 every year since 2004). The different financial institutions however contributed unequally to the total number of STRs (securities dealers, life insurance companies and life insurance brokers and dealers have sent limited numbers of STRs).

32. No criminal or civil proceedings lie against persons and entities for making a suspicious transaction report, a terrorist property report, a large cash transaction report or an electronic funds transfer report in good faith or for providing FINTRAC with information about suspicions of money laundering or of the financing of terrorist activities. The provisions in relation to tipping off are also fully in line with the FATF standards. FINTRAC gives very detailed guidance related to STRs to assist financial institutions in implementing and complying with STR requirements and provides satisfactory general feedback to large financial institutions. Specific feedback is provided within the legislative limitations. The PCMLTFA requires reporting entities to submit reports to FINTRAC on large cash transactions and electronic funds transfers and the FATF requirements in that area are met.

33. The requirements in relation to internal procedures, policies and controls to prevent ML and FT are generally sound, but some changes are needed to bring them fully in line with the FATF standards. FRFIs have generally adopted enterprise-wide AML/CFT standards based on the OSFI Guideline and supervisory practice. There is no specific requirement regarding the enforcement of AML/CFT measures consistent with Canadian or FATF requirements in foreign branches and subsidiaries.

34. In addition, Canadian financial entities are prohibited from entering into a business relationship with shell banks or with foreign financial institutions that have correspondent banking relationships with shell banks. Canada is broadly in compliance with the FATF requirements in this regard.

35. FINTRAC is responsible for ensuring compliance with the PCMLTFA. FINTRAC's compliance program is based on a collaborative risk-based approach divided into two categories: the promotion of compliance and the monitoring of compliance. FINTRAC has signed MOUs with certain financial and gaming regulators or supervisors to share AML/CFT supervisory information. In addition, some regulators have provisions under their own legislation or codes of conduct that impose similar requirements to, or which complement the key provisions in the PCMLTFA. Globally, there are unequal degrees of regulation and supervision, depending on the sectors and provinces although OSFI is responsible for regulating well over 80% of the Canadian financial sector as measured by total assets. It is worth mentioning that the entities which are currently not subject to the PCMLTFA are not subject to prudential supervision either.

36. The number of examinations performed by FINTRAC appears to be relatively low compared with the total number of reporting financial entities (potentially more than 100 000) although a single FINTRAC examination can cover a large number of reporting entities (*e.g.* in the case of life insurance companies/agents and securities firms/dealers). Even including examinations conducted by FINTRAC's MOU partners, the figures remain rather low, except for the banking and federally regulated trust companies sectors which have a good supervisory coverage by OSFI. The use of a sophisticated risk-based model helps FINTRAC prioritise its supervisory activities. Those activities encompass not only examinations of reporting entities but also guidance, outreach, self-assessment tools and follow-up actions after examinations.

37. The securities sector is regulated by provincial securities regulatory authorities (SRAs) and has been subject to limited AML/CFT supervision. The on-site AML/CFT assessments conducted by OSFI since 2003 in the federally regulated life insurance sector amount to 90% of the industry measured by its assets but less than 10% of the supervised population. AML/CFT supervision by provincial financial supervisors appears to be less effective for life insurance agents because AML/CFT controls are mostly assessed by FINTRAC. In addition, despite the focus put on that sector, FINTRAC had managed to perform controls on only 60 credit unions and *caisses populaires* up to mid-2007, out of a total population of 1 250 reporting entities.

38. Under the current version of the PCMLTFA and its Regulations, FINTRAC has limited powers of enforcement against reporting entities and their directors or senior management for failure to comply with or properly implement AML/CFT requirements. Currently, FINTRAC cannot impose penalties and is limited to referring cases to law enforcement for investigation. Strengthening the sanctions regime in June 2008 with the introduction of administrative and monetary penalties should be a crucial enhancement of the system. The current PCMLTFA provides for a series of criminal sanctions for contraventions of various provisions of the Act. These can lead to criminal penalties of up to CAD 2 million in fines and five years in prison for non-compliance. The December 2006 amendments expanded the regime of criminal sanctions to the violations of most of the provisions of the PCMLTFA and regulations.

39. OSFI has a wider range of possible enforcement actions or sanctions than FINTRAC. Nevertheless, sanctions remain infrequently used, and do not appear to be sufficiently effective, proportionate and dissuasive, though this may be partially due to the early intervention strategy adopted by OSFI. In the securities sector, except for IDA which has effectively applied in a number of cases heavy sanctions to its members for non compliance with AML/CFT standards, it seems that the powers of sanction have generally not been used by SRAs or SROs in that area, as they have rarely issued specific rules or regulations related to AML/CFT and consider such issues to be mainly FINTRAC's responsibility.

40. Measures aimed at preventing criminals or their associates from holding a significant or controlling interest or holding a management function in a financial institution, as well as the "fit and proper" principle are widespread. There is no systematic harmonization of these requirements across the federal and provincial systems. At the time of the on-site visit, there was no compulsory obligation

for FRFIs to implement screening procedures for directors or senior management, after the initial incorporation or authorisation procedures are concluded.

41. There was no registration regime for MSBs at the time of the on-site visit although Canada has created a federal registration regime that will enter into force in June 2008. The preventive measures currently applicable to MSBs (especially in relation to CDD, reporting of suspicious transactions or SRVII) present serious weaknesses and the MSB sector is subject to a limited range of preventive measures that are not in compliance with international standards. In addition, the sanction regime applicable to MSBs that fail to comply with the PCMLTFA is currently not effective, proportionate and dissuasive. Canada should ensure effective implementation of the registration system for MSBs in force in June 2008 and ensure that the requirements applicable to MSBs fully meet the FATF requirements.

4. Preventive Measures – Designated Non-Financial Businesses and Professions (DNFBPs)

42. The PCMLTFA currently covers casinos, real estate brokers and sales representatives and accountants and accounting firms. Lawyers, Quebec Notaries, BC Notaries, dealers in precious metals and stones, Internet casinos, and TCSPs are not currently captured by the PCMLTFA and therefore are not subject to the requirements under Recommendations 5, 6 and 8-11. It should be noted that Internet casinos are illegal in Canada, but servers hosting such activity exists in Canada, and Canada should either take law enforcement action to eliminate this illegal activity, or regulate these casinos. The requirements in relation to Recommendation 5 and 13 applicable to land-based casinos, real estate brokers and sales representatives and accountants do not meet the FATF standards. Canada has not implemented any specific AML/CFT measures concerning PEPs that are applicable to DNFBPs. There are no specific legislative or other enforceable obligations for DNFBPs to take measures to prevent the misuse of technological developments in ML/TF schemes. The DNFBPs are not required to have policies and procedures in place to address any specific risk associated with non face-to-face business relationships or transactions. Provisions in relation to record-keeping with regard to casinos, real estate brokers and sales representatives and accountants are not fully in line with the FATF standards.

43. Because of limited staff resources, FINTRAC is not in a position to ensure an efficient monitoring of the effective application of AML/CFT legislation in the non-financial sectors captured by the PCMLTFA, especially in sectors/provinces where the primary regulators or SROs are not or insufficiently involved in AML/CFT compliance supervision. Canada should ensure that supervisory actions (especially on-site examinations) vis-à-vis casinos and more generally with regard to all DNFBPs are reinforced. With regard to DNFBPs, the sanction regime available to FINTRAC is currently inadequate but should be strengthened when administrative and monetary penalties are introduced in June 2008.

5. Legal Persons and Arrangements & Non-Profit Organisations

44. Canada's corporate registry and information collection system does not adequately focus on obtaining information relating to the beneficial owner or controller of bodies corporate in Canada. The information collected and maintained (including changes in information) relates almost solely to persons and other corporations that are the immediate owners or controllers of a corporation through shareholdings. The federal corporate registrar should consider measures to mitigate the threat that may arise from the use of legal persons to perpetrate money laundering and terrorist financing. Canada should ensure that competent authorities have access to accurate and current information on the ultimate beneficial owners and controllers of all legal persons on a timely basis.

45. The Canada Business Corporations Act (CBCA) appears to allow for the ownership of corporations through the use of bearer shares, although it is likely that the number of bearer shares is limited. Nonetheless, there do not appear to be any special measures in place to ensure disclosure of beneficial owners of these shares in order to mitigate the ML or TF risk.

46. Except for the province of Quebec (where the *fiducie* is similar to the trust), all provinces are common law jurisdictions and have trust laws. Canada relies on the investigatory powers of law enforcement to obtain or have access to information concerning the beneficial ownership and control of trusts and *fiducies*. These powers are generally sound and widely used. In the case of trusts and *fiducies*, limited, partial information is available, and even where certain information is recorded by agencies such as CRA or FINTRAC, agencies can only share this information with law enforcement authorities in limited circumstances. Canada should implement measures to ensure that adequate, accurate and timely information is available to law enforcement authorities concerning the beneficial ownership and control of trusts and *fiducie* in Québec.

47. Canada has a well-established registration system for charities and has taken considerable steps to implement SR VIII. Registered charities include most organizations that raise and distribute funds for social or humanitarian purposes. Charities represent the most significant portion of the financial resources of the NPO sector and account for a substantial share of the sector's foreign activities. Nevertheless, in line with the FATF's risk-based approach, Canada should continue to monitor risks in other segments of the NPO sector.

6. National and International Co-operation

48. Canada has developed a large number of initiatives to improve co-operation mechanisms among the different domestic stakeholders taking part in the fight against money laundering and terrorist financing. The interagency cooperation between the FIU and law enforcement authorities is not fully effective and should be enhanced in order for Canada to optimise its capacity to investigate ML and TF cases. Canada should consider encouraging more bilateral contacts among agencies.

49. Almost all of the provisions of the Palermo and Vienna Conventions have been fully implemented, and only some minor technical deficiencies remain. Canada has extensive formal and limited informal means of providing mutual legal assistance (MLA) to requesting countries. Where the evidence can only be gathered pursuant to a court order, Canada's Mutual Legal Assistance in Criminal Matters Act ("MLACMA" or "the Act") is the domestic legislation that enables a Canadian court to issue orders compelling the production or authorizing the seizure of evidence at the request of a treaty partner. Canada has a centrally-coordinated MLA regime involving: the Department of Justice, Crown prosecutors, the Judiciary and, on occasion, law enforcement agents who execute Canadian courts' orders. Canada should focus on improving the effectiveness of the current regime and the collection of adequate data.

50. Under the MLACMA, Canada can directly enforce foreign orders for the restraint, seizure and forfeiture of assets on receipt of a request from a treaty partner or designated entity in line with the FATF requirements. However, in terms of implementation, there is limited evidence of effective confiscation assistance, and Canada should consider how this could be enhanced.

51. The money laundering and terrorist financing offences are extraditable offences under Canada's Extradition Act. The current legal provisions on extradition meet the FATF standards; however Canada should maintain better extradition request data, so as to better assess the timeliness of assistance.

52. In general, law enforcement authorities can engage in a wide range of international co-operation. FINTRAC can also share its intelligence with foreign counterparts. As the AML/CFT supervisor, FINTRAC has the legal capacity to exchange supervisory information with foreign regulators, but has not yet entered into any MOUs that will allow it to share in practice. On the other hand, OSFI can exchange compliance information with foreign counterparts.

7. Other issues

53. Overall, authorities seem to be well-equipped, staffed, resourced and trained. There are concerns about the availability of resources within FINTRAC to undertake a sufficient number of comprehensive examinations. The number of staff at FINTRAC dedicated to the analysis of ML/TF cases is also too low. Finally, the authorities in charge of processing MLA requests should acquire additional resources to fulfil their tasks.

54. Canada collects a large set of statistics although more comprehensive data should be gathered regarding ML investigations and sentencing, MLA and extradition requests.

MUTUAL EVALUATION REPORT

1. GENERAL

1.1 General Information on Canada

55. Canada consists of 10 provinces (Alberta, British Columbia, Manitoba, Newfoundland and Labrador, New Brunswick, Nova Scotia, Ontario, Prince Edward Island, Québec and Saskatchewan), and three territories (the Northwest Territories, Nunavut and Yukon). Ottawa, Ontario, is the national capital. Geographically, it is the second-largest country in the world, with a land area of 9.9 million square kilometres. Canada is bordered by the United States of America to the south and northwest (Alaska), with coastlines on the Pacific Ocean to the west, the Arctic Ocean to the north and the Atlantic Ocean to the east. Approximately 86 % of Canada's 32 million people live in the country's four largest provinces: Ontario (39 %), Québec (24 %), British Columbia (13 %) and Alberta (10 %). Canadians have an average life expectancy of 80 years and the median age is currently 39 years. Canada's two official languages are English and French.

56. Canada is the eighth-largest economy in the world with about 70% of the economy devoted to services. Manufacturing now accounts for just over 25% and the primary sectors account for around 5%. In 2006, Canadian per capita gross domestic product (GDP) was CAD 44 083.

System of government

57. Canada is a federal state. Pursuant to the Constitution Act, 1867, the governing power of the country is divided between the federal government and provincial governments. The federal government is responsible for matters that affect all of Canada, including national defence, criminal law, banking, citizenship and foreign relations. Provincial and territorial governments look after such matters as education, health care and social services. They share responsibilities with the federal government in some areas. For instance, the federal government has legislative jurisdiction over criminal law and procedure, while the provinces are responsible for the administration of the courts of criminal jurisdiction including federal courts constituted under section 96 of the Constitution. This provincial jurisdiction includes the constitution, maintenance and organization of provincial courts in both civil and criminal jurisdictions, and civil procedure as applied in provincial courts. There is also a third level of government at the community level, known as municipal (or local) government, which is responsible for local matters.

58. Canada has a Westminster parliamentary system of government. Parliament is divided into three heads of power: the Queen, the Senate (the upper house of 105 members) and the House of Commons (the lower house of 308 members). Canada is a constitutional monarchy; Her Majesty Queen Elizabeth II is Canada's official head of state. She is represented in Canada by the Governor General, who gives Royal Assent, in the name of the Queen, to all legislation passed by Parliament. The Queen appoints the Governor General on the advice of the Prime Minister. One of the most important roles of the Governor General is to ensure that Canada always has a Prime Minister. The House of Commons, the Senate and the Governor General must approve all parliamentary bills before they become law. The government introduces most parliamentary legislation, but the Senate can also introduce its own bills, except bills to spend public money or impose taxes.

Legal system and hierarchy of laws

59. Canada is governed by the common law, or rule of precedent, and by a civil law system in Québec. Every federal law must be drafted in both official languages but, because of Canada's dual legal system, it must also respect both the common law and civil law traditions in the provinces. Provinces have a similar system for passing legislation into force with the exception that provincial legislatures do not have an upper house. As such, in order for provincial legislation to become law, it

requires enactment by the provincial legislature. The Queen's provincial representatives, the lieutenant governors, give Royal Assent, in the name of the Queen, to all legislation enacted by provincial legislatures. Territorial and local governments are not sovereign units. The powers of territories are delegated by Parliament, while those of local governments are delegated mainly by provincial governments.

60. Legislation and regulations are developed in a transparent manner to ensure they reflect the values of society and to ensure that use of the government's legislative and regulatory powers result in the greatest net benefit to Canadian society.

61. When a legislative proposal is made to the Cabinet, it is up to the sponsoring Minister to demonstrate that there are no other ways to achieve the policy objectives effectively. The decision to address a matter through a bill or regulation is made by Cabinet on the basis of analysis of the matter and its alternative solutions, consultations with partners and stakeholders, analysis of impacts of the proposed solution and analysis of the resources that the proposed solution would require. A bill must pass through a series of parliamentary stages (in the House of Commons and the Senate) before it becomes law. The final stage is Royal Assent. The Constitution Act, 1867 states that the approval of the Crown, signified by Royal Assent, is required for any bill to become law after passage by both Houses. Royal Assent can be given by the Governor General as the Queen's representative in Canada or a Deputy of the Governor General.

62. Regulations are another form of law that often stem from the introduction or amendments to legislation. Regulations are not made by Parliament but are made by persons or bodies to whom Parliament has delegated the authority to make them (such as the Governor in Council, a Minister or an administrative agency). Authority to make regulations must be expressly delegated by an Act.

63. The Statutory Instruments Act and the Regulatory Policy of the Government of Canada guide the development of regulations. The Statutory Instruments Act establishes a process designed to ensure that regulations are made on a legally secure foundation. A key element of the Policy is that Canadians are consulted, and that they have an opportunity to participate in developing or modifying regulations and regulatory programs. Each proposed regulation must pass through a series of steps before coming into force, including pre-publication, "making" the regulation, registration, publication, and distribution.

64. Draft regulations are pre-published in Part I of the Canada Gazette to give those who are interested in a regulatory proposal an opportunity to express their views. The length of pre-publication depends on the type of regulation, but typically lasts between 30 and 75 days. Following the period of pre-publication, regulations are "made" by the authority designated in the enabling Act and then transmitted to the Clerk of the Privy Council (within 7 days) for registration. Registration is a crucial step in the case of regulations because it determines when they take effect. Typically, regulations that must be registered come into force on the day they are registered. Following registration, regulations are published, in Part II of the Canada Gazette within 23 days after their registration.

The Canadian Charter of Rights and Freedoms

65. Canada has always sought to protect individual rights and freedoms through legislative enactments such as the Canadian Bill of Rights. This bill became law in 1960 and, as a federal statute, is limited in scope and has no application to provincial laws. On the other hand, the Canadian Charter of Rights and Freedoms enacted in 1982 is part of Canada's Constitution. Unlike the Bill of Rights, it constitutionally entrenches the basic principles and values by which Canadians live and govern themselves. It applies to both federal and provincial jurisdictions and guarantees, among other things, that everyone, regardless of colour, religion, race, belief or a ground analogous thereto, has certain fundamental rights and freedoms "subject only to such reasonable limits prescribed by law as can be demonstrably justified in a free and democratic society."

66. The Charter outlines fundamental rights and freedoms such as the right to life, liberty and security of the person; equality rights, such as the right to protection against discrimination; legal rights of persons accused of crimes, such as the right to a fair trial; freedom of conscience; freedom of religion; freedom of thought and freedom of association.

Canada's Privacy Laws

67. *Public Sector*. Privacy laws regulating the collection, use and disclosure of personal information by governments and the public sector have been in place in Canada since the early 1980s. On 1 July 1983, the Canadian federal government enacted the Privacy Act. This Act imposes obligations on some 150 federal government departments and agencies to respect privacy rights. Companion freedom of information legislation, called the Access to Information Act, was enacted at the same time. Most of Canada's provincial governments have followed suit with similar legislation covering both access to information and protection of privacy in provincial and municipal operations.

68. In relation to the fight against money laundering and terrorist financing, the Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA) sets out numerous provisions specifically designed to protect the privacy of individuals and defines the circumstances under which the Canadian Financial Intelligence Unit (the Financial Transactions and Reports Analysis Centre of Canada, FINTRAC) may disclose personal information. The impact of the PCMLTFA on the privacy of Canadians and the existence of sufficient safeguards in the anti-money laundering and counter terrorist financing legislation has raised discussions in Canada[8]. The amendments that are being brought to the AML/CFT legislation are scrutimized to ensure that the new requirements do not unduly compromise the privacy of Canadians.

69. *Private Sector*. As of 2007, Canadian business and private sector organizations are also subject to federal or provincial privacy protection legislation governing both customer and, with some exceptions, employee information. Québec was the first Canadian jurisdiction to introduce privacy protection legislation applicable to the private sector when it implemented its Act Respecting the Protection of Privacy in the Private Sector in 1994. The federal government enacted the Personal Information Protection and Electronic Documents Act (PIPEDA) effective January 1, 2001. PIPEDA applies to federally-regulated private sector organizations (*i.e.* organizations in the transportation, communications, broadcasting, federal banking and offshore sectors, as well as in Canada's three territories), and to other private sector organizations in provinces that have not enacted "substantially similar" legislation. It applies to personal information and health information that is collected, used or disclosed in the course of commercial activity that takes place across the Canadian border, between provinces, and within a Canadian province that has not enacted "substantially similar" legislation. To date, Alberta and British Columbia have joined Québec in enacting their own private sector privacy legislation. The Privacy Act gives individuals the right to access and request correction of personal information about themselves held by these federal government organizations.

70. The governments of all provinces and territories in Canada, except for Newfoundland and Labrador, also have legislation governing the collection, use and disclosure of personal information. The legislation varies from province to province, but the general right to access and correct personal information exists in all, and each has a commissioner or ombudsman who is authorised to handle complaints.

Court System

71. Canada's court system comprises four levels of courts with varying jurisdictions. First there are provincial and territorial courts, which handle the great majority of criminal cases and some civil cases (*e.g.* family law). Second are the provincial and territorial superior courts (which are federally constituted but provincially administrated, Courts under 96 of the Constitution). Generally, these

[8] See for instance Bill C-25, *An Act to amend the Proceeds of Crime (Money Laundering) and Terrorist Financing Act, the* Opening Statement by the Privacy Commissioner of Canada at: http://www.privcom.gc.ca/parl/2006/parl_061213_e.asp.

courts deal with more serious crimes. They may also take appeals from provincial and territorial court judgments. On the same hierarchical level is the Federal Court, which is responsible for various matters of federal jurisdiction, including immigration and tax cases. At the next level in the hierarchy are the provincial and territorial courts of appeal (again federally constituted) and the Federal Court of Appeal. The final arbiter of the law and highest court of appeal for all matters is the Supreme Court of Canada. The Supreme Court of Canada also plays a special role as adviser to the federal government on interpretation of law. In such a case, a specific question reaches the Supreme Court not after making its way through the court system, but via a direct referral from the government. Such cases are often called "Supreme Court references." Under the Canadian Charter of Rights and Freedoms, individuals accused of the most serious criminal offences (classified as indictable offences) generally have the right to choose to be tried by a judge and jury.

Measures against corruption

72. Corruption is considered to be a serious offence and the Canadian authorities have indicated that it is given high priority in Canadian domestic law. The federal government has amended existing legislation (including the Income Tax Act) and enacted new legislation (Corruption of Foreign Public Officials Act), parliamentary rules and administrative provisions to prevent and prohibit corruption.

73. Most recently, the Government adopted the Federal Accountability Act which puts in place a five-year lobbying ban, eliminates corporate and union donations, and protects whistleblowers, among other reforms. It also updated indictable offences for fraud with respect to public money or money of a Crown corporation, as well as penalties for these offences that include fines and imprisonment. An amendment to the Criminal Code makes persons convicted of those fraud offences ineligible for employment by the Crown, as well as being unable to otherwise contract with the Crown or benefit from contracts between the government and another person.

74. Canada plays an active role in the fight against corruption in a number of fora, such as the United Nations (UN), the Organisation for Economic Co-operation and Development (OECD), Asia-Pacific Economic Cooperation (APEC) and the Organization of American States (OAS). In 1998, Canada ratified the OECD Convention on Combating Bribery of Foreign Public Officials in International Business Transactions, thus triggering the convention's entry into force. Canada also ratified the OAS's Inter-American Convention Against Corruption at the OAS. More recently, efforts have focused on the negotiation of the UN Convention Against Corruption (UNCAC) on 31 October 2003, and Canada signed the UNCAC on 21 May 2004, and ratified it on October 2, 2007.

Ethics

75. Under the Constitution, the judiciary is separate from and independent of the other two branches of government, the executive and the legislative. Judicial independence is a guarantee that judges will make decisions free of influence and based solely on fact and law. It has three components: security of tenure, financial security and administrative independence. The Canadian Judicial Council, which is responsible for federally appointed judges, consists of the chief justices of all of the federal courts and provincial and territorial superior courts. The federal government created it to promote efficiency, consistency and good service in these courts. The Council has developed a set of ethical principles for judges, designed to assist judges in maintaining their independence, integrity and impartiality.

76. Prosecutors, known in Canada as Crown counsel, exercise their independence as representatives of an Attorney General. As such, the "independence" of Crown counsel is a delegated independence. Federal Crown counsel are obliged to make decisions in accordance with the policies of the Attorney General in the Federal Prosecution Deskbook. In general, each province also has a deskbook or a similar document to guide the provincial Crown counsel in their day-to-day work. Crown counsel is obliged to exercise independent judgment in making decisions. They are accountable for their decisions, and they must consult where required. Police officers are also subject to strict professional and ethical codes of conduct.

1.2 General Situation of Money Laundering and Financing of Terrorism

Predicate offences

77. Illicit proceeds from a variety of criminal activities contribute to the ongoing money laundering situation in Canada although drug trafficking is considered the source of much of the money laundered. Other sources of proceeds of crime include, but are not limited to, prostitution rings, contraband smuggling, illegal arms sales, migrant smuggling, and white-collar crime such as securities offences, real estate fraud, credit card fraud and telemarketing fraud.

78. The sales of illegal drugs in Canada amount to several billion dollars annually. Marijuana is one of the few drugs produced on a large scale in Canada. As such, an increasing amount of drugs is being smuggled into other countries, primarily the United States. There is evidence that in certain areas, both cocaine- and marijuana-trafficking organizations use money service businesses and currency exchanges to convert Canadian and U.S. dollars without going through formal exchange channels.

FINTRAC disclosures to law enforcement

79. Financial transactions in FINTRAC's drug-related case disclosures were cash intensive and, very often, of significant dollar value. Related financial activity frequently involved the use of foreign currency exchanges and casinos, and the physical or electronic movement of funds into or out of Canada. The vast majority of 2005/2006 disclosures fell into two readily identifiable categories of predicate offences: suspected illegal drugs and suspected fraud.

80. Suspected drug case disclosures were most prevalent and revealed the activity of small, homogenous networks of individuals. Suspected fraud cases were the largest in terms of scope, volume of transactions and dollar value. As opposed to the drug cases, suspected fraud cases appeared more complex and more organized. Many had a significant international dimension, and usually involved more than four businesses and four individuals. These companies often made heavy and uneconomical use of electronic funds transfers, and used multiple companies to conceal criminal funds.

Types of Criminal Organizations

81. Increasingly over the last several years, the Integrated Proceeds of Crime Units[9] (IPOC Units) have focused their investigation and assistance work on organized crime. Overall, more than 80% of the major files involved organized crime groups, climbing from 74% prior to 2001 to over 85% in the years since. Outlaw motorcycle gangs and other types of organised crime are present in Canada.

Money Laundering Methods

82. The money laundering methods used in Canada have remained relatively consistent in recent years. They essentially consist of: smuggling; money service businesses and currency exchanges; casinos; purchase of real estate; wire transfers; establishment of offshore corporations; credit cards, stored value cards and new payment methods; use of nominees; use of foreign bank accounts; use of professional services (lawyers, accountants, etc.); and reinvestment and distribution in illicit drugs.

83. At the placement stage, criminals are using money service businesses or casinos. Electronic funds transfers are being used for layering and at the integration stage, criminal proceeds are used to purchase high-value assets – such as cars, boats, jewellery, gold, diamonds and collectible items – in attempts to conceal the origin of the funds. Most recently, there have been signs that criminals are turning to such methods as Internet payments or cross-border movement of gold bullion.

---

[9] The IPOC Initiative brings together the skills, knowledge and abilities of a diverse group of experts including law enforcement officers, lawyers from the Department of Justice, forensic accountants and property managers from Public Works and Government Services Canada, Officers from Canada Border Services Agency, as well as Tax Agents from Canada Revenue Agency. The integration of the partner agencies facilitates a coordinated approach towards combating organized crime. For more information, see Section 2.6 of the report.

84. **Currency smuggling**. Cash continues to be a vehicle of choice for money laundering in Canada. Investigators regularly make large cash seizures of Canadian and U.S. currency and seize assets purchased with cash, such as real property, vehicles, personal property (jewellery, furniture and appliances), collectibles (antiques, coins, stamps) and other assets. Money launderers seem to be increasingly using the most rudimentary forms of money laundering, such as physically smuggling cash domestically and across international borders. Since 1994, nearly CAD 3 billion worth of contraband and cash has been seized as a result of the Pipeline/Convoy/Jetway Program[10].

85. **Money Service Businesses and Currency Exchanges**. Money service businesses (MSBs) and currency exchanges (F/Xs) play a role in money laundering activities, especially in large marijuana-producing areas, such as the Greater Vancouver region of British Columbia, where proceeds from sales in the U.S. must be converted into Canadian dollars. Both cocaine- and marijuana-trafficking organizations use some F/Xs to handle transactions involving different currencies used in cross-border activities. It appears that some foreign exchange dealers have also purposely dealt with other MSBs or foreign exchange dealers to avoid more traditional financial services, thereby limiting potential suspicions of links to criminal activity. Cheque cashing businesses have also been used as fronts for money laundering.

86. **Casinos**. Criminals use the Canadian casino industry extensively to launder illicit funds. They employ various techniques, including refining, exchanging currency, and chip purchases.

87. *Refining*. This term usually refers to the exchange of CAD 20 bills for CAD 50 or CAD 100 bills at the cash counter. In a variation often called the "ticket in ticket out" technique, criminals feed street-level money (CAD 5, CAD 10 and CAD 20 bills) into video lottery terminals. After minimal play, they cash the ticket stub at the counter for CAD 100 bills. In some instances, organized groups divide money to be refined among a number of individuals. They then enter the casino and go their own way. Once they have refined the money, they meet again outside the casino to assemble the total amount.

88. *Currency exchange*. Criminals are using casinos more frequently for currency exchange services. Several individuals associated with marijuana grow operations have used casinos to convert their proceeds of crime from U.S. currency into Canadian currency. Also, on occasion, they try to obtain casino cheques. In one case, a known chemical drug trafficker travelled to a casino outside his province of residence to exchange U.S. currency, obtained in Canada from drug-trafficking activities, for Canadian currency. Groups of people will also divide U.S. currency into small amounts to be exchanged for Canadian currency. They tend to use multiple casino locations. After exchanging the currencies, they meet again to assemble the total amount.

89. *Chip Purchases*. Buying casino chips in excess of the level of play and then cashing them out for a casino cheque is a known money laundering technique, frequently used by groups attempting to launder large sums of money. Some groups will travel outside their province of residence to use this technique. Reports from casinos to FINTRAC show that criminals tend to divide this money laundering activity into two separate tasks: some individuals buy casino chips, while others redeem these chips for a casino cheque. The group meets outside the casino to assemble the total amount. The separation of tasks makes it difficult to identify the individuals involved and to introduce detection methods. There is also evidence that casino chips are used as currency to purchase narcotics and contraband.

90. **Front companies**. Businesses that are especially attractive to money launderers are ones that customarily handle a high volume of cash transactions, such as retail stores, restaurants, bars, video rental stores, arcades, gas stations and food markets. As mentioned earlier, F/Xs, MSBs, and payday loan and cheque cashing businesses can also be used as fronts.

---

[10] The RCMP program's focus is the detection and seizure of contraband moving across Canada in cars and transport trucks.

91. **Real Estate**. Ongoing trends related to money laundering in the real estate sector include the following: (1) the use of nominees to register and make payments associated with real properties; (2) the use of facilitators — lawyers, real estate agents and mortgage brokers — to circumvent legal procedures, falsify documents and obscure the true nature of real estate transactions; and (3) the use of private mortgages (often involving the previous owner of a real property), and loan-back schemes.

92. **Gatekeepers**. Professionals such as accountants and lawyers act as "gatekeepers" when they provide access to the financial sector for their clients. This fact is open to abuse by criminals, who seek to use the gatekeeper to access the financial system, while themselves remaining anonymous. These professionals can also help clients move or conceal the proceeds of illegal activity.

93. **Credit Cards**. Credit cards are being used more frequently in every step of the money laundering process. In the initial placement stage, such techniques as "smurfing" or "structuring" can be used. Credit cards can be used to "commingle" legitimate revenues with proceeds of crime. At the layering stage, credit cards can be used in various ways: to transfer funds between accounts, to buy financial instruments and to carry out transactions in offshore jurisdictions. In the final integration stage, criminals primarily use credit cards to buy financial investments and luxury, "big ticket" items.

94. **Precious Stones**. Some investigations have revealed that the Canadian diamond industry is vulnerable to the threat of organized crime and money laundering.

95. **Stored Value and New Payment Methods**. Canadian law enforcement agencies have identified the use of credit cards, stored value cards and prepaid credit cards as an element of a growing number of money laundering schemes in Canada.

96. Internet payment systems (IPSs) are still quite new; one of the most popular systems, PayPal, was founded in 1998. IPSs allow users to send money around the world without going through the normal paths of the world's banking system. IPS accounts could be used to settle purchases of narcotics, contraband items, cigarettes, alcohol or stolen properties, for example.

97. **Trade-Based Money Laundering (TBML).** The Canadian law enforcement authorities have identified cases of TBML in relation to Colombian criminal organizations and cocaine importation in Canada.

98. **White-Label ATMs**. The Canadian law enforcement authorities have been confronted with cases involving White-Label automated teller machines (ATMs) which are owned and operated by independent service operators — individuals or companies — rather than banks. There are limited requirements on who can own or operate a white-label ATM due to a Competition Tribunal decision[11]. The owners of white-label ATMs have access cards that enable them to load cash into the machine. However, they are asked to identify the source of those funds only once, when they first set up the machine.

Terrorist Financing

99. Canadian authorities have identified a number of terrorist organisations operating in Canada. Investigations have shown that terrorist cells have a tendency to remain self-sufficient by generating funds locally. In some instances, they may do so by committing petty crimes, such as welfare fraud or credit card fraud. In other instances, cell members have started businesses to glean financial information from unsuspecting customers in order to clone credit cards and commit identity thefts. The RCMP has intelligence indicating that suspected terrorist entities in Canada are raising funds through drug trafficking or donating a portion of their criminal proceeds to support terrorism.

[11] In its decision of June 20, 1996, (CT-95 / 2) the Federal Competition Tribunal made an order that opened up the ATM market to independent operators. Prior to this decision, only banks and other deposit taking financial institutions had been allowed to join the *Interac Association* and operate ATMs.

100. Terrorists use techniques similar to those used by money launderers to evade authorities' attention and to protect the identity of their sponsors and the ultimate beneficiaries of the funds. Terrorist financing methods seen in Canada include the following: (1) the physical transportation of cash and other valuables; (2) the formal banking system; (3) MSBs and F/Xs; and (4) Internet value transfer systems. The most common venue for moving funds for the purpose of terrorism is the traditional banking system, since terrorism-related transactions can be camouflaged in the sheer volume of normal banking transactions.

101. In the course of fiscal year 2005/2006[12], FINTRAC made 34 case disclosures with a value of some CAD 256 million related to other threats to the security of Canada. FINTRAC observed that a large percentage of its case disclosures had an international component, where funds were wired to locations known to be terrorist hot spots. A number cases involved large cash deposits, made to personal or business accounts, where the funds were subsequently wire transferred out of the country.

102. **Value Cards.** Apart from wire transfers, value cards used to transfer funds for the purposes of terrorism are a relatively new trend in Canada and internationally. Value cards can be assets to terrorist supporters as they offer a convenient mechanism to quickly and easily transfer funds, often under the cloak of anonymity.

103. **Internet Payment Systems**. The newest terrorist financing method observed in RCMP investigations is the use of the Internet, where terrorist entities have set up accounts with electronic money services. These accounts can be credited from anywhere in the world by any person, and credits can be transferred from one account to another. These accounts can then be used to make purchases online. Credits can be purchased with cash at participating stores in the form of value cards in increments such as CAD10 or CAD20, similar to pre-paid telephone calling cards. Each card has a serial number. Once that number is entered on the money services website, the value of the card can be credited to a specific account. Such money services accounts facilitate the issuing of credit card accounts where electronic money services have agreements with banks. Users can transfer credits from these electronic money services accounts to credit card accounts, then use the credit cards in the normal fashion. These electronic money services are of particular concern because they are managed outside Canada.

104. **Charities**. Charities may collect donations from the public to support humanitarian causes overseas and forward the funds to overseas locations via the regulated banking system. At the receiving end, however, a portion of the funds may be diverted to support terrorism, with or without the complicity of Canadian donors and collectors. Analysis shows that charities and other non-profit organizations (NPOs) have figured in over one-third of FINTRAC disclosures related to suspected terrorist activity financing. These cases appeared to be associated with the collection of funds and financial movement suspected of being related to terrorist financing activity. These included: the use of multiple accounts by several NPOs, making the tracing of funds more difficult; the movement of funds to locations/countries of conflict, making it difficult to determine whether or not they are used for legitimate charitable purposes; and finally, the use of personal accounts by individuals or business accounts directly associated to NPOs, suggesting the possibility that accounts, other than the NPO accounts, are being used to collect and move funds.

Terrorist Financing Charges Brought Before Canadian Courts

105. Since the Anti-Terrorist Act came into effect in Canada in December 2001, there have been two instances where terrorist financing charges have been laid. Those two cases are currently before the courts.

106. The first case involves an individual named Momin Khawaja. He has been charged with seven offences under the Anti-Terrorist Act, including one charge related to terrorist financing under

[12] As is standard practice for the Government of Canada, fiscal years cover the period of April 1st to March 31st of the following year.

section 83.03 of the Criminal Code (providing property or services for terrorist purposes). This case has not been adjudicated yet. The case is linked to ongoing court proceedings in the U.K., where a terrorist allegedly attempted to build a 600-kilogram fertilizer-based bomb to attack targets in that country.

107. The second case involves the "Toronto 18" group. In June 2006, 18 individuals were arrested and charged in Canada with various offences under the Anti-Terrorist Act. Three of the 18 individuals were charged with terrorist financing offences under section 83.03 of the Criminal Code. None of these cases have been adjudicated yet. The most notable activities of this group included undergoing para-military training in Canada in December 2005, allegedly for terrorist purposes. This training allegedly spawned the formation of a sub-group in March 2006 that had the clear intention of building truck bombs to carry out terrorist attacks in the Toronto area.

1.3 Overview of the Financial Sector and DNFBP

Overview of the financial sector

Background

108. Overall, the financial sector contributes 6 percent of Canada's gross domestic product and has a yearly payroll of over CAD22 billion. The city of Toronto – located in Canada's most populous province, Ontario – is recognized as the centre of Canada's financial sector, with most of the large banks' headquarters, the country's equity exchanges (the Toronto Stock Exchange), the country's sole central securities depository (the Canadian Depository for Securities), the country's largest securities regulator (the Ontario Securities Commission), and offices of various regulators and other financial institutions. Two other major cities – Montréal, located in the province of Québec, and Vancouver, in the province of British Columbia – have vibrant financial sector activities.

109. While the financial sector in Canada is diverse and includes many service providers, it should be noted that the sector is significantly integrated, as different players offer similar services and "financial groups" or conglomerates offer a variety of financial products. Most notably, banks represent the largest portion of the Canadian financial services industry, reporting CAD1 257 billion in domestic assets in 2003, or over 70% of total assets within the financial sector. This integration is even more significant in light of the fact that Canada's six largest domestic banks account for the bulk of the activity, holding over 90% of all banking assets. Further, in the securities industry, the 11 largest firms (six of which are owned by the same largest domestic banks) account for 71% of total industry revenues. The five largest life insurance companies account for over 60% of the net premiums written by life insurers in Canada.

110. The following table compares the financial activities that define financial institutions under the FATF standards with financial sector entities subject to Canada's AML/CFT requirements:

Financial Activities as Defined by the FATF	Banks	Credit Unions, Caisses Populaires, Cooperative Cooperative Credits Societies	Trust and Loan Companies	Investment Dealers	Mutual Fund Dealers	Portfolio Managers/ Investment Counsellors	Life Insurance Companies, Brokers and Agents	Money Service Businesses	Credit Card Companies	Crown Corporations That Accept Deposits	Canada Post (Money Orders)
1. Accepting deposits	✓	✓	✓							✓	
2. Lending	✓	✓	✓	✓	✓	✓	✓		✓		
3. Financial leasing	✓		✓				✓				
4. Transferring money or value	✓	✓	✓				✓	✓			
5. Issuing or managing means of payment	✓	✓	✓						✓		✓
6. Providing financial guarantees and commitments	✓	✓	✓				✓				
7. Trading: money market instruments, foreign exchange, securities, futures	✓	✓	✓	✓	✓	✓	✓				
8. Participating in securities issues	✓	✓	✓	✓	✓	✓	✓				
9. Managing portfolios	✓	✓	✓	✓	✓	✓	✓				
10. Safekeeping and custodial services	✓	✓	✓								
11. Investing and managing funds on behalf of others	✓	✓	✓	✓	✓	✓	✓				
12. Providing life insurance		✓					✓				
13. Changing money and currency	✓	✓	✓					✓			

Notes

1. There are businesses that specifically provide financial leasing arrangements. However, based on a risk analysis, the government has decided not to impose AML/CFT requirements on financial leasing companies.
2. Some businesses are involved solely in providing the credit card payment infrastructure to allow information to flow from the merchant to the company that manages the credit card accounts. These businesses have been excluded from the AML/CFT requirements due to their limited involvement in financial transactions.

Banking sector

111. *Background*. As of October 2006, there were 21 domestic banks, 25 foreign bank subsidiaries and 25 foreign bank branches operating in Canada (20 full-service branches and 5 lending branches). At the end of 2005, these institutions had over CAD2.1 trillion in global assets, including CAD1.5 trillion in domestic assets – accounting for about 70% of the total assets within the Canadian financial services sector. The six largest domestic banks account for the bulk of the activity, holding over 90% of banking assets as of the end of 2005[13]. The market concentration is as follows (December 2005):

[13] This does not include the assets of non-bank deposit-taking institutions, such as credit unions and caisses populaires.

Bank	Number of Deposit-taking branches in Canada	Number of ATMs in Canada	112. Assets (CAD billions)	Market Share (%)
Royal Bank of Canada	1 104	3 906	486	23.6
Toronto Dominion Bank	1 014	2 400	369	17.9
The Bank of Nova Scotia	950	2 500	324	15.8
Bank of Montreal	968	2 700	301	14.6
Canadian Imperial Bank of Commerce	1 100	4 000	289	14
National Bank of Canada	457	788	104	5.1
Total	5 593	15 994	1 872	91.0

Source: Office of the Superintendent of Financial Institutions.

113. Canada's banks operate through an extensive network that includes close to 6 000 branches and about 15 000 automated teller machines (ATMs) across the country. Canadians have access to an additional 35 000 ATMs operated by non-bank third parties. Canada has the highest number of ATMs per capita in the world and benefits from the highest penetration levels of electronic channels such as debit cards, Internet banking and telephone banking.

114. *Regulation and supervision*. Under the Bank Act, the federal government is responsible for the regulation of banks in Canada. However, given the diverse nature of the banks' activities, some of their subsidiary activities – such as trustee services and securities dealing – are provincially regulated. FINTRAC is responsible for ensuring compliance with AML/CFT requirements by banks and the Office of the Superintendent of Financial Institutions (OSFI) is the federal agency responsible for supervising banks in Canada. The Bank of Canada, Canada's central bank, works with other agencies and market participants to promote the safe and efficient operation of the financial system's key elements.

Credit Unions and *Caisses Populaires*

115. *Background.* Credit unions and *caisses populaires* are cooperative financial institutions owned and controlled by their members. Their ownership and corporate governance are based on cooperative principles, and their primary commitment is to serve their members' financial needs. In most provinces, each customer is required to become a member of the credit union or *caisse populaire*. Each member of a credit union or *caisse populaire* becomes a shareholder and has one vote, regardless of the size of deposit or share capital held. Members may run for election to the board, attend the annual meeting and vote on the election of directors and other matters. As shareholders, members are also entitled to yearly dividends and profit sharing.

116. In Québec, the provincially regulated Desjardins Group is the largest financial institution and consists of a network of *caisses populaires*. Outside Québec, all credit unions are shareholders in one of the nine provincial centrals, which are responsible for ensuring liquidity at the provincial level and providing services as a trade association. In turn, all nine provincial centrals are the primary shareholders of Credit Union Central of Canada (CUCC), which is responsible for establishing liquidity policy and overseeing liquidity maintenance at the national level.

117. Credit unions and *caisses populaires* are diversifying their services into non-traditional areas including full-service brokerage functions, mutual funds, commercial lending and wealth management. Some credit unions and *caisses populaires* are active in the insurance market as well. Credit union and caisse populaire membership was approximately 10.7 million by the end of 2005, or one third of Canada's population. Membership is highest in Québec, where 68 % of the population belongs to a caisse populaire.

118. At the end of 2005, the cooperative financial sector had 3 450 locations and about 4 800 ATMs. Credit unions and *caisses populaires* have also been purchasing bank branches, particularly in isolated

areas, helping to ensure that all Canadians continue to have access to financial services. At the end of 2005, Canada's credit union sector consisted of some 1 250 institutions. Credit unions and *caisses populaires* have maintained strong market shares in such key service areas as residential mortgage financing (14% as of 2005), consumer credit (7%) and deposit services (13%).

119. *Regulation and Supervision*. All credit unions and *caisses populaires* are provincially or territorially incorporated, as there is no federal legislation providing for the incorporation of credit unions or caisse populaires. As a result, the sector is regulated at the provincial / territorial level for prudential soundness and market conduct. As with the banking sector, FINTRAC is responsible for ensuring compliance with AML/CFT requirements by credit unions and *caisses populaires*. Both the provincial centrals that elected to be regulated by the federal level and the CUCC are supervised for prudential purposes by OSFI.

Insurance sector

120. In Canada, insurance companies are categorized as either life and health, or property and casualty. Consistent with FATF standards, AML/CFT requirements apply only to life and health insurance companies. Insurance products are sold by agents and brokers, some of them selling exclusively a single company's products (tied agents) while others sell insurance products of multiple companies (independent agents and brokers). AML/CFT requirements also directly apply to these insurance agents and brokers.

121. *Background*. In 2004, about 24 million Canadians and their dependants were covered by some form of life and health insurance. The total value of life insurance owned by Canadians was over CAD2.6 trillion. In 2004, Canada's life and health insurance industry comprised 105 firms, down from 120 firms in 2004 and 163 firms in 1990. This decline is largely the result of foreign insurers selling their operations to Canadian insurance companies, although there has been significant merger and acquisition activity among Canadian companies as well. In 2004, the 5 largest companies accounted for approximately 64% of the net premiums written by life insurers in Canada. Four of these firms, and 7 of the top 10 firms, are Canadian companies, as noted with a (C) in the following table. In the insurance industry, the market concentration is as follows (December 2005):

Company	Market share (%)
Great-West Life (C)	17.8
Manulife (C)	16.8
Sun Life (C)	15.4
Munich Re	6.9
Desjardins Life (C)	6.7
Total (top five)	**63.7**
Industry Total	**100.0**

Sources: Department of Finance calculations, using data from OSFI, l'Autorité des marchés financiers du Québec and corporate annual reports.

122. *Regulation and Supervision*. The federal and provincial governments share jurisdiction over the regulation of life insurance companies. In practice, the industry is largely regulated for financial soundness by OSFI, as federally incorporated companies account for over 90% of the total premium income of life insurers. While provinces reserve the power to ensure that federally incorporated companies conducting business in their jurisdictions are financially sound, all provinces except Québec accept federal regulation in this regard. FINTRAC is responsible for ensuring compliance with AML/CFT requirements for all life insurance companies.

Trust and Loan Companies

123. *Background*. Trust and loan companies offer services similar to those provided by banks; for instance, they accept deposits and make personal and mortgage loans. Trust companies, however, can

also administer estates, personal and institutional trusts, trusted pension plans and agency contracts. Although banks themselves are not permitted to undertake these activities directly, banks own the largest trust companies.

124. Before the 1990s, trust and loan companies – with their wide network of branches – provided major competition to the banks. In 1992, prohibitions on the ability of banks to acquire trust companies were removed. As a result the landscape in this industry changed dramatically. The recession and subsequent drop in the real estate market at that time also dealt a heavy blow to trust companies. As a result, the independent trust industry, as measured by assets owned, declined by more than half from 1990 to 1999.

125. Currently, 81 relatively small trust and loan companies operate in Canada. They account for less than 2% of the assets in the financial sector. The few remaining independent trust companies – among them Equitable Trust, Home Trust and Effort Trust – deal primarily in mortgage lending.

126. *Regulation and Supervision.* Both levels of government regulate trust and loan companies. Market conduct is regulated at the provincial level, and federally incorporated trust and loan companies are regulated for prudential purposes by OSFI under the Trust and Loan Companies Act. FINTRAC is responsible for ensuring compliance with AML/CFT requirements for all trust and loan companies.

Securities

127. *Background*. The Canadian securities industry plays a key role in Canada's financial services sector. The securities industry is made up of integrated, institutional and retail firms. Integrated firms offer products and services that cover all aspects of the industry for both the institutional and retail markets. Their functions include raising debt and equity capital for companies, helping governments raise capital to fund their operations and serving retail investors. Institutional firms provide services to large corporate clients such as pension funds, insurance companies, mutual fund organizations, banks and trust companies. Retail firms, which include full-service firms and discount brokers, offer a wide range of products and services to retail investors. Some 90 000 Canadians are licensed or registered as dealers and advisers participants.

128. There are a large number of firms in Canada that are involved in the securities industry. Generally speaking, the firms can be broken down into four categories: investment dealers firms that can sell all types of securities, mutual fund dealers firms that can only sell mutual fund products, investment counsel and portfolio management firms that provide investment advice and counselling, and restricted dealers/limited market dealers that can only sell restricted types of securities.

129. The number of firms participating in the Canadian securities industry has risen consistently throughout the last two decades. In the investment dealers firms category, the market is dominated by retail firms, followed by institutional firms and integrated firms. However, integrated securities firms, the six largest of which are owned by the big six domestic banks, account for 71% of total industry revenues. Retail firms accounted for 18% of revenues, while institutional firms accounted for 11%.

130. *Regulation*. In Canada, securities regulation is an area of provincial responsibility. FINTRAC is responsible for ensuring compliance with AML/CFT requirements for all securities dealers. Provincial and territorial securities regulatory authorities are members of Canadian Securities Administrators (CSA), an umbrella organization of the 13 regulators that serves as a forum for coordinating and harmonizing the regulation of Canadian capital markets. Securities regulators also delegate certain aspects of securities regulation to self-regulatory organizations, including the Investment Dealers Association of Canada, Market Regulation Services, Inc. and the Mutual Fund Dealers Association of Canada.

Money Service Businesses (MSBs) including Foreign Exchange Dealers

131. *Background*. Money service businesses (MSBs) in Canada refer to firms that remit or transmit funds by any means, through any person, entity or electronic funds transfer network. It also applies to those parties who issue or redeem money orders, travellers' cheques or other similar negotiable instruments. MSBs include alternative money remittance systems (such as hawala, hundi or chitti). They also include financial entities that remit or transfer funds – or issue or redeem money orders, travellers' cheques or other similar negotiable instruments – for anyone who is not an account holder. Banks, trust companies, *caisses populaires* and credit unions, for example, are only considered to be MSBs when they do occasional transactions, such as transactions for non-account holders.

132. The MSB sector includes currency exchange dealers and comprises many different businesses in Canada, including established money transfer companies such as Western Union and MoneyMart; and one-person businesses that offer money transfer or currency exchange services in tandem with another activity, such as operating a convenience store, video rental service or ethnic store. FINTRAC has identified some 700 businesses offering money transfer or currency exchange services throughout Canada. A number of these MSBs entered into a contract with agents to offer their products at various locations.

133. *Regulation and Supervision*. Although MSBs are not specifically covered by prudential or market conduct regulation in Canada, these businesses are subject to AML/CFT requirements and FINTRAC assesses AML/CFT compliance standards of MSBs.

Overview of the Designated Non-Financial Businesses and Professions (DNFBPs)

Background

134. The following designated non-financial businesses and professions (DNFBPs) are subject to Canada's AML/CFT requirements: casinos, real estate agents and accountants. In addition, the Government of Canada is currently in discussion with the following DNFBPs to cover these entities under AML/CFT requirements: lawyers, notaries (in Québec and British Columbia only) and dealers in precious metals and stones. Trust and company services providers are not separately recognised nor regulated as a separate business category and do not fall under the AML/CFT regime. Trust companies, accountants, lawyers and other independent legal professions provide such services.

135. The DNFBPs in Canada are as follows:

Reporting Entities	# of Reporting Entities	Primary Regulator	AML/CFT Regulator
Casinos	91	Provincial authorities	FINTRAC
Real estate agents	100 000	Provincial authorities and SRO	FINTRAC
Accountants	157 000	SRO	FINTRAC
Lawyers/notaries	89 000	SRO	FINTRAC
Dealers in precious metals and stones	4 000	None	FINTRAC

136. It should be noted that the number of reporting entities generally represents the entire sector. As some DNFBPs are subject to the PCMLTFA only in specific circumstances, only a small fraction of the sector will actually be required to comply with the AML/CFT requirements. For example, the majority of accountants are employed by corporations or in public practice, while only a small fraction of the 157 000 are actually employed within professional firms in private practice.

Casinos

137. *Permanent casinos*. Permanent casinos were established in Canada starting in the early 1990s. Currently, there are casinos in seven provinces (Nova Scotia, Québec, Ontario, Manitoba, Saskatchewan, Alberta and British Columbia) and one territory (Yukon). These include 34 commercial

casinos, 23 charity casinos, 22 Slot facilities and 8 First Nation casinos. Combined revenues for commercial casinos only were CAD3.5 billion in 2004 and CAD3.7 billion in 2005.

138. Gaming products include a wide variety of card games, roulette and slot machines. Varied financial services area available at casinos, including some that resemble services provided by financial institutions. Depending on the province, casinos can open customer deposit or credit accounts, have facilities for transmitting and receiving funds transfers directly from other institutions, and offer cheque cashing and foreign exchange dealer services. These services are ancillary to their core financial services, which are the sale and redemption of chips/tokens.

139. In Canada, provinces are responsible for licensing, operating and regulating legal forms of gaming, a responsibility that includes creating the rules for gaming products and financial services available within the casinos. FINTRAC is responsible for ensuring that casinos have implemented AML/CFT requirements outlined in the PCMLTFA. Gaming regulators are provincial agencies and exchange information through the Canadian Association of Gaming Regulators (CAGRA). This informal group provides a forum for exchanging regulatory information and techniques; collecting and disseminating regulatory and enforcement information, procedures and experiences; and providing ongoing education and training.

140. *Internet and cruise ship casinos*. Internet casinos do not fall in the scope of the PCMLTFA as no province has approved an Internet casino to date. Despite this, servers hosting illegal online casino gaming facilities exist within Canada. In addition, cruise ships can offer casino facilities under strict conditions in Canadian waters and are not covered by the AML/CFT legislation.

Real Estate Agents

141. The real estate industry in Canada consists of approximately 100 000 licensed real estate brokers and sales representatives working through 99 local real estate boards, 10 provincial associations, a territorial association and a national association. Brokers and sales representatives work with either a purchaser or a seller of real estate to manage a real estate transaction.

142. Provinces are responsible for the regulation of real estate industry professionals. In addition to provincial regulators, industry associations or boards at the national, provincial and local levels provide support, advocacy and training for real estate professionals. The Canadian Real Estate Association (CREA) comprises all provincial real estate associations and local boards throughout the country and is concerned with improving real estate practices across Canada. A key focus of CREA's activities is educating members about federal issues, including AML/CFT issues. There are 11 provincial and territorial real estate associations whose members are local real estate boards within the province or territory. The associations offer educational programs. Many provincial associations also provide real estate licensing courses. Local real estate boards maintain close contact with practising agents and provide detailed information about the local market. Local boards promote standards and make their members aware of publications and training courses available from federal and provincial associations. FINTRAC is responsible for ensuring that real estate agents have implemented the AML/CFT requirements outlined in the PCMLTFA.

Accountants

143. The accounting industry consists of firms and individuals providing a range of accounting services, which include auditing and reviewing financial records, preparing financial statements and accounting reports, developing budgets, designing accounting systems and providing advice on accounting matters. Accountants may also provide other related services, such as bookkeeping and payroll services, tax return preparation, and management consulting and insolvency services. In 2005, almost 22 000 establishments provided accounting services. The largest 20 firms generated 54% of the total operating revenues.

144. There are three main categories of professional accountants in Canada: chartered accountants (CAs), certified general accountants (CGAs) and certified management accountants (CMAs). There

are approximately 60 000 CAs, 51 000 CGAs and 35 000 CMAs. All of these accountants may be required to report to FINTRAC, depending on the types of financial transactions they undertake for clients. Each of the three categories of accountants is represented by a national association: the Canadian Institute of Chartered Accountants, the Certified General Accountants Association of Canada or the Society of Management Accountants of Canada. The associations representing CAs and CGAs are working to form a single body.

145. Provinces are primarily responsible for regulating the professional activities of accountants. Provincial accounting associations within each designation enforce the by-laws, codes of ethics and rules of professional conduct established by each designation to ensure that accountants are protecting the public interest. Provincial associations can discipline members for violations of the standards by imposing sanctions and revoking registration. FINTRAC is responsible for ensuring that accountants have implemented the AML/CFT requirements outlined in the PCMLTFA.

Lawyers and Notaries

Legal Counsel

146. The Federation of Law Societies of Canada is the national coordinating body of the 14 law societies in Canada (one for each of the 10 provinces except Québec, which has two societies and one for each of the three territories), which are responsible for regulating Canada's 88 500 lawyers and Québec's 3 500 notaries in the public interest. The Federation addresses key issues associated with the legal profession in Canada and sponsors two major national continuing legal education programs and intervenes in cases where protection of the public is of national concern.

147. The legal profession in Canada is governed by the laws, rules and regulations of the provincial or territorial law society of which a lawyer is a member. Provincial law societies regulate provincial legal professionals to ensure a competent and ethical bar. Provincial legislation authorises law societies to educate and license lawyers, and to regulate conduct, competence and capacity. Law society by-laws and rules of professional conduct set out the professional and ethical obligations of all members of the profession. Members failing to meet these obligations are subject to the provincial society's complaints and disciplinary process.

148. The Canadian Bar Association is a professional, voluntary organization formed in 1896. It was incorporated by a Special Act of Parliament on April 15, 1921. Today, the association represents some 35 000 lawyers, judges, notaries, law teachers and law students from across Canada. The main functions of the Canadian Bar Association are to act as an advocate and to provide personal and professional development and support.

Notaries

149. Unlike notaries in the province of Québec, who provide legal advice under Québec's civil code, notaries in British Columbia do not provide legal advice and are governed by the British Columbia Notaries Act. They are permitted to undertake only limited activities and they are allowed to hold trust accounts to carry out their duties.

150. It should be noted that notaries in provinces other than Québec and British Columbia are restricted to oath taking and document certification, except in Prince Edward Island where the profession is prohibited by law. These notaries do not conduct any financial transactions and the transfer of property is done exclusively through lawyers in these provinces.

151. British Columbia notaries are a self-governing profession under the Society of Notaries Public in British Columbia. The society enacts rules and by-laws, and regulates and sanctions its members, in a manner similar to that of a provincial law society. The governing legislation assigns the number of notaries that can be active in each of 84 specified provincial districts. The total number of notaries allowed in the province is 332.

Dealers in Precious Metals and Stones (DPMSs)

152. The precious metals and stones[14] industry in Canada consists of many stages and intermediaries. Canadian companies are active in sectors of the industry ranging from mining to retailing. While large firms predominate in the mining and production sector, dealers in precious metals and stones are primarily small firms. Of the more than 4 400 businesses in Canada involved in retailing, wholesaling, repairing and manufacturing jewellery, 90% have 20 or fewer employees. Estimates are that these activities employ 30 000 to 35 000 people, with over 60% working in the retail segment. Membership in industry associations and regulatory bodies is voluntary.

153. Canada has risen to become the world's third largest diamond-producing country by value. The rise in standing is due largely to the recovery of higher-quality stones than previously expected. The RCMP (see its Annual Report 2004) believes that accompanying the increase in diamond production is a corresponding increase in vulnerabilities and potential points of infiltration by organized crime groups. In general, more mines are in operation, more diamond-related companies are formed and a larger secondary diamond industry is developing. Organized crime interest in the diamond industry is monitored by the RCMP-led diamond protection service with the cooperation of the Canadian diamond and diamond exploratory industry.

154. The Canadian Jewellers Association is the dominant industry association, with a membership base that includes the majority of Canadian jewellery wholesalers and retailers. The Jewellers Vigilance Committee of Canada plays a role in preventing money laundering and fraud in the jewellery industry. As a voluntary, not-for-profit association, its mandate includes promoting consumer protection, publishing ethical guidelines, assisting law enforcement agencies and providing information on illegal activities, including fraud, smuggling and money laundering. It is funded in large part by industry contributions.

1.4 Overview of commercial laws and mechanisms governing legal persons and arrangements

Types of legal persons or arrangements recognised in Canada

155. Various types of business structures are available to Canadian entrepreneurs, including sole proprietorships, partnerships, limited or incorporated companies, and cooperatives. While the most appropriate corporate structure depends on factors such as the number of people involved, the type of business, tax issues, liability concerns and financial requirements of the firm, most Canadian businesses are incorporated to create a distinct legal entity separate from their owners. For this reason, most businesses elect to use the corporation as their legal form. There are an estimated 1.5 million corporations in Canada.

156. Incorporation may be done provincially, territorially or federally, giving a company the right to operate under its corporate name in a particular province or territory, or throughout Canada. However, a federally incorporated business must still register in each province in which it does business. A provincially or territorially incorporated corporation must also register in other provinces and territories, and can also conduct business in those other jurisdictions and nationally. While roughly 15% of corporations are incorporated federally, these firms are generally the largest companies and the most active ones, nationally and internationally. The main federal law establishing the legal and regulatory framework for corporations is the Canada Business Corporations Act (CBCA). Most provinces and territories have incorporation systems with measures broadly similar to the requirements in this Act. Cooperatives may also be incorporated either federally or provincially.

157. Most corporations in Canada are structured as private corporations, public corporations, unlimited liability companies or cooperatives, which are defined as follows:

[14] Precious metals and stones refer to high-value commodities used in the jewellery industry, such as gold, platinum, diamonds, tanzanite, emeralds, rubies and sapphires.

- *Private corporations*: One or more people can form a private corporation. A private corporation cannot sell shares or securities to the public. Most small businesses are private companies, and virtually all corporations start out that way.
- *Public corporations*: A public corporation is one that issues securities for public distribution. Besides filing incorporation documents, a public corporation must employ outside auditors and must distribute audited financial statements. It is subject to extensive disclosure and other requirements imposed by provincial securities regulators and corporate law. See section (c), below.
- *Unlimited liability companies*: These are currently permitted in Nova Scotia and Alberta only. They shelter shareholders from liability in most circumstances except on liquidation, when shareholders are liable for the excess of debts over assets.
- *Cooperatives*: These enterprises are jointly owned by the members who use their services. All members of a co-op are equal decision-makers in the cooperative, using a democratic system of one member, one vote. Federal cooperatives may issue shares and, therefore, have both members and shareholders.

158. Although the corporation is the most popular type of legal arrangement for Canadian businesses, the following types of legal persons and arrangements are also available in Canada:

- *Trusts*: A trust encompasses any relationship in which the legal and equitable (beneficial) titles to property are separated. Various types of trusts can be created in Canada. They are discussed in more detail in section 5.2 of this report.
- *Not-for-profits*: A not-for-profit organization is an organization not intending or intended to earn a profit for its members. Both provincial and federal not-for-profit legislation exists. The federal law governing not-for-profit organizations is the Canada Corporations Act, Part II.
- *Sole proprietorships*: A sole proprietorship is an unincorporated business that is owned by one individual and has no legal existence apart from the owner. Its liabilities are the owner's personal liabilities.
- *General partnerships*: A general partnership is the relationship between two or more persons who carry on a trade or business together. Each person contributes money, property, labour or skill, and expects to share in the profits and losses of the business.
- *Limited partnerships*: A limited partnership is an unincorporated business with at least one general partner and one or more limited partners. General partners have unlimited liability and limited partners have limited liability up to the amount of their investment.
- *Limited liability partnerships*: Most Canadian jurisdictions permit the formation of limited liability partnerships (LLPs). Under such a structure, which is generally restricted to eligible professions such as lawyers and accountants, a partner is not personally liable for any debts, obligations or liabilities of the LLP that arise from any negligent act by another partner or by any person under that partner's direct supervision and control. The law does not reduce or limit the liability of the firm. All of the firm's assets and insurance protection remain at risk. In addition, all partners of an LLP remain personally liable for their own actions and for the actions of those they directly supervise and control.

1.5 Overview of strategy to prevent money laundering and terrorist financing

a) AML/CFT Strategies and Priorities

159. Canada has continuously increased the responsibilities, funding and powers of domestic organizations working to identify, disrupt and dismantle money laundering and terrorist financing networks. It has also committed to engaging more actively in international fora.

160. Canada's AML/CFT regime has three primary objectives: detecting and deterring money laundering; preventing terrorist financing; and facilitating the investigation and prosecution of money laundering and terrorist financing offences. To do this, Canada has targeted the three stages of money laundering – placement, layering and integration – in its legislation (this report provides detailed information on this particular point).

Role of the Private Sector

161. As Canada moves forward with new legislation and regulations, some time and effort is invested in comprehensive discussions – with reporting entities in particular, and with the private sector generally – to get views and comments. These views are generally taken into account in rolling out new processes or requirements, or in amending existing ones.

Balance with Privacy Rights

162. The PCMLTFA strikes a careful balance between the privacy rights of Canadians and the needs of law enforcement and national security agencies. The Act upholds the principles outlined in the Canadian Charter of Rights and Freedoms (part of the Canadian Constitution), where Section 8 establishes a constitutional protection against unreasonable search and seizure, and the Privacy Act, which regulates the dissemination of personal information collected by government agencies. As a result, the PCMLTFA contains significant provisions specifically designed to balance the obligation to submit reports with an obligation to strictly control the release of information obtained from submitted reports.

Assessments

163. Canada's AML/CFT regime has undergone three separate, independent evaluations in recent years. Two of the evaluations – one performed by the Office of the Auditor General (OAG[15]) and the other by EKOS Research Associates, Inc., an independent research group – occurred in 2004[16]. The last assessment was a parliamentary review that a committee of the Senate of Canada carried out in the summer of 2006; its interim report was tabled in October 2006 (see Section 6.1 of the report for further information).

Parliamentary Review of the PCMLTFA

164. Section 72 of the PCMLTFA calls for a parliamentary review of the administration and operation of the Act five years after the legislation was passed. Therefore, in the summer of 2006, the Standing Senate Committee on Banking, Trade and Commerce held hearings in which witnesses from both the private sector and federal public service provided comments on Canada's AML/CFT regime and its effectiveness.

165. The Senate Committee tabled a report[17] that highlighted the need for the AML/CFT regime to meet domestic requirements, as well as the importance of meeting international obligations to ensure that the world is "safer and more secure." The report reiterated the importance of an appropriate balance between providing law enforcement and security agencies with the proper information to fight money laundering and terrorist financing, and protecting the privacy rights of Canadians. The review was conducted in the knowledge that the federal government had proposed legislative changes stemming from a consultation paper released by the Department of Finance in June 2005. The

---

15 To ensure accountability and transparency, the Office of the Auditor General (OAG) independently audits federal government departments and agencies, most Crown corporations, and many other federal organizations. The OAG reports publicly up to four times a year to the House of Commons on matters that the Auditor General believes should be brought to the attention of the House. In addition, the OAG testifies before parliamentary committees on the Office's audits.

16 See report at: http://www.fin.gc.ca/activty/pubs/nicml-incba_e.pdf.

17 *Stemming the Flow of Illicit Money: A Priority for Canada*. Parliamentary Review of the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act*. Ottawa: Standing Senate Committee on Banking, Trade and Commerce, October 2006.

recommendations made in the Senate report reinforced the proposed amendments to the PCMLTFA (see below).

Recent Initiatives

166. In June 2005, the federal government issued a consultation paper "*Enhancing Canada's Anti-Money Laundering and Anti-Terrorist Financing Regime*". Extensive consultations took place with financial intermediaries and professional groups following the release of the paper. A description of the key amendments to the PCMLTFA enacted on December 14, 2006 can be found in Section 3 of the report.

167. Further to the above amendments, complementary initiatives are planned (for instance, FINTRAC is working to provide more frequent and more valuable feedback to reporting entities and FINTRAC will issue guidance for new requirements including the reporting of suspicious attempted transactions, the implementation of the risk-based approach and the treatment of politically exposed persons and for new reporting sectors)[18]..

The Institutional Framework for Combating Money Laundering and Terrorist Financing

b) Key Partners in the AML/CFT Regime

168. The current AML/CFT regime is grounded in the "National Initiative to Combat Money Laundering" (NICML), which was established in 2000. The original partners of the NICML included the following.

Department of Finance

169. Along with broad responsibility for regulation of the financial sector, the Minister of Finance has had – since 1999 – responsibility for Canada's AML/CFT regime (originally known as the NICML). However, as noted, a number of key departments and agencies in the federal government are responsible for implementing different aspects of the regime.

170. As the lead organization, the Department of Finance develops AML/CFT policy, including the PCMLTFA and its associated regulations. The department coordinates all activities under the AML/CFT regime, including consultations with stakeholders. It does so in conjunction with other government departments and agencies, provincial governments, the private sector – including industry associations – and non-governmental bodies. The department also participates in strategic domestic and international activities that support the Canadian government's AML/CFT commitments. Specifically, the department leads the Canadian delegation to the FATF, the Caribbean Financial Action Task Force and the Asia/Pacific Group on Money Laundering.

Financial Transactions and Reports Analysis Centre (FINTRAC)

171. FINTRAC, Canada's financial intelligence unit was established in July 2000 under the PCMLTFA to help detect and deter money laundering and terrorist financing activity. FINTRAC is an independent government agency that reports to Parliament through the Minister of Finance. It operates as an independent agency at arm's length from law enforcement, security and other agencies to which it discloses information (see further developments in Section 2.5 of the report).

18 In addition, an AML/CFT advisory committee was created in late 2007, and comprises both public and private sector representatives. This body will work to enhance cooperation and coordination (see Section 6.1 of the report).

Department of Justice

172. A single minister, holding the twin titles of Minister of Justice and Attorney General of Canada, heads the Department of Justice. Criminal law, as a statute of national jurisdiction exclusively under the constitutionally legislative authority of Canada, includes criminal offences and criminal procedure. Authority to develop that law and procedure is given to the minister of justice. The minister is responsible for the Criminal Code of Canada and the development of criminal offences, as well as all laws on criminal procedure. The minister is responsible for the Mutual Legal Assistance in Criminal Matters Act and the Extradition Act.

Public Prosecution Service of Canada (PPSC)

173. The PPSC is a federal government organization, created on December 12, 2006, pursuant to the *Director of Public Prosecutions Act*. The PPSC fulfills the responsibilities of the Attorney General of Canada in the discharge of his criminal law mandate by prosecuting criminal offences under federal jurisdiction and by contributing to strengthening the criminal justice system. The PPSC is an independent organization, reporting to Parliament through the Attorney General of Canada.

Public Safety and Emergency Preparedness Canada (PSEPC)

174. PSEPC is responsible for providing support to the minister of public safety on all matters of public safety and national security, including money laundering and terrorist financing. PSEPC support is multi-dimensional and touches on many aspects of Canada's AML/CFT regime. PSEPC provides the minister with policy development and advice on AML/CFT policies and programs. In addition, PSEPC also works with other regime partners – the RCMP, CSIS and CBSA – that are accountable to the minister on issues of horizontal or mutual interest. PSEPC chairs the Interdepartmental Working Group on Terrorist Listings, in support of the minister's statutory responsibilities to recommend entities to be listed under the Criminal Code.

175. The Minister of Public Safety, with the Minister of Revenue, is also responsible for a critical aspect of Canada's AML/CFT regime under the Charities Registration (Security Information) Act (CRSIA) to prevent the use of charities for terrorist financing.

Canada Revenue Agency (CRA)

176. One of the CRA's responsibilities is to ensure that each person pays the taxes associated with all of his or her income and activities. If FINTRAC discloses information suspected of being relevant to the investigation or prosecution of a money laundering offence or terrorist activity financing offence to law enforcement, and also determines that the information is relevant to an offence of evading or attempting to evade taxes or duties under an Act of Parliament, it will disclose the same information to the CRA. The information received from FINTRAC may lead the CRA to initiate a new enforcement action or serve as additional information in support of an ongoing enforcement action.

177. The CRA's mandate to administer the Income Tax Act in respect of registered charities gives it a responsibility to ensure that the tax benefits reserved for Canada's charities are not used to provide terrorist financing in the guise of charity. The enactment of the CRSIA as Part V of the Anti-Terrorism Act redefined the CRA's role and the importance of protecting the integrity of Canada's registration system for charities.

Canadian Security Intelligence Service (CSIS)

178. CSIS has a mandate to collect, analyze, and retain information or intelligence on activities that may on reasonable grounds be suspected of constituting threats to the security of Canada. CSIS is the Government of Canada's principal advisor on national security. CSIS's role in the regime is to receive FINTRAC disclosures regarding suspected threats to the security of Canada and to gather intelligence,

which may be passed to the RCMP for potential criminal proceedings. CSIS also provides voluntary information reports to FINTRAC.

Royal Canadian Mounted Police (RCMP)

179. As the national police force – and as the provincial or local police force, in many jurisdictions across Canada – the RCMP plays a fundamental role in Canada's AML/CFT regime. The RCMP investigates money laundering and terrorist financing cases and acts as a liaison in exchanging criminal intelligence with international police forces. RCMP liaison officers around the globe assist Canada in pursuing AML/CFT cases.

180. In response to the September 11, 2001 terrorist attacks on the U.S., the RCMP Financial Intelligence Branch was created to address the issue of terrorist fundraising. This intelligence/investigative body was established to support national security efforts to identify financial intelligence and enforcement opportunities related to terrorist financing, as well as to provide direction and support to field units. An Internet investigation team was established as part of the branch to investigate terrorist fundraising on the Internet.

181. Finally, the RCMP plays a significant training and awareness-raising role among AML/CFT partners and the private sector, and in international fora. Indeed, the RCMP has provided direct technical assistance and training to police forces in developing countries to help them conduct AML and terrorist financing investigations and enhance their investigative techniques.

Canada Border Services Agency (CBSA)

182. The PCMLTFA requires that all large amounts of currency and monetary instruments imported or exported to or from Canada, including those transported by mail, be reported to a border services officer (BSO). In addition, BSOs now have the responsibility to enforce the physical cross-border reporting initiative, which includes the authority to examine baggage and conveyances, and to question and search individuals for unreported or falsely reported currency and monetary instruments. CBSA also plays a key role in denying admission to Canadian territory to non-citizens who pose security threats to Canada.

Office of the Superintendent of Financial Institutions (OSFI)

183. OSFI regulates and supervises federally regulated financial institutions, which comprise banks, federally regulated insurance companies, cooperative credit associations, and federally regulated trust and loan companies. It administers financial institution governing statutes (the Bank Act, the Insurance Companies Act, the Trust and Loan Companies Act, and the Cooperative Credit Associations Act). OSFI issues guidance to federally regulated financial institutions, as well as warning notices regarding entities that it believes may be of concern to the business community and the public.

Other Participants in AML/CFT Efforts

184. In addition to the nine key partners in the AML/CFT regime discussed above, other departments also participate in the fight against money laundering and terrorist financing.

Department of Foreign Affairs and International Trade

185. The Department of Foreign Affairs and International Trade (DFAIT) has responsibility for international elements of Canada's efforts to address money laundering and terrorist financing. The Minister of Foreign Affairs is responsible for the designation of entities and individuals in Canada associated with terrorist activities listed by the United Nations 1267 Sanctions Committee or under Resolution 1373 of the United Nations Security Council. This designation effectively freezes their

assets and prohibits fundraising on their behalf. DFAIT is also the primary interlocutor and negotiator for Canada in terms of international conventions and treaties that address money laundering, terrorist financing and other related public safety issues, such as bribery, corruption or illicit drugs.

Industry Canada

186. The Minister of Industry is responsible for the Canada Business Corporations Act, under which companies can federally incorporate their business with Industry Canada. When a business does so, the department collects information about the enterprise, including the business name and address, and information about the directors.

Office of the Privacy Commissioner of Canada

187. The Office of the Privacy Commissioner plays an important role in ensuring that the necessary safeguards protecting privacy are upheld. The Privacy Commissioner is an officer of Parliament who reports directly to the House of Commons and the Senate and who regularly provides views on Canada's AML/CFT regime. The Privacy Commissioner has the ability to audit FINTRAC and financial institutions etc. to ensure privacy laws are respected.

Public Works and Government Services Canada, Seized Property Management Directorate

188. The Seized Property Management Directorate is responsible for the management and disposition of assets – including movable property, real estate, cash and securities – that have been seized or forfeited for illicit drug trafficking and money laundering offences. It also acts as a holding facility for currency and monetary instrument seizures.

Provincial Bodies

189. A number of provincial department and agencies, regulators and self-regulatory organizations have a role to play in the fight against money laundering and terrorist financing. These organizations include the following (further information is provided in Sections 2, 3 and 4 of the report):

- Provincial, territorial and municipal law enforcement agencies, such as the Ontario Provincial Police, la Sûreté du Québec and city police forces, who participate as part of various IPOC units.
- Provincial Crown prosecutors and courts.
- Provincial and territorial financial sector regulators, such as the Financial Services Commission of Ontario, the Ontario Securities Commission, l'Autorité des marchés financiers du Québec and the British Columbia Gaming Commission.
- Self-regulatory organizations, such as the Law Society of Upper Canada, the Investment Dealers Association and Canadian Institute of Chartered Accountants.

c) Approach concerning risk (see Section 3.1 of the report)

Application of AML/CFT obligations to certain sectors

190. In Canada, certain financial institutions as defined by the FATF Recommendations are not covered by the AML/CFT regime since Canada considers that these entities pose little or no threat of money laundering/terrorist financing. Canada's risk based approach is centred around the principle that financials sectors are brought into the AML/CFT regime if there is a proven risk of ML/TF. This differs from the FATF approach to risk as defined in the Methodology where a list of activities and operations must be covered by the AML/CFT regime unless there is a proven low risk of ML or TF (see Section 3.1 of the report for further analysis).

Risk-based approach taken by financial institutions

191. The government takes risks into account at various levels for regulatory purposes. For example, the PCMLTFA requires reporting entities to file reports with FINTRAC for cash transactions of CAD10 000 or more. However, a specific risk assessment identified legitimate cash-intensive businesses, such as big box stores and grocery store chains, whose large cash transactions would not have to be reported to FINTRAC. Further, reporting entities are not required to identify clients that are publicly listed companies in Canada, since such companies already have to meet comprehensive disclosure and other filing requirements set by provincial securities regulators.

Use of a Risk-Based Approach in Supervision of Compliance by Competent Authorities

192. The competent authorities use a risk-based approach when supervising reporting entities for compliance with the legislation. FINTRAC and OSFI have taken a risk-based approach in developing and implementing their supervisory programs (see Section 3.1 of the report).

d) Progress since the last mutual evaluation or assessment

193. Since the last mutual evaluation report (1997), Canada has implemented a large number of developments in its AML/CFT regime both in terms of statutory amendments and structural changes. The most high-profile development was the enactment of the Proceeds of Crime (Money Laundering) and Terrorist Financing Act. This report discusses these changes in detail.

2 LEGAL SYSTEM AND RELATED INSTITUTIONAL MEASURES

Laws and Regulations

2.1 Criminalisation of Money Laundering (R.1 & R.2)

2.1.1 Description and Analysis

Recommendation 1

194. In Canada, all criminal offences must be set out in national law, as passed by the Parliament of Canada. Most criminal offences are found in the Criminal Code[19]. However other federal laws, including a number of profit motivated criminal offences (for example drug offences) are established in other federal laws, such as the Controlled Drugs and Substances Act[20].

195. *Criminalisation of ML on the basis of the UN Conventions*. The Vienna and Palermo conventions require countries to establish as a criminal offense the following intentional acts: conversion or transfer of proceeds; concealment or disguise of the true nature, source, location, disposition, movement or ownership of or rights with respect to proceeds; and the acquisition, possession or use of proceeds (Article 3(1)(b)(i)-(ii) of Vienna; Article 6(1)(a)(i)-(ii) of Palermo). This obligation is subject to the fundamental/constitutional principles and basic concepts of the country's legal system (Article 2(1), Vienna convention; Article 6(1), Palermo convention).

196. In Canada, the money laundering offence, which can be found under section 462.31 of the Criminal Code (CC) is part of a broad proceeds of crime regime designed to cover all obligations in the 1988 Vienna Convention and the 2000 Palermo Convention to criminalize the concealment or laundering of proceeds of crime and the possession of such proceeds or criminal instrumentalities. Section 462.31 encompasses acts of using, transferring the possession of, sending or delivering to any person or place, transporting, transmitting, altering, disposing of or otherwise dealings with, in any manner and by any means, any property or any proceeds of any property. The prohibited activity must be undertaken with an intent to conceal or convert that property or those proceeds, and knowing or believing that all or a part of that property or of those proceeds was obtained or derived directly or

[19] R.S.C. , 1985, c. C-46 as amended-See http://laws.justice.gc.ca/en/C-46/index.html.

[20] S.C. 1996, Chap. 19, see http://laws.justice.gc.ca/en/c-38.8/229593.html.

indirectly as a result of the commission of a designated offence. A designated offence means *(a) any offence that may be prosecuted as an indictable offence under the Criminal Code or any other Act of the Parliament, other than an indictable offence prescribed by regulation or (b) a conspiracy or an attempt to commit, being an accessory after the fact in relation to, or any counselling in relation to, an offence referred to in paragraph a)* (see s. 462.3 (1) CC). The possession of proceeds of crime is covered in section 354(1) of the Criminal Code. That section makes it an offence to knowingly possess money or property derived directly or indirectly from any indictable Canadian criminal offence or any foreign offence, that had it been committed in Canada would have been an indictable offence in Canada. There is also an offence covering the importation of property derived from foreign crimes into Canada (s.357).

197. The elements of Canada's primary money laundering offence are for the most part criminalised in line with all of the requirements of the Vienna and Palermo Conventions. However, in one aspect the Canadian money laundering offence in Section 462.31 requires an additional mental element that is not required under either Convention. Namely, Section 462.31 requires that the person handling property or proceeds of property has the intent to conceal or convert same. ("Every one commits an offence who uses, transfers the possession of, sends or delivers to any person or place, transports, transmits, alters, disposes of or otherwise deals with, in any manner and by any means, any property or any proceeds of any property ***with intent to conceal or convert that property or those proceeds***, knowing or believing that all or a part of that property or of those proceeds was obtained or derived directly or indirectly as a result of (*a*) the commission in Canada of a designated offence; or (*b*) an act or omission anywhere that, if it had occurred in Canada, would have constituted a designated offence" (emphasis supplied).

198. The Conventions require the conversion or transfer of property to be an offence where the defendant knows that the property involved is the proceeds of crime and does so for one of the following two purposes: (1) concealing or disguising its illicit origin; *or* (2) for the purpose of helping any person who is involved in the commission of the predicate offence to evade the legal consequences of his or her action (Palermo, Article 6(1)(a)(i) and Vienna, Article 3(1)(b)(i)). However, section 461.31 sets out only one purpose element (for the purpose of concealing or disguising its illicit origin) instead of the two alternatives required by the Convention. Canada notes that in the alternative the relevant conduct may be covered by s.354, though the assessment team believes that will not be the case for many of the factual scenarios criminalised by s.462.31. This is a minor technical deficiency that could inhibit some prosecutions.

199. *Property that represents the proceeds of crime*. As indicated above, the money laundering offence extends to property or proceeds of property that was obtained or derived directly or indirectly as a result of the commission of a designated offence. The concept of "property" is broadly defined in section 2 of the Criminal Code and meets the FATF requirements. Under this section, property includes "*(a) real and personal property of every description and deeds and instruments relating to or evidencing the title or right to property, or giving a right to recover or receive money or goods, and (b) property originally in the possession or under the control of any person, and any property into or for which it has been converted or exchanged and anything acquired at any time by the conversion or exchange"*.

200. The Criminal Code includes a wide definition of possession in subsection 4(3). It provides that a person possesses anything when he has it in his personal possession or knowingly (i) has it in the actual possession or custody of another person, or (ii) has it in any place, whether or not that place belongs to or is occupied by him, for the use or benefit of himself or of another person. Where one of two or more persons has anything in his custody or possession, with the knowledge and consent of the rest, it shall be deemed to be in the custody and possession of each and all of them.

201. It is not necessary that a person is convicted of a predicate offence when proving that property is the proceeds of crime, only proof that the property emanates from a criminal acquisition is sufficient (beyond a reasonable doubt is the standard of proof). This principle has been confirmed by case law.

Further clarity is provided in the forfeiture provision in subsection 462.37(2) CC: *(2) where the evidence does not establish to the satisfaction of the court that the designated offence of which the offender is convicted, or discharged under section 730, was committed in relation to property in respect of which an order of forfeiture would otherwise be made under subsection (1) but the court is satisfied, beyond a reasonable doubt, that that property is proceeds of crime, the court may make an order of forfeiture under subsection (1) in relation to that property.* The targeted property is subject to forfeiture without a conviction for the predicate offence.

202. *Predicate offences for ML*. Canada essentially applies an all crime approach to its money laundering scheme by including all indictable offences *i.e.* those offences subject to imprisonment for more than six months, as designated (or predicate) offences (see the definition above) with some exceptions. Summary conviction offences as those with a fine of not more than two thousand dollars or imprisonment for up to six months or to both. For example, the financing of terrorism is an indictable offence subject to up to 10 years in prison.

203. In addition, the Canadian offence classification system includes a hybrid offence classification approach to some offences. That approach provides that the offence may be treated as a less serious summary conviction offence or a more serious indictable offence at the discretion of the prosecutor. For example, theft can be an indictable offence with varying jail terms or a summary conviction offence depending on the amount stolen. Section 34 of the Interpretation Act (that provides interpretation of legislation) applies to hybrid offences, providing: "*(1) where an enactment creates an offence, (a) the offence is deemed to be an indictable offence if the enactment provides that the offender may be prosecuted for the offence by indictment; (b) the offence is deemed to be one for which the offender is punishable on summary conviction if there is nothing in the context to indicate that the offence is an indictable offence; and (c) if the offence is one for which the offender may be prosecuted by indictment or for which the offender is punishable on summary conviction, no person shall be considered to have been convicted of an indictable offence by reason only of having been convicted of the offence on summary conviction"*. As a result, any hybrid offence is treated as an indictable offence until the prosecutor makes an election.

204. The offence of possession of property derived from a crime under Section 354 and Section 357 are essential elements in Canada's broader money laundering and proceeds of crime approach. The possession offence covers the possession of any property or thing, or any proceeds of any property or thing, where there is knowledge that all or any part of the property, thing, or of the proceeds was obtained directly or indirectly from: (a) the commission in Canada of an offence punishable by indictment; or (b) an act or omission anywhere that, if it had occurred in Canada, would have constituted an offence punishable by indictment. Again, the predicate offences for the offence of possession of property derived from crime cover all serious (indictable) offences in Canada. There is no excluded predicate offence for the offence of possession of property derived from crime. This offence, which is broad in scope, also covers factual circumstances that amount to possession of stolen property offences *e.g.* stolen motor vehicles, or simple cases of persons caught in possession of small quantities of drugs and cash. While the assessors were advised that a large majority of s.354 cases dealt with such conduct, a statistical breakdown of s. 354 offences prosecuted by the Attorney General of Canada indicated that none of those offences were cases where the particular charge was receiving of stolen property.

205. There is also a separate criminal offence, which is a designated offence for the purposes of the definition of proceeds of crime, in section 357 of the Criminal Code. Section 357 creates an offence where importing anything into Canada that a person obtained outside Canada by an act that, if it had been committed in Canada, would have been the offence of theft or an offence under Section 342 (theft, forgery, etc., of credit card) or 354 (possession of property obtained by crime). This is an indictable offence in Canada.

206. As mentioned earlier, the money laundering offence specifies that the predicate offence must be a designated offence. The definition of designated offences, in section 462.3 of the Criminal Code,

provides that some indictable offences, prescribed by regulation, will not be designated offences for the purposes of money laundering[21]. The following provides the list of excluded offences:

The indictable offences under the following Acts are excluded from the definition of "designated offence" in subsection 462.3(1) of the Criminal Code:

(a) Budget Implementation Act, 2000.
(b) Canada Agricultural Products Act.
(c) Copyright Act.
(d) Excise Act, except for the indictable offences under subsections 233(1) and 240(1).
(e) Excise Tax Act.
(f) Feeds Act.
(g) Fertilizers Act.
(h) Foreign Publishers Advertising Services Act.
(i) Health of Animals Act.
(j) Income Tax Act.
(k) Meat Inspection Act.
(l) Nuclear Safety and Control Act, except for the indictable offence under section 50 (offence to possess certain nuclear substances, etc.
(m) Plant Protection Act.
(n) Seeds Act.

207. Indictable offences in these 14 Acts have been excluded from the scope of relevant indictable offences for the purposes of Section 462.31 ML offences as these offences are penalized through other Acts. However, if charges were instituted under other federal laws, including the Criminal Code, and they were prosecuted by indictment, they would fall within the money laundering offence since all other indictable offences are covered by the money laundering offence[22]. The absence of provisions on copyright offences in the Criminal Code means that copyright related offences are not predicate offences for Section 462.31 ML, although offences involving trademarks and trade descriptions (Sections 406 to 410, Criminal Code) are predicate offences for Section 462.31 ML. Canada takes the position that Section 354 criminalizes possession of the proceeds of copyright offences. However, Section 354 covers only one portion of the three types of ML offences that Canada should criminalize under the relevant Conventions, and thus gaps still exist as Section 354 does not cover all varieties of ML offences contemplated by this Recommendation. Although this constitutes a minor technical failure and is a relatively small gap in the regime, this deficiency should be addressed by the Canadian authorities. To avoid any potential gaps of this sort, the assessors suggest the removal of the list of excluded offences and recommend that Canada include all indictable offences (including those prescribed by regulations) as predicate offences for Section 462.31 ML.

208. The scope of the offence category lists, as set out in the FATF 40 Recommendation's Glossary Description of Designated Categories of Offences, are covered as money laundering offences in the Criminal Code and offences in specific federal statutes. The FATF categories are cross-referenced to some of the Criminal Code or other indictable offences, in relevant federal laws, as follows:

- Participation in an organised criminal group and racketeering- *Criminal Code sections 467.11, 467.12 & 467.1.*
- Terrorism, including terrorist financing- *Criminal Code sections 83.02, 83.03, 83.94 83.12 and 83.18 to 83.231.*

[21] Regulations Excluding Certain Indictable Offences from the Definition of "Designated Offence". SOR/2002-63 see- http://canadagazette.gc.ca/partII/2002/20020213/html/sor63-e.html.

[22] Canadian provinces and territories also enact laws that contain provincial offence provisions. No province may enact a criminal law, with the result that none of the provincial offences are offences for the purposes of money laundering or possession of property derived from crime provisions in the Criminal Code.

- Trafficking in human beings and migrant smuggling- *Criminal Code section 279.01 and sections 117 & 118 of the Immigration and Refugee Protection Act.*
- Sexual exploitation, including sexual exploitation of children- *Criminal Code section 212.*
- Illicit trafficking in narcotic drugs and psychotropic substances -*Sections 5 to 7 of the Controlled Drugs and Substances Act.*
- Illicit arms trafficking- *Criminal Code sections 99 to 108.*
- Illicit trafficking in stolen and other goods- *Criminal Code sections 354 & 462.31.*
- Corruption and bribery- *Criminal Code sections 119 to 125; 426 and Section 3 of the Corruption of Foreign Public Officials Act.*
- Fraud- *Criminal Code sections 341, 342(3), 371, 374 to 376, 378, 380, 381, 385 to 394 and 396.*
- Counterfeiting currency- *Criminal Code sections 449 to 460.*
- Counterfeiting and piracy of products- *Criminal Code sections 406 to 411.*
- Environmental crime- *Sections 272 to 274 and 276 of the Canadian Environmental Protection Act, 1999.*
- Murder, grievous bodily injury- *Criminal Code sections 229 to 240 and 264.1 to 273.*
- Kidnapping, illegal restraint and hostage-taking- *Criminal Code sections 279 to 283.*
- Robbery or theft- *Criminal Code sections 343 and 322 to 334.*
- Smuggling-*Sections 153 to 160 of the Customs Act.*
- Extortion- *Criminal Code section 346.*
- Forgery- *Criminal Code sections 57, 342 & 342.1 369 to 378.*
- Piracy- *Criminal Code sections 74 & 75.*
- Insider trading and market manipulation- *Criminal Code section 382.1.*

209. *Extraterritorial predicate offences*. Jurisdiction to prosecute the money laundering and possession of property offences under Canadian law is established so long as the foreign conduct would have been an offence had it occurred in Canada (and whether or not the offence constitutes an offence in the foreign country). This explicit extension of jurisdiction is permitted under the general rule found in subsection 6(2) of the Criminal Code, which states that no person can be convicted of an offence committed outside Canada unless federal law explicitly extends jurisdiction to do so.

210. As is the case with money laundering, Canadian courts may assert criminal jurisdiction over acts taking place in another state if they are connected to other acts that take place in Canada in furtherance of criminal behaviour, or if the acts in the other state have some injurious consequence within Canada. For example, as defined in subsection 4(3) of the Criminal Code, possession of property derived from crime or the laundering of such property give rise to jurisdiction in Canada.

211. The leading Supreme Court of Canada case on jurisdiction is R. v. Libman, [1985] 2 S.C.R. 178, in which the Court held that "all that is necessary to make an offence subject to the jurisdiction of our courts is that a significant portion of the activities constituting that offence took place in Canada. As it is put by modern academics, it is sufficient that there be a "real and substantial link" between an offence and this country, a test well-known in public and private international law. (par. 74)". The Court stated that Canada "should not be indifferent to the protection of the public in other countries" (par.77).

212. The determination of what a "significant portion" or a "real and substantial link" will depend on the particular fact situation, but does not depend on an extensive physical connection between the offence and Canada[23]. In summary, if the crime giving rise to the possession of property occurred outside of Canada but the possession element of the offence occurs in Canada, the crime could be prosecuted in Canada.

[23] See Canada (Human Rights Commission) v. Canadian Liberty Net, [1988] 1 S.C.R. 626; United States of America v. Lépine, [1994] 1 S.C.R. 286 and R v. Hammerbeck (1993), R.F.L. (3d) 265, 26 B.C.C.A.

213. *Self-money laundering*. In Canada, an individual who launders their own proceeds commits a money laundering offence given the extensive definition of "person" and "property" in section 2 of the Criminal Code. Canadian case law supports this position[24].

214. *Ancillary offences*. Canada's Criminal Code includes ancillary or inchoate criminal offences. Section 21 CC criminalizes being party, which includes aiding and abetting, to the offence of money laundering[25]. Section 22 CC provides for a general counselling offence[26]. Section 23 CC provides for accessory after the fact. The *actus reus* and *mens rea* of an attempt are set out in Section 24(1) CC that creates liability for attempting to commit an offence regardless of whether it was, in fact, possible to commit the offence. It is a question of law whether an act or omission by a person who has the intent to commit an offence is mere preparation or an attempt to commit the offence. To illustrate how the courts normally draw the line between mere preparation and attempt, see the following two cases: R. v. Deutsch, [1986] 2 S.C.R. 2 and R. v. Sorrell and Bondett (1978), 41 C.C.C. (2d) 9.

215. Section 465 CC contains the relevant provisions on conspiracy. Section 465(1)(c) states that everyone who conspires with anyone to commit an indictable offence is guilty of an indictable offence and liable to the same punishment as that to which an accused who is guilty of the offence would, on conviction, be liable. Section 465(3) makes it an offence to conspire in Canada to do anything abroad referred to in section 465(1), if it is an offence under the laws of that place. Additionally, it is an offence under section 465(4) to conspire outside Canada to do anything in Canada referred to in 465(1). Canada explains that it is not a defence to a charge of conspiracy that an accused, having agreed to carry out the unlawful act with the intention to carry out the common design, later withdraws from the conspiracy, as the offence is complete upon the making of the agreement. Further to subsection 34(2) of the Interpretation Act, section 465 of the Criminal Code (conspiracy) would apply to the offences in the Act.

216. Section 463 CC sets out the sentence for anyone convicted of the inchoate offence. Section 464 provides for the offence of counselling offences that are not committed. Finally, to clarify any possible ambiguity in respect to the concept of designated offences for money laundering, Section 462.3 (b) CC refers to inchoate offences in the definition of "designated offences". Therefore, every indictable offence, including ancillary offences, is covered by the money laundering offence, unless they have been excluded by regulation as described above.

217. *Additional elements*. As discussed above, Canada's money laundering and possession of property offences establish jurisdiction so long as the foreign conduct would have been an offence if it had occurred in Canada. Whether or not the offence constitutes an offence in the foreign country is not taken into account. More specifically, the concept of "proceeds of crime" establishes the parameters of

---

[24] See R. v. Falahatchia (1995) 99 C.C.C. (3d) 420 (On C.A.); R. v. Cazzetta [2003] J.Q. N. 43 (Que C.A.).

[25] Section 21 (1) CC: "Everyone is a party to an offence who (a) actually commits it; (b) does or omits to do anything for the purpose of aiding any person to commit it; or (c) abets any person in committing it. (2) Where two or more persons form an intention in common to carry out an unlawful offence and to assist each other therein and any one of them, in carrying out the common purpose, commits an offence, each of them who knew or ought to have known that the commission of the offence would be a probable consequence of carrying out the common purpose is a party to that offence". For case law, see R. V. Fraser (1984), 13 C.C.C. (3d) 292 (B.C.C.A.) or R. V. Dunlop and Sylvester [1979] 2 S.C.R. 881 or R. V. Thatcher [1987] 1 S.C.R. 652.

[26] Section 22 CC: 22. (1) Where a person counsels another person to be a party to an offence and that other person is afterwards a party to that offence, the person who counselled is a party to that offence, notwithstanding that the offence was committed in a way different from that which was counselled. (2) Every one who counsels another person to be a party to an offence is a party to every offence that the other commits in consequence of the counselling that the person who counselled knew or ought to have known was likely to be committed in consequence of the counselling.

the nature of the property that may be relevant to a money laundering offence[27]. See also Sections 462.31 and 354(1) and Section 357 CC as described above).

Recommendation 2

218. *Natural persons that knowingly engage in ML activities*. Authority to prosecute a natural person has always existed in Canada. The criminal offences of money laundering and possession of property derived from crime clarify any ambiguity. They provide that the offence covers activity undertaken by "everyone". The Criminal Code defines "everyone" in section 2 in an expansive fashion to include an "organization". An "organization" is itself defined to mean a public body, body corporate, society, company, firm, partnership, trade union, municipality, or an association of persons that is created for a common purpose and has an operational structure. The concept includes natural and legal persons.

219. As regards knowledge, or intent, it is an essential element in all criminal offences, including the money laundering and possession of property derived from crime offences. Since these are criminal offences, the onus to prove the knowledge element beyond a reasonable doubt rests on the prosecution (known as the Crown in Canada). However, in Canada the prosecutor does not have to establish actual knowledge. A prosecutor can establish the required knowledge element by establishing that the accused was wilfully blind or reckless. In R. v. Sansregret, [1985] 1 S.C.R. 570, the Supreme Court held that recklessness and wilful blindness can be used to establish the criminal law requirement for intention. In addition, for the money laundering offence in Section 462.31 of the Criminal Code, further clarification was provided by an amendment adding the words "or believing" to the knowledge element in that offence[28].

220. *Inference from objective factual circumstances*. Canadian prosecutors may rely upon both direct and circumstantial evidence to prove their case in any criminal prosecution. The authority to use such evidence was recently canvassed by the Manitoba Court of Appeal in R. v. Jenner (2005), 195 C.C.C. (3d) 364 at paragraph 20: *"…It was contended that proof of knowledge as to the character of the substance would place upon the Crown a difficult, if not impossible, burden. I cannot agree with the contention. Proof of knowledge is no more difficult than the proof of intent in any criminal prosecution. Knowledge, like intent, is a state of mind. It cannot, generally speaking, be proved as a fact but can only be inferred from facts which are proved. A jury, on properly established facts, should experience no more difficulty in finding knowledge than it does in finding intent*".

221. The Ontario Court of Appeal, in R. v. Aiello (1978), 38 C.C.C. (2d) 485 affirmed 46 C.C.C. (2d) 128n (S.C.C.), opined, at page 488, on the same point: *"…The trial Judge in our view should have further directed the jury that it was not necessary for the prosecution to prove the required knowledge by direct evidence, but that it could be inferred from the surrounding circumstances, such as, for example, the finding of the drug on the accused person in his trouser pant leg, his evidence that he figured that it must be a drug, the circumstances in which, and the place where he had picked up the package*".

222. The ability to rely on circumstantial evidence in a ML case is more specifically enhanced by Section 462.39 CC, which provides that: "*…the court may infer that property was obtained or derived as a result of the commission of a designated offence where evidence establishes that the value, after the commission of that offence, of all the property of the person alleged to have committed the offence exceeds the value of all the property of that person before the commission of that offence and the court*

---

[27] Section 462.3 CC: "*in this Part, "proceeds of crime" means any property, benefit or advantage, within or outside Canada, obtained or derived directly or indirectly as a result of (a) the commission in Canada of a designated offence, or (b) an act or omission anywhere that, if it had occurred in Canada, would have constituted a designated offence*".

[28] An amendment in May 1997 added "belief" to the money laundering offence, so as to overcome the problem that "sting" operations could not be conducted by the police as the use of government money as "proceeds" meant that no offence was committed.

is satisfied that the income of that person from sources unrelated to designated offences committed by that person cannot reasonably account for such an increase in value".

223. *Criminal liability for legal persons*. Authority to prosecute a legal person exists in Canada. As indicated above, the scope of any relevant criminal offence is found in the specific money laundering and possession of property derived from crime offences. These offences refer to "everyone" and the Criminal Code defines "everyone" to include an "organization". Section 2 defines "organization" expansively to mean a public body, a body corporate, a society, a company, a firm, a partnership, a trade union or an unincorporated association.

224. Following recent modifications to the Criminal Code to deal with legal persons, corporations may be held criminally liable: (a) as a result of the actions of those who oversee day-to-day operations but who may not be directors or executives; (b) when officers with executive or operational authority intentionally commit, or direct employees to commit, crimes to benefit the organization; (c) when officers with executive or operational authority become aware of offences being committed by other employees but do not take action to stop them; and (d) when the actions of those with authority and other employees, taken as a whole, demonstrate a lack of care that constitutes criminal negligence.

225. Fines imposed against corporations that are found criminally liable can range from up to CAD100 000 for a prosecution on summary conviction, a less serious offence, to no set limit for indictable or more serious offences. The Criminal Code was also amended with respect to sentencing and the concept of corporate probation[29].

226. *Sanctions for ML*. Canada's possession of property derived from crime (Subsection 354(1) CC carries a maximum penalty of 10 years imprisonment if the property involved is a "testamentary instrument," or exceeds CAD5 000 in value (otherwise it is only a 2 year maximum), as does the separate offence of bringing into Canada property obtained by crime (Section 357). The Section 462.31 ML offence also carries a maximum penalty of 10 years, regardless of the value of the property involved. A person convicted of an attempt to commit such a crime or as an accessory after the fact may be subjected to a penalty of one-half of that available for actual committing the underlying offence (Section 463). If the charge is for counselling an offence that is not committed, the maximum penalty is the same as if the person was convicted of an attempt, namely one-half of that available for actual committing the underlying offence (Section 464). If the person is convicted of a conspiracy, the maximum penalty is five years imprisonment (subparagraph 465(1)(b)(ii)). It should also be noted that the proceeds of crime are forfeitable. If the property that would otherwise be forfeitable is no longer available for forfeiture, Section 462.37 provides for a fine in lieu of forfeiture alternative with consecutive jail time in default ranging from a maximum of six months to ten years depending on the amount of the fine.

227. All of the referenced terms of incarceration can apply to a natural person, but it is not possible to incarcerate a legal person. As a result, the Criminal Code deals with this reality in Sections 718.21 and 735(1) and imposes an additional fine ranging from a maximum of CAD100 000 for summary conviction offences to an amount determined by the court for the more serious indictable offences.

228. Limited information was given to the assessment team on ML sentencing (a sample of 28 ML sentences from 1993 to 2006 was provided and no example was given of a Section 462.31 ML sentence of a legal person). In the examples that were provided, penalties for Section 462.31 ML ranged from 6 months (for CAD29 000 laundered) to 10 years (conviction for laundering proceeds, conspiracy to launder, drug trafficking and CAD30 million laundered). No comprehensive statistics are available on Section 462.31 ML sentencing, nor on possession of proceeds cases and the data provided is a snap shot of cases that cover a long period of time. A lack of statistics on sanctions imposed on natural and legal persons means that the effectiveness of sanctions for ML cannot be properly assessed.

[29] See Section 718.21CC which sets out sentencing factors that the court must consider while sections 721, 730, 732.1, 734 and 735 updated other sentencing considerations for convicted corporations.

Statistics (Recommendation 32)

229. The following table provides the number of charges pursuant to Section 462(31) CC (ML offence) and the outcomes of the trials.

Year	2003/2004	2004/2005	2005/2006	**Total**
Charges laid down pursuant to S.462(31) CC	220	292	211	**723**
Guilty pursuant to S.462(31) CC	5	6	10	**21**
Committed for trial (ongoing case) pursuant to 462(31) CC	8	6	3	**17**

230. There is no figure on the number of Section 462.31 ML cases that are either self-money laundering or third-party money laundering.

231. The following table provides the number of charges pursuant to Section 354 (possession of property obtained by crime) and the outcomes of the trials. The assessment team was not provided with information to indicate how many of these cases were more in the nature of simple possession of stolen goods type offences as compared to possession of the proceeds of serious offences *i.e.* what is considered as traditional money laundering. Nor was data available on how many offences involved more than CCAD5 000 in assets. The team was advised that the data in the s. 354 table includes a large majority of minor possession offences involving either minor cases of possession of small quantities of drugs and cash or receipt of stolen goods. Canada analysed a sample of approximately 1 000 cases which showed a large majority were linked to funds derived from drug offences and a much smaller number were linked to thefts.

Year	2003/2004	2004/2005	2005/2006	**Total**
Charges laid down pursuant to S.354 CC	24 434	24 410	16 971	**65 815**
Guilty pursuant to S.354 CC	3 962	4 025	2 163	**10 150**
Committed for trial (ongoing case) pursuant to S.354 CC	587	579	249	**1 415**

232. The following table provides an overview of the number of charges laid by the RCMP's IPOC units in money laundering and possession of proceeds of crime cases. The other category includes weapons related charges, drug related charges, breach of probation and fraud charges, to name a few.

Charge Type	**Files**	**2001**	**2002**	**2003**	**2004**	**2005**	**2006**	**Total**
Possession of POC	Number	28	231	157	78	31	16	**541**
	Percent	52.8%	40.3%	52.3%	17.5%	10.8%	34.9%	**31.7%**
Money laundering	Number	4	319	109	57	97	25	**611**
	Percent	7.6%	55.7%	36.3%	12.8%	33.7%	54.4%	**35.8%**
Other	Number	21	23	34	311	160	5	**554**
	Percent	39.6%	4.0%	11.3%	69.7%	55.6%	10.9%	**32.5%**
TOTAL	Number	**53**	**573**	**300**	**446**	**288**	**46**	**1,706**
	Percent	**100%**	**100%**	**100%**	**100%**	**100%**	**100%**	**100%**

2.1.2 Recommendations and Comments

233. The anti-money laundering offences are comprehensive and Canada generally meets the requirements under Recommendations 1 and 2. The primary ML offence set forth in Section 462.31 is broad in its scope, but the assessors recommend that all indictable offences, including those prescribed by regulations, should be predicate offences for ML, since copyright offences are currently not covered by this provision. Conversely, the Section 354 possession of property offence covers property from all indictable offences, and the two offences should thus be consistent in their scope. The Section 462.31 offence is technically inconsistent with the relevant UN Conventions in that it injects an additional specific intent mental element that is not required by those Conventions. Section 462.31 should be rewritten to make clear that the perpetrator need not have the specific intent to conceal (or disguise), but that that instead that only "purpose" or result of the particular transaction must be such. In addition, Canada should craft language that makes sure Section 462.31 covers transfers and conversions that have as their purpose helping any person who is involved in the commission of a predicate offence or offences evade the legal consequences of his or her actions. Alternatively, Canada should consider removing the purpose element from Section 462.31 completely, thus making it consistent with s.354, albeit it broader than the Convention requirements.

234. The assessment team has concerns on whether prosecutions of ML offences have been effectively implemented. A reasonable number of charges are laid for section 462.31 ML offences (723 from 2003 to 2006) in a country where, based on the information made available, money laundering is considered to be a significant criminal problem. However, the number of convictions in that period for that offence is very limited, 21 from 2003 to 2006. In addition there are 17 charges currently committed to trial. This means less than 3% of Section 462.31 charges laid have resulted in convictions. There have been more than 65,000 charges laid under s.354 from 2003 to 2006, with 10 150 convictions for that offence. Another 1 415 charges are pending trial. The team was advised that this was because prosecutors either pursue predicate offences or a s.354 possession offence which they are more familiar with, and which is easier to prove as it does not require the additional intent element set forth in Section 462.31. Canada advised the assessment team that the volume of s.354 offences charged and convicted shows that it is aggressively pursuing the crime of money laundering. However, in summary, the team is concerned about the overall effectiveness of action taken to convict money launderers, due to the following considerations:

(a) The very low number of convictions for s.462.31 (which is the offence focussed on active money laundering).

(b) The information which suggests that the bulk of s.354 offences are not ML offences as contemplated by FATF (an examination of the Criminal Code shows that this offence, which was created in 1974, is closely linked to actions to be taken in relation to possession of stolen property – Canada also indicated in paragraph 152 above that s.354 (and also s.462.31) are offences dealing with illicit trafficking in stolen goods and other property) or that the charges laid under s.354 often involve minor offence.

(c) Other important government agencies that combat ML and TF are focused on s.462.31 e.g.FINTRAC can only make disclosures to law enforcement when it has reason to believe a TF offence or s.462.31 ML offence is implicated, but cannot make such a disclosure when a s.354 offence is suspected. Moreover, when FINTRAC receives law enforcement VIRS, it focuses its analytical resources on VIRS that involve s.462.31 offences, and not VIRS that involve s.354 offences. IPOC units lay more s.462.31 charges than s. 354 charges in spite of the 99 to 1 ratio in favour of s.354 that exists elsewhere.

235. (d) If the property is valued at less than CAD5 000 and does not involve a "testamentary instrument" the maximum penalty is 2 years as opposed to the 10 year sentence that is available for the more serious Section 354 offences as well as all Section 462.31 offences.

(e) Even if the assessment team where to credit s.354 offences as ML offences in all cases (which it does not), the fact remains that only 17% of s. 354 charges laid resulted in convictions or have been committed to trial, which is still very low.

236. The emphasis on and preference for pursuing the predicate crimes and the offence of possession of property obtained by crime, in addition to the lack of comprehensive data on investigations and prosecutions at federal and provincial levels, lead the evaluation team to conclude that the statutes available for countering ML are not being used as effectively as they could be. Canada should develop a more proactive approach to prosecuting the specific money laundering charge under s.462.31.

2.1.3 Compliance with Recommendations 1 & 2

Rec.	Rating	Summary of factors underlying ratings
R.1	LC	▪ The ML offence does not cover all designated categories of predicate offences (copyright related offences). ▪ Section 462.31 ML offence contains a purposive element that is not broad enough to meet the requirements of the Conventions or R.1. ▪ The number of convictions for Section 462.31 ML is very low, as is the percentage of convictions in comparison to charges laid.
R.2	LC	▪ The number of convictions for Section 462.31 ML is very low. ▪ Due to the lack of data on ML sentencing, is not possible to assess whether natural and legal persons are subject to effective, proportionate and dissuasive sanctions for ML.

2.2 Criminalisation of Terrorist Financing (SR.II)

2.2.1 Description and Analysis

237. *The terrorist financing offence*. In 2001, the Anti-terrorism Act (ATA) amended the Criminal Code to create three criminal offences related to the financing of terrorism. These amendments to the Criminal Code enabled Canada to implement international obligations under the UN Security Council Resolution 1373 and the UN International Convention for the Suppression of the Financing of Terrorism. The three terrorist financing offences under the Code are broadly defined and operate in an expansive fashion.

238. Section 83.02 of the Criminal Code makes it an offence to "wilfully and without lawful justification or excuse, directly or indirectly provide or collect property intending or knowing that it will be used, in whole or in part, to carry out a "terrorist activity" as defined in section 83.01(1) or any other act or omission intended to cause death or serious bodily harm to a civilian or to any other person not taking an active part in the hostilities in a situation of armed conflict, if the purpose of that act or omission, by its nature or context, is to intimidate the public, or to compel a government or an international organization to do or refrain from doing any act".

239.

240. Section 83.03 makes it an offence to "directly or indirectly collect property or to make available, provide, or invite a person to provide property or financial or other related services: (a) intending or knowing that they be used, in whole or in part, for the purpose of facilitating or carrying out a terrorist activity, or for the purpose of "benefiting" a person who is facilitating or carrying out a terrorist activity; or, (b) knowing that, in whole or part, they will be used by or will benefit a terrorist group".

241. Section 83.04 makes it an offence to "*use property, directly or indirectly, in whole or in part, for the purpose of facilitating or carrying out a terrorist activity*". It is also an offence under this section to possess property, intending or knowing that it will be used, directly or indirectly, in whole or in part, for the purpose of facilitating or carrying out a terrorist activity.

242. Under Section 83.01 of the Criminal Code, "terrorist activity" means:

> (*a*) an act or omission that is committed in or outside Canada and that, if committed in Canada, is one of the following offences:
>
> (i) the offences referred to in subsection 7(2) that implement the *Convention for the Suppression of Unlawful Seizure of Aircraft*, signed at The Hague on December 16, 1970,

(ii) the offences referred to in subsection 7(2) that implement the *Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation*, signed at Montreal on September 23, 1971,

(iii) the offences referred to in subsection 7(3) that implement the *Convention on the Prevention and Punishment of Crimes against Internationally Protected Persons, including Diplomatic Agents*, adopted by the General Assembly of the United Nations on December 14, 1973,

(iv) the offences referred to in subsection 7(3.1) that implement the *International Convention against the Taking of Hostages*, adopted by the General Assembly of the United Nations on December 17, 1979,

(v) the offences referred to in subsection 7(3.4) or (3.6) that implement the *Convention on the Physical Protection of Nuclear Material*, done at Vienna and New York on March 3, 1980,

(vi) the offences referred to in subsection 7(2) that implement the *Protocol for the Suppression of Unlawful Acts of Violence at Airports Serving International Civil Aviation*, supplementary to the *Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation*, signed at Montreal on February 24, 1988,

(vii) the offences referred to in subsection 7(2.1) that implement the *Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation*, done at Rome on March 10, 1988,

(viii) the offences referred to in subsection 7(2.1) or (2.2) that implement the *Protocol for the Suppression of Unlawful Acts against the Safety of Fixed Platforms Located on the Continental Shelf*, done at Rome on March 10, 1988,

(ix) the offences referred to in subsection 7(3.72) that implement the *International Convention for the Suppression of Terrorist Bombings*, adopted by the General Assembly of the United Nations on December 15, 1997, and

(x) the offences referred to in subsection 7(3.73) that implement the *International Convention for the Suppression of the Financing of Terrorism*, adopted by the General Assembly of the United Nations on December 9, 1999, or

(*b*) an act or omission, in or outside Canada,

(i) that is committed

(A) in whole or in part for a political, religious or ideological purpose, objective or cause, and

(B) in whole or in part with the intention of intimidating the public, or a segment of the public, with regard to its security, including its economic security, or compelling a person, a government or a domestic or an international organization to do or to refrain from doing any act, whether the public or the person, government or organization is inside or outside Canada, and

(ii) that intentionally

(A) causes death or serious bodily harm to a person by the use of violence,

(B) endangers a person's life,

(C) causes a serious risk to the health or safety of the public or any segment of the public,

(D) causes substantial property damage, whether to public or private property, if causing such damage is likely to result in the conduct or harm referred to in any of clauses (A) to (C), or

(E) causes serious interference with or serious disruption of an essential service, facility or system, whether public or private, other than as a result of advocacy, protest, dissent or stoppage of work that is not intended to result in the conduct or harm referred to in any of clauses (A) to (C),

and includes a conspiracy, attempt or threat to commit any such act or omission, or being an accessory after the fact or counselling in relation to any such act or omission, but, for greater certainty, does not include an act or omission that is committed during an armed conflict and that, at the time and in the place of its commission, is in accordance with customary international law or conventional international law applicable to the conflict, or the activities undertaken by military forces of a state in the exercise of their official duties, to the extent that those activities are governed by other rules of international law.

243. In line with the UN Convention, safeguards have been incorporated into the ATA with respect to the terrorist financing offences, including the legal threshold of knowledge and intention. In addition, the Attorney General's consent is required to institute proceedings.

244. In Canada's criminal code, the provisions that criminalize terrorist financing use the term "property", as opposed to the term "funds" that is used in the TF convention. As seen in Sections 83.02, 83.03, and 83.04 of the Criminal Code, terrorist financing offences refer to "property", which is defined in section 2 as including *(a) real and personal property of every description and deeds and instruments relating to or evidencing the title or right to property, or giving a right to recover or receive money or goods, (b) property originally in the possession or under the control of any person, and any property into or for which it has been converted or exchanged and anything acquired at any time by the conversion or exchange"* (see Section 2.1 of the report). This definition is very broad and is consistent with the definition of "funds" in the Terrorist Financing Convention.

245. The TF Convention states that the terrorist financing offence need not require that the funds: (i) were actually used to carry out or attempt a terrorist act(s); or (ii) be linked to a specific terrorist act(s). The wording in the Canadian terrorist financing offence makes reference to the collection of property with the intention that it be used, or knowing that it will be used for terrorist activity. The threshold of criminal conduct is met here if there is an intention to carry out terrorist activity and therefore does not require that funds are actually used to carry out the activity. This is consistent with the requirements of the TF Convention and the Recommendation. The Code, unlike the TF Convention, does not make reference to specific acts of terrorism, the use of funds by a terrorist organisation or to an individual terrorist, but uses the broadly defined term "terrorist activity". Terrorist activity as defined in the code includes an act or omission, committed to achieve specific ends. The Code also requires that the act be concluded with intention to achieve specific listed outcomes. The Code does not make direct reference to a specific terrorist individual, but the existing terrorist offences in part II.1 of the Criminal Code, together with the definition and jurisdiction sections in s. 7 can be used to define and cover the issue. The terrorist offences in Part II.1 of the Code and the reference to "terrorist activity" are specifically designed to interrelate. A terrorist activity is an act or omission, in other words conduct. That conduct is undertaken by individuals and terrorist groups. Indeed "terrorist groups" are defined as an "entity". An "entity" is defined as a person and the definition includes an "organization". Section 2 of the Criminal Code reinforces this by providing an expansive definition of an "organization" as any legal person. Finally every criminal offence that could be committed is structured to cover natural and legal persons by the word "everyone". As a result a specific terrorist individual is included in every relevant offence.

246. Section 24 of the Criminal Code provides that "every one who, having an intent to commit an offence, does or omits to do anything for the purpose of carrying out his intention is guilty of an attempt to commit the offence whether or not it was possible under the circumstances to commit the offence." As such, the Criminal Code offences referred to above include attempts to commit them. Further, the definition of "terrorism offence" in the Criminal Code (see above) specifically includes attempts to commit them as part of the definition of this term.

247. The terrorism financing offences include a conspiracy or attempt to commit, being an accessory after the fact or counselling in relation to the offences. This covers "participating as an accomplice" in the Terrorist Financing Convention. Further, sections 21 (parties to an offence), 22 (counselling an

offence), 23 (accessory after the fact), and 465 (conspiracy) of the Criminal Code confirm that the specific offences include being an "accomplice".

248. Regarding organizing or directing others to commit an offence, section 83.03 in its prohibition of inviting others to provide property, financial or other services would cover most of this activity. Further, the offence of instructing to carry out activity for a terrorist group (section 83.21) and instructing to carry out terrorist activity (section 83.22) could cover as well the activity of organizing or directing others to commit terrorist financing offences.

249. Finally, the terrorist financing offences and the definitions of terrorist activity and terrorist group provide that individuals alone or as part of a group of persons that act intentionally to further criminal purposes would be covered.

250. *FT as a predicate offence for ML*. Terrorism offences, as indictable offences under the Criminal Code, are predicate offences to which Canada's proceeds of crime legislation apply. These offences fall within the definition of "designated offences" found in section 462.3 of the Criminal Code. A conspiracy, an attempt, being an accessory after the fact in relation to, or counselling in relation to, a terrorism offence are also "designated offences" that are subject to this regime.

251. The terrorist financing regime in the Criminal Code includes provisions on the freezing, seizure/restraint, forfeiture and disposition of property as well. They are found in sections 83.08-83.15 and link with the existing provisions on proceeds of crime and forfeiture of offence-related property (Part XII.2 and sections 490.1-490.9).

252. *Jurisdiction over FT offences*. The specific terrorism financing offences apply in Canada regardless of whether the person alleged to have committed the offence is in Canada or in a different country than that of the terrorist group or in which the terrorist activity has or will occur. In addition, terrorism financing offences could be prosecuted, under certain limitations as required by the general principle of international criminal law jurisdiction, even if these offences have taken place in another country (see Sections 3.73 to 3.75 of the Criminal Code).

253. Finally, of note is the expansive territorial reach of section 354 (possession of property obtained by crime includes act or omission outside Canada) and section 462.3 ("proceeds of crime" includes any property outside Canada derived from an act or omission occurring outside Canada).

254. *Inference from objective factual circumstances*. In Canada, the intentional element of terrorism offences may be inferred from objective factual circumstances that are themselves proven through admissible evidence.

255. It is a well-established principle of criminal evidence that "any fact from which may be inferred a fact in issue or a fact relevant to an issue is admissible; it is called "circumstantial evidence" (McWilliams' Canadian Criminal Evidence, 4th ed., 2003). As regards knowledge, or intent, it is an essential element in all criminal offences, including the money laundering and possession of property derived from crime offences. Since these are criminal offences, the onus to prove the knowledge element beyond a reasonable doubt rests on the prosecution (known as the Crown in Canada). However, in Canada the prosecutor does not have to establish actual knowledge. A prosecutor can establish the required knowledge element by establishing that the accused was wilfully blind or reckless. In R. v. Sansregret, [1985] 1 S.C.R. 570, the Supreme Court held that recklessness and wilful blindness can be used to establish the criminal law requirement for intention. The rules of evidence apply with equal force to proof by circumstantial evidence as to proof by direct evidence. The evidence in both instances must be equally credible, admissible and relevant[30].

[30] See Re R. v. Truscott [1967] 2 C.C.C. 285 (S.C.C.).

256. *Criminal liability of legal persons.* In Canada, criminal liability for terrorism offences, including financing of terrorist activities and groups, applies to "everyone", which includes "an organization", defined in section 2 of the Criminal Code (see Section 2.1 of the report).

257. Section 22.2 defines the liability of an organization as a party to an offence, where the offence is one that requires proof of fault other than negligence. The prosecution must prove that one of the "senior officers" at least had the intent in part to benefit the organization and either: (a) such officer acting within the scope of his authority was a party to the offence; (b) the senior officer had the requisite mens rea (mental element) for the offence, was within the scope of his authority and directed others to do the required act, or (c) the officer did not take reasonable measures to stop the commission of the offence by others. In addition, corporations may be held criminally liable for actions of employees who are their directing minds[31].

258. *Parallel criminal, civil or administrative proceedings.* There is no prohibition on such parallel proceedings in Canada. Section 11 of the Criminal Code provides that "no civil remedy for an act or omission is suspended or affected by reason that the act or omission is a criminal offence."

259. *Sanctions*. A person or organization that is convicted of a terrorist financing offence (sections 83.02, 83.03 or 83.04 of the Criminal Code) may be sentenced to up to 10 years imprisonment in Canada.

260. The actual sentence imposed will reflect the purpose and principles of sentencing set out in sections 718 and following of the Criminal Code. The purpose of sentencing is to contribute to respect for the law and maintenance of a just, peaceful and safe society by imposing just sanctions that denounce unlawful conduct, deter the offender and others from committing offences, separate the offenders from society where necessary, assist in rehabilitating offenders and provide reparation for harm done to victims or to the community. The fundamental principle of sentencing is that a sentence must be proportionate to the gravity of the offence and degree of responsibility of the offender.

261. The fact that the offence is a terrorist offence is an aggravating circumstance that should result in an increase in the sentence (section 718.2(a)(v) of the Criminal Code.)

262. In respect of criminal liability of legal persons (organizations), section 735 of the Criminal Code provides for fines in lieu of imprisonment in certain circumstances.

Statistics (Recommendation 32)

263. The RCMP's National Security branch maintains a summary of key activities and milestones which contain the following statistics for a two month period:

- Number of terrorist groups disrupted.
- Cases submitted for prosecutions.
- Number of active anti-terrorism financing investigations.
- Number of tactical intelligence packages disseminated to field units.
- Number of disclosures to FINTRAC.
- Number of hours spent listing terrorist entities, and the number of charities de-registered.

264. For example for the time period of 1 April – 30 June 2006, the following statistics were recorded:

Active Anti-Terrorist Financing Investigations in Canada –	52
Disclosures to FINTRAC	7
Number of requests responding to Foreign Governments –	72
Number of Files Successfully concluded	601

[31] See Canadian Dredge & Dock Co. v. The Queen, [1985] 1 S.C.R. 662.

Number of Terrorist Groups disrupted	6

265. Other mechanisms which are reported are monthly reports in a narrative format with respect to central coordination of Anti-terrorism financing investigations, anti-terrorism training and the coordination and monitoring the status of charities.

266. Regarding prosecutions, one person, Mohammad Momin Khawaja has been charged with 7 terrorism offences, including providing, inviting a person to provide, and making available property and financial services, to a terrorist group in the United Kingdom, intending or knowing that they would be used, in whole or in part, for the purpose of facilitating or carrying out terrorist activity, or for the purpose of benefiting the terrorist group or others who were facilitating or carrying out terrorist activity, contrary to Section 83.03(a) of the Criminal Code. This case has not been adjudicated yet.

267. A total of 20 individuals have been charged with terrorist offences in two cases, including three persons charged under, Section 83.03 of the Criminal Code. Neither of these cases have been adjudicated yet, and since 2001 there have been no other prosecution or convictions. Given the not insignificant number of investigations, and the more than 600 files successfully concluded, the lack of any convictions since 2001 indicates a lack of effectiveness, despite the two prosecutions that are now before the courts.

2.2.2 Recommendations and Comments

268. The definition of "terrorist activity" in the Criminal Code incorporates by reference to specific offences set out in the Code, acts committed in a large number of international conventions. Canadian authorities should give consideration to ways to rationalise the references currently found in disparate locations, without losing the applicability within their country of the additional acts defined in the conventions.

269. The statistics compiled by the RCMP provide a clear indication of an increase in levels of terrorist related activity in Canada, with a large number of investigations and files. Only three persons have been charged with terrorist financing and these charges have not yet been heard. Nobody has been convicted. Given these facts it does not appear that as yet the TF offence is being effectively used. The overall effectiveness of the TF offence and regime is an issue that the authorities will need to pay close attention to going forward.

2.2.3 Compliance with Special Recommendation II

Rec.	Rating	Summary of factors underlying ratings
SR.II	LC	▪ The lack of any TF convictions and the very limited number of prosecutions shows that the offence has not yet been fully and effectively used.

2.3 Confiscation, freezing and seizing of proceeds (R.3)

2.3.1 Description and Analysis

270. *Confiscation*. Canada's Criminal Code contains provisions that authorise the confiscation (hereinafter "forfeiture") of proceeds of crime while the Criminal Code and its Controlled Drugs and Substances Act (CDSA) each have provisions to forfeit "offence-related property," which is Canada's term used to cover "instrumentalities." Forfeiture of "proceeds of crime" is fully covered in Criminal Code in sections 462.37, 462.38, and 462.43. Forfeiture of "offence-related property" is accomplished under the Criminal Code sections 490.1 and 490.2 and the CDSA sections 16 & 17. Offence related property includes instrumentalities intended for use in the commission of specified crimes (see definition of "offence-related property," Criminal Code Section 2). Only simple possession of controlled substances, which is a standalone offence in the CDSA, is not included in that Act's definition of "offence related property." Forfeiture is available for all money laundering and terrorist financing offences, as well as direct forfeiture as an option for all predicate offences. Conviction for any indictable offence or a conspiracy or attempt to commit an indictable offence can give rise to

forfeiture (see definition of "designated offence," Criminal Code section 462.3(1)). Subsection 462.3(1) of the Criminal Code exempts, by regulation, certain offences arising under 14 designated Acts of Parliament from the money laundering predicates and hence also the forfeiture regime.

271. Subsections 462.37 (3) & (4) of the Criminal Code provides for a fine or imprisonment in lieu of forfeiture. Canada considers this alternative as the forfeiture of property of equivalent value. However, the fine in lieu option is discretionary as subsection 462.37(3) states "the court may" impose same rather than "shall." The fine in lieu option arises in a proceeds of crime case where counsel for the Attorney General applies for forfeiture, thus it is an option completely in the control of the prosecutor and one that is rarely pursued in practice as only CAD3.3 million has been collected through this method. Moreover, the court, in theory could, elect not to impose such a fine. Nor is it clear that "fines," which are generally deemed to be a form of punishment, are to be treated the same way as "forfeitures" would be under Canadian law. For example, it does not appear that Criminal Code section 491.1 could be used to disburse such a fine to victims. Fines in lieu of forfeiture can be imposed for the amount of proceeds of crime that have been dissipated or located outside Canada. If there are no assets to which such a fine can be applied the court "shall" impose a jail sentence. The fine is enforced as a civil judgement against any other property that the offender owns at that time or may acquire in the future. It does not apply to non proceeds property the perpetrator transferred to third persons before the fine was imposed. If the accused later obtains wealth or accesses hidden illicit wealth not discovered at sentencing, he or she can be forced to comply with the monetary fine previously imposed. The prosecutor would have to anticipate such a windfall in advance and take the extra steps in the prosecution to obtain such an order, which does not seem to be a very practical solution. It is not prosecution service policy to get such an order in all cases in which forfeiture is an issue, and likely is only done if proceeds are spent and the prosecutor learns that non-tainted assets exist before sentencing. Section 734.7 of the Criminal Code provides the Attorney General with the flexibility to enforce the fine rather than apply to the court to have the offender serve the mandatory time in default. The fine and imprisonment in lieu of forfeiture option is an awkward attempt to ameliorate the problem of dissipated forfeitable assets.

272. Section 2 of the Criminal Code broadly defines "property" to include all real and personal property of every description and deeds and instruments relating to or evidencing the title or right to property, or giving a right to recover or receive money or goods as well as property originally in the possession or under the control of any person, and any property into or for which it has been converted or exchanged and anything acquired at any time by the conversion or exchange. The definition of "proceeds of crime," in section 462.3(1) of the Criminal Code specifically includes any property, benefit or advantage obtained or "derived directly or indirectly" as a result of the commission of a designated offence. Thus, in light of the definitions of "property" and "proceeds of crime" Canada's forfeiture provisions appear to permit the forfeiture of "income, profits or other benefits" as proceeds of crime[32].

273. Property is forfeited to Canada, whether it is held by the criminal defendant or a nominee third party. The relevant Canadian forfeiture provisions focus on identity of the property as either the "proceeds of crime" or "offence-related property" as the deciding factor as to whether it can be forfeited, rather than the actions or relationship of a property's owner to the offence committed. However, the latter inquiry may be relevant to the issue of the "innocent ownership" in any challenges made to the restraint, seizures and forfeiture of property by purported *bona fide* third-party owners of property that might be subject to forfeiture.

274. *Seizure.* Canada has a wide range of search and seizure or restraint authorities in its criminal laws to assist in confiscation matters. Canada does not use the term "freezing" in its law with the only exception being terrorist property as described and provided for in section 83.08 of the Criminal Code. In Canada, "freezing" is simply accomplished via restraint orders.

---

[32] See the Quebec Court of Appeal decision of R. v. 170888 Canada Ltée, (1999), 135 C.C.C (3d)367.

275. *Search Warrants.* Criminal Code section 487 and section 11 of the CDSA permit the police or a "public officer" to obtain judicial warrants, on the basis of reasonable grounds to believe that in a building, place or receptacles items described in the warrant will be found, and gives one authority to enter, search and seize the things set out in the warrant. The things to be searched for may include anything "in respect of which" an offence against any Act of Parliament has been or is suspected of having been committed, anything that will afford evidence of an offence, and anything intended to be used to commit an offence, and any offence-related property. *See, e.g.* subsections 487(1)(a) through (c.1). Section 487 of the Criminal Code sets out a broad search and seizure authority in Canadian criminal law but other Acts, including the CDSA, have stand alone search warrant provisions as well. In spite of those provisions, in light of Canada's Interpretation Act and case decisions, a Criminal Code section 487 search warrant is available in the investigation of every criminal offence. The authority to issue a search warrant to search and seize almost "anything" does have some limitations. The most significant is that intangible items, such as money on deposit in a bank account or real property, cannot be seized under the authority of a search warrant[33].

276. These Criminal Code search warrants can be issued by a justice of the peace and are available at any relevant stage in the investigative process. In the course of any execution of a search warrant, section 489 of the Criminal Code authorises the peace officer executing a search warrant to seize other things not listed in the warrant which he or she discovers that are obtained from the commission of crime, used in the commission of crime or afford evidence of another offence under any Act of Parliament. The issuing court, may order the detention and preservation of the property for three months (see Subsection 490(2)). However, the detention period can be extended and it is automatically extended as soon as charges are instituted.

277. *Special search warrant for proceeds of crime*. Section 462.32 of the Criminal Code provides authority for counsel for the Attorney General (*i.e.* the crown prosecutor) to obtain a special search warrant to seize property that is subject to forfeiture, which includes the proceeds of crime, but is obtained from a Judge, as opposed to a Justice of the Peace. Once a special search warrant against proceeds of crime is obtained and executed, section 462.35 provides that any seizure is effective for six months after execution. This period of detention may be extended and such an extension is continued once a criminal charge is initiated where a forfeiture of the property may occur. Pursuant to subsection 462.32(2.1) a special search warrant's search authority, once issued, is effective throughout Canada. It is not possible to obtain a special search warrant to search and seize proceeds of crime that may be forfeitable pursuant to the relevant forfeiture provisions when the relevant thing (*i.e.* the property) is outside of Canada. The Attorney General is required to give undertakings for damages and costs when obtaining such warrants, which according to Canadian officials "has not presented any problems" because since 1993, Canada has paid less than CAD50,000 in undertakings.

278. *Restraint order provisions for proceeds of crime and offence related property.* Sections 462.33 and 490.8 of the Criminal Code, respectively, permit the Attorney General to apply for restraint orders to restrain forfeitable proceeds of crime and forfeitable offence-related property. Such restraint orders are *in personam* orders prohibiting the persons named in the order from disposing or dealing with any property specified in the order. The order, once issued before a judge, is effective throughout Canada but also applies to property all over the world, and the persons subject to, *i.e.* served with, the order will commit an indictable offence for knowingly breaching the order (see Subsections 462.33 (3.01), (3.1) and (11), and 490.8 (3.1) and (9). The restraining order, to be effective, must be served upon all relevant parties in Canada, and it applies only against such served persons. The Attorney General must provide undertakings for damages and costs when restraining forfeitable proceeds of crime, which, according to Canadian officials, has not presented any problems (Criminal Code section 462.33(7). No undertaking is required for the restraint of offence-related property (Criminal Code section 490.8).

[33] See *R. v. Banque Royale du Canada* (1985), 18 C.C.C. (3d) 98 (Que. C.A.).

279. For forfeitable property located abroad, with the exception of a restraining order served on a person in Canada who controls property located abroad, Canada, like most nations, would have to rely upon its treaty relationships to obtain the restraint or seizure of such foreign property.

280. *Seizure made ex parte*. An ordinary search warrant for evidence or offence related property, under either section 487 the Criminal Code or section 11 the Controlled Drugs and Substances Act, are in practice *ex-parte* applications. The regular Criminal Code search warrant provisions do not expressly state that the application may be made *ex-parte* as a matter of right[34]. The CDSA Section 11, as well as Criminal Code section 490.8, for the restraint of offence-related property, the special search warrant for proceeds of crime under Criminal Code section 462.32, the restraint order for proceeds of crime under Criminal Code section 462.33, and the CDSA's restraint order for offence related property under section 14, all specify that the application may be *ex-parte*. However, in the case of the seizure or restraint of proceeds of crime the provisions include an additional consideration for the issuing judge. Subsections 462.32(5) and 462.33(5) each provide that the issuing judge may require that the applicant Attorney General provide notice of the application to any person, unless giving such notice before the issuance of the warrant would result in the disappearance, dissipation or reduction in value of the property or otherwise affect the property so that all or a part thereof could not be seized pursuant to the warrant. The Attorney General's filed materials in support of the application must make showing of factors that justify an *ex-parte* hearing as a matter of course, or only after the issue is raised by the court. There were no statistics showing how often Canadian judges required the Attorney General to provide notice. Canada advised that the practice is that courts grant such orders *ex-parte*.

281. *Criminal Code search warrant.* Criminal Code section 487 search warrants are available to law enforcement officers to help trace assets subject to forfeiture (see above). A law enforcement officer applying for a search warrant must provide the issuing justice or judge with reasonable grounds to believe an offence has occurred and that there is evidence in the place to be searched. The officer need not disclose the entirety of the investigation but must disclose information which would tend to call into question the reliability of the grounds relied on to obtain the warrant. Law enforcement agents pointed out that in response to Canadian case law on the reliability of evidence in search warrants, the applications for regular search warrants have become very lengthy, and often hundreds, even thousands, of pages in length. In practice, there often is a full-disclosure of all evidence that might be relevant to the case, rather than just evidence relevant to the specific search in question. This extra detail, although possibly not legally required, is provided in an abundance of caution. Thus, in practice, this makes obtaining a search warrant a very time-consuming and labour-intensive process.

282. *A Criminal Code confirmation order.* Section 487.013 of the Criminal Code provides authority for law enforcement to obtain essential information confirming the existence of an account relationship from any financial institution, as defined in section 2 of the Bank Act or any other entity covered by the PCMLTFA. A law enforcement officer applying for a confirmation order must provide the issuing justice or judge with reasonable grounds to suspect an offence has occurred or will occur and that the financial institution's information will assist the investigation of the offence. The single restriction on the confirmation order is that the person or organization named in the order that is required to confirm information must not be a target of the investigation. Finally, section 487.017 creates an offence when the person subject to the confirmation order fails to produce the documents or data. Confirmation of an account relationship will allow a law enforcement official to aver that such records exist whenever they seek a search warrant or production order against the relevant entities.

283. *Criminal Code Production order.* Frequently there are cases where evidence is required, but the more invasive search warrant is unnecessary. The Criminal Code also provides for a less intrusive obligation to produce documents or data in section 487.012. Section 487.015 allows that party subject to a production order to apply to the court for an exemption if disclosure would breach legal privilege

[34] See *Nova Scotia (Attorney General) v. MacIntyre*, [1982] 1 S.C.R. 175 at 179-180 ("The issuance of a search warrant is a judicial act on the part of the justice, usually performed ex parte and in camera, by the very nature of the proceedings").

or the documents or data are not in the person's possession or control. Section 487.016 specifically provides that the person may not object to production on the basis of self incrimination while insuring that the documents or data may not be used against the producing person except for perjury charges. Finally, section 487.017 creates an offence when the person subject to the production order fails to produce the documents or data. The production order, similar to a confirmation order, provides that the person or organization named in the order to produce must not be a target of the investigation.

284. *A Criminal Code general warrant*. The Criminal Code confirmation order reveals the existence of an account relationship and a production order will result in the production of existing data and documents. A search warrant will allow for the seizure of things, including documents or data that exist in the place at the time the place is searched. The problem with all of these provisions is that they provide a means to obtain existing evidence, rather than anticipatory evidence that may come into existence at a known or reasonable time in the future. There are cases where the financial data or other information will come into existence at a period in the future. There are also cases where law enforcement may wish to undertake a surreptitious search and inspection. The Criminal Code addresses these scenarios in its section 487.01 general warrant authority. The court issuing a general warrant must be satisfied, by information on oath in writing that an offence has or will occur and that information, but not necessarily evidence, concerning the offence will be obtained. Provided that the judge is satisfied that a general warrant is in the best interests of the administration of justice and that no other specific authority exists for would provide for a warrant, authorisation or order then the requested authority for the required technique, procedure or device to be used or thing to be done is authorised by the general warrant. Using this authority it is possible to obtain a general warrant for a financial monitoring order for a specified time into the future.

285. *Tax Information.* Section 462.48 of the Criminal Code provides a specific process to properly obtain the production of income tax information in a criminal investigation, at the investigatory stage. Such production is limited to investigations of drug, organised crime, money laundering offences with a drug or organised crime predicate, and terrorism offences. Hence, it is not available to trace assets pre-indictment in cases that do not involve organised crime, drug or terrorism charges. The importance of a Criminal Code production order for tax information in any investigation for the offences set out in subparagraph 462.48(1.1) is that the tax authorities, pursuant to section 241 of the Income Tax Act, are otherwise immune from criminal search warrants.

286. *Voluntary Disclosures and Privacy Laws*. Canada's professional law enforcement relies on cooperation from voluntary witnesses for much criminal investigation activity. This cooperation is reinforced by means of a safe harbour protection in respect to proceeds of crime in Criminal Code section 462.47, which states in the relevant part: "*. . . subject to section 241 of the Income Tax Act, a person is justified in disclosing to a peace officer or the Attorney General any facts on the basis of which that person reasonably suspects that any property is proceeds of crime or that any person has committed or is about to commit a designated offence.*[35]"

287. Subsection 7(2) of PIPEDA provides that an organization may elect to use "personal information" that it has reasonable grounds to believe could be useful in the investigation of a contravention of the laws of Canada, a province or a foreign jurisdiction that has been, is being or is about to be committed, and the information is used for the purpose of investigating that contravention. Subsection 7(3), or more specifically subparagraphs (c.1), (d) and (e), allow an organization to voluntarily disclose "personal information" without disclosing the fact of that disclosure to their customer.

288. Subsection 7(3) (c) of PIPEDA requires organizations to comply with subpoenas or warrants issued as well as any orders made by a court, person or body with jurisdiction to compel the production of information, or to comply with rules of court relating to the production of records. While

35. Section 241 of the *Income Tax Act* creates an offence for any Revenue Canada employee to disclose any income tax information to anyone absent a court order or specific but limited exceptions in the *Income Tax Act.*

PIPEDA was carefully constructed to still permit voluntary disclosures to law enforcement, and clearly does not prohibit same, several regulated private sector persons that met with the FATF assessment team wrongly thought that PIDEDA was at odds with the voluntary disclosure provisions in the Criminal Code, and the mandatory disclosures to FINTRAC that are required by the PCMLTFA. Law enforcement further opined that the enactments of PIPEDA and the PCMLTFA have had a chilling effect on the number of voluntary disclosures to law enforcement under the Criminal Code.

289. *Bona fide third party - immediate relief from seizure*. Subsection 489.1 provides that the seizing peace officer, if satisfied as to ownership of the thing and that its detention is not required for the investigation or other proceeding, may elect to return the thing they seized to the lawful owner or person lawfully entitled to possession of the thing, rather than detaining the thing after obtaining a detention order from the court. In that case the peace officer must obtain a receipt from the person to whom the officer returned the thing and file that receipt with the justice issuing the warrant. A search warrant directed to a public officer (i.e. a person who has been appointed or designated to administer or enforce the applicable federal or provincial laws and who is named in the warrant) is subject to subsection 489.1(2) with the result that anything seized by that public officer may not be returned, but rather the public officer must file a report or bring the thing to the court for the court's determination on detention or return. If the thing is required for a subsequent proceeding, such as a forfeiture application, the officer must, like any public officer, make a section 490 return to the court. This return is for the purpose of either seeking a detention order or allowing the court to determine its return.

290. *Post seizure judicial release*. Section 490 applies to all seized property other than seized or restrained proceeds of crime seized as a result of a special search warrant under section 462.32 of the Criminal Code and restraint order under section 462.33 of the Criminal Code. If an item is seized under the authority of section 14 of the CDSA, then the section 490 Criminal Code's process applies, with the exception of a controlled substance pursuant to sections 13 & 15 of the CDSA. Under Section 490 a person in possession at the time of seizure or the owner has a right to seek the return of the seized thing. In the case of the person in possession they may demonstrate hardship that may be caused by the continued possession of the thing by the state (see subsections 490(7) & (8)). The lawful owner or person lawfully entitled to possession of the seized thing may, at any time, institute an application for the return of the seized thing pursuant to subsection 490(10). The court considering any return application must consider if the seized thing is required for some other purpose, such as a forfeiture application (see subsections 490(9) & (11)). These provisions apply up until the time that the court considers any relevant forfeiture application.

291. *Release of offence related property*. There are special provisions for offence-related property, since that property may be forfeited upon conviction. It is also possible for the person in possession of offence-related property to successfully apply for the return of the seized thing due to a claim of hardship (see subsection 490(8). In that case, a criminal recognizance is an option for the court to consider, pursuant to subsection 490.9 (1), if the thing falls under the Criminal Code's definition of offence-related property. If the property is offence-related property under the CDSA's definition subsection 13 (6) of that Act also contemplates return under the supervision of a criminal recognizance. If the court elects to return seized or restrained offence-related property to the relevant person the court ordered recognizance can require the owner to preserve and retain the thing, making it available for the subsequent forfeiture application. The terms can include a requirement to surrender the thing in advance of the forfeiture application. Any failure to comply with the recognizance can lead to the forfeiture of the amount covered by the recognizance.

292. *Relief from a seizure or restraint of proceeds of crime.* Section 462.34(a) of the Criminal Code provides that any person with an interest in the seized or restrained property may apply to the court to return their seized proceeds of crime or vacate any restraint order against proceeds of crime. These applications must be brought upon notice to the Attorney General under Criminal Code section 462.34(2). The court may order return and the judge may impose a criminal recognizance, under Criminal Code section 462.34(4)(a). Alternatively, the court may simply return the property if it is

satisfied that the original order should not have been issued per section 462.34(6), or the applicant is an innocent owner in a case where the property is not required for any investigation or proceeding per section 462.34(6)(b). Things seized pursuant to a section 462.32 special search warrant may be immediately released to their lawful owner by the seizing agent under section 462.32(4.1) if certain mitigating factors are present.

293. Section 462.34 provides an immediate opportunity to apply to vary or vacate the special search warrant or restraint order. That authority is used in support of the more frequent application under section 462.34 to obtain access to the property for the purposes of the persons business, living and legal expenses under section 462.34(4)(c). The argument that such property, as property obtained from crime, may create an offence when it is placed in the hands of a third-party, such as legal counsel, is addressed by subsection 462.34(7). As a result, it is common to have the court deal with applications, against seized or restrained proceeds of crime, for the purposes of funding a person's business, living and legal expenses. Between 2000 and 2007 Canada seized or restrained CAD572.8 million in assets, while in the same period court ordered payouts for all business, living and legal expenses was CAD8.3 million. Nonetheless, the forfeiture statistics suggest that a significant proportion of property seized for forfeiture is not actually being forfeited.

294. There are checks and balances in the ability to seek such funding since the property is theoretically dissipated by such orders. Subsection 462.34(4) requires an order unless "… the judge is satisfied that the applicant has no other assets or means available for the purposes set out in this paragraph and that no other person appears to be the lawful owner of or lawfully entitled to possession of the property." This means that if the applicant has other assets or means or if there is a lawful owner of the relevant property the court cannot dissipate that property to fund the applicant's expenses. Of course, it is often difficult for the Attorney General to prove that the applicant has other assets in cases were the accused is particularly adept at hiding his or her criminal proceeds. The authority to seek funded legal expenses out of seized or restrained proceeds of crime is further circumscribed by subsections 462.34(5) to (5.2) of the Criminal Code. If there is a lawful owner (*i.e.* a victim) of the relevant property, the court should not dissipate that property to fund the applicant's expenses. Finally, the court may, but is not required to, consider the applicable legal aid tariff rate in releasing funds to cover legal expenses under Criminal Code Section 462.34(5).

295. *Forfeiture and third party relief.* In addition to the protecting the rights of *bona fide* third-parties in cases where seizure or restraint occurred, the same parties have rights at the time of a forfeiture application of offence-related property or proceeds of crime. Section 490.4 of the Criminal Code and section 19 of the CDSA require third-party protection in the case of forfeiture against offence-related property. Section 462.41 provides a similar protection for third-parties in the case of a forfeiture application against proceeds of crime.

296. All *bona fide* third-parties have a right to notice of the forfeiture application and the right to participate in that application. In addition, section 490.5 of the Criminal Code and Section 20 of the CDSA establish the right of these third parties to also seek relief from forfeiture if they did not appear at the original forfeiture application. In the same fashion section 462.42 of the Criminal Code creates an identical right of third-parties to seek relief from forfeiture of proceeds of crime if they did not appear at the original forfeiture application. Finally, in all cases, the forfeited property may not be sold for thirty (30) days to give all parties an opportunity to institute an appeal (see s. 490.7 of the Criminal Code or s. 22 of the CDSA for offence related property and section 462.45 of the Criminal Code for proceeds of crime).

297. *Victims of crime and forfeiture.* Victims may not have a direct and valid interest in the property that is targeted for forfeiture simply because their property had been laundered long before the seizure and forfeiture issues developed. Those victims have and interest in the criminal but not a specific interest in property targeted for forfeiture. As a result they will not have standing to challenge the forfeiture order. This issue is addressed by sections 738 and 740. It is further ameliorated by subsection 462.49 of the Criminal Code, which continues and gives priority to any Act of Parliament

respecting restitution to or compensation of victims. The Criminal Code does contain restitution to persons affected by crime provisions in sections 738 to 740. As a result, victim restitution and forfeiture effectively coexists in Canada.

298. *Authority to prevent or void actions.* Canada does have the authority, in any appropriate case, to void actions designed to frustrate the forfeiture of property. If the targeted asset is offence-related property, section 490.3 of the Criminal Code or section 18 of the CDSA can be used to set aside a conveyance that occurs after the seizure or restraint. In the case of proceeds of crime section 462.4 provides for the same authority. In addition, if the person receiving the relevant property knew or should have known that the property was proceeds of crime and the transfer occurred before the seizure or restraint that person commits the offence of possession of property derived from an indictable offence under section 354(1) of the Criminal Code. A convicted owner is also subject to a fine in lieu of forfeiture resulting from that owner's dissipation of the property.

Additional elements

299. Membership in a criminal organization is not an offence in Canada. Nor are all the assets of an organization engaged in criminal activity something that can be seized, restrained or forfeited, simply because it is owned by an organization found to be operating for criminal purposes. Those assets would have to be either offence-related property or the proceeds of crime from an offence committed by the organization before they can be subject to forfeiture.

300. Several Canadian provinces have enacted civil forfeiture laws[36]. Other legislation has been passed but not yet in force (Alberta's Victims Restitution and Compensation Act, 2001) or pending before a Legislative Assembly (Quebec's Bill 36 "An Act respecting the forfeiture, administration and appropriation of proceeds and instruments of unlawful activities"). Generally, these provisions allow proceeds of crime to be forfeited in a civil setting under a civil standard. In addition, for indictable offences under the Criminal Code, if an information has been laid against a person, and that person subsequently dies or absconds, a criminal court can issue an *in rem* forfeiture judgment against the proceeds of crime or offence-related property upon a showing beyond a reasonable doubt that the subject property is the proceeds of, or relates to, the offence charged in the information. *See* Criminal Code sections 462.38 and 490.2. Finally, after conviction on any designated offence, a criminal court can order the forfeiture of property that is shown, beyond a reasonable doubt, to be the proceeds any other indictable offence, even if the property is not the proceeds of the offence of conviction. *See* Criminal Code section 462.37(2).

301. On November 25, 2005 a significant revision to the criminal forfeiture provisions, created a reverse onus provision against some proceeds of crime. Subsection 462.37(2.01 to 2.08) of the Criminal Code apply to these cases. The provision covers organized crime offences and drug offences contrary to sections 5, 6 and 7 of the CDSA, including a conspiracy or an attempt to commit, being an accessory after the fact in relation to, or any counselling in relation to an offence under those sections if they were prosecuted by indictment.

Implementation Issues

302. Canadian forfeiture statistics reveal that between 2000 and 2007 Canada's property manager was responsible for the post seizure/restraint of CAD572.8 million in assets. In the same period the realized value of forfeited assets was only CAD203.93 million (roughly 36% of property sought for forfeiture has actually been realised). Canada informed the assessors that the property manager currently has another CAD325.5 million in assets under its management but it is unclear what portion of that amount includes recent seizures or what portion involves assets already captured in the forfeiture statistics. Forfeited funds are often maintained for appeals and other reasons well after they

[36] Remedies for Organized Crime and Other Unlawful Activities 2001, see http://www.e-laws.gov.on.ca/DBLaws/Archives/20050101/Statutes/English/01r28_e.htm; Manitoba The Criminal Property Forfeiture Act, 2004 see http://web2.gov.mb.ca/laws/statutes/ccsm/c306e.php; Saskatchewan, The Seizure of Criminal Property Act 2005, see http://www.qp.gov.sk.ca/documents/English/Statutes/Statutes/S46-001.pdf ; British Columbia , The Civil Forfeiture Act 2005.

are on the forfeiture side of the ledger so property under management figures could include large amounts of forfeited property. It appears that in the period 2000-2007, the RCMP's IPOC Units were responsible for approximately for 40% (CAD82.39 million) of Canada's total forfeitures. Thus, the IPOC Unit forfeiture data is the best model for measuring the overall effectiveness of Canada's forfeiture program, particularly as IPOC Units specialize in proceeds of crime investigations and therefore should be getting above-average results.

303. The value of the IPOC Unit seizures appears to be declining over the last 3 years, particularly if the 2004 figures are omitted, and certainly compared to the first three years of data. This is possibly due to the IPOC Unit's relatively recent focus on more labour intensive cases intended to dismantle criminal organizations, which naturally takes away resources from pure proceeds of crime recovery efforts that had been the initial focus of the IPOC Units. A better measure of effectiveness is the IPOC Units overall seizure to forfeiture ratio from 2000 to 2007. Considering that 96% of the IPOC Unit cases from 2000 through 2007 are already closed, it means the lag-time between seizures and forfeitures is not that significant and the cumulative figures are fairly up-to-date. The cumulative IPOC Unit forfeitures over the seven-year period is about 45% the value of the property initially seized or restrained for forfeiture. Over the past seven years Canada is averaging about CAD27 million a year in forfeitures, and over the last 4 years about CAD33 million a year, and has declined slightly over the last two years. If the IPOC units are losing or releasing 55% of restrained assets prior to forfeiture, and the forfeiture numbers are stagnating or declining over time, this suggests that effective is declining. Based on studies, IPOC representatives suggested the 55% seizure-forfeiture gap was potentially due to payment of attorney fees and living expenses of accused persons, and/or. plea bargains. IPOC representatives acknowledged that the seizure/forfeiture gap is still an area of concern. Lack of systemized forfeiture training may be a factor affecting the stagnation of forfeiture numbers.

304. The loss of potentially forfeitable assets, in theory, could be offset by fines in lieu of forfeiture. Section 462.37(3)(d) of the Criminal Code permits a court to substitute a fine for assets no longer available for forfeiture. Even assuming a court would later punish an accused for having successfully petitioned the same court for living or legal expenses under section 462.34(4), in IPOC Unit cases only CAD3.3 million of fines in lieu of forfeiture were "imposed" in the last six years, a small amount when compared to the close to CAD100 million of assets that were seized but not forfeited over that same time period. Further, it is unclear what portion of the CAD3.3 million was actually paid to the Crown. Finally, fines in lieu of forfeiture that are not paid to the Crown may result in higher sentences for the person convicted of the underlying offence. However, the government of Canada has not provided any IPOC Unit data or other law enforcement data indicating how often sentences have been increased for a failure to pay fine in lieu of forfeiture. Thus, it is very difficult to assume that this aspect of the law has been an effective and adequate deterrent to the judicially assisted wasting away of forfeitable assets that IPOC representatives and the statistical data has identified. According to the forfeiture data, it appears a great majority of the assets sought for forfeiture in Canada are not being forfeited.

305. Outside of the IPOC units, there seemed to be less emphasis on confiscation efforts in other law enforcement units or the Crown counsel in general. In an effort to fill some of the deficiencies of the criminal forfeiture regime, certain provinces are experimenting with specialized units and non-conviction based forfeiture regimes, but those programs are still in their infancy and their impact to date has been very limited. Several non-IPOC law enforcement units complained that IPOC units no longer have the resources to assist them with most of their forfeiture needs and feel that they do not have the expertise or resources to handle the forfeiture part of the case. IPOC representatives admitted that they have had to turn down work presented by other agencies and units because the increasing complexity of their cases and their limited resources require them to focus on other aspects of the cases. The IPOC units are hoping to address the assistance shortfall by providing training to other law enforcement agencies so that these entities could handle their own forfeiture matters. IPOC representatives have trained a few hundred law enforcement agents in the last couple of years, but the

scope of the training was limited and Canada has many thousands of agents that did not receive such training.

306. The IPOC Units have been asked to do more complex matters with limited resources. There also seemed to be very little if any coordinated or sophisticated training efforts in the forfeiture area. One legal expert mentioned that he gave at least six lectures to law enforcement groups per annum. It was unclear if he is the only prosecutor giving such lectures. In any event, at most this training is discretionary and not mandatory. Nor does there seem to be any one entity responsible for coordinating Canada's day-to-day forfeiture efforts, forfeiture policy, or forfeiture strategy, or even the collection of forfeiture data, outside of the federal property manager (the federal property manager manages seized assets derived from federal law enforcement cases, *i.e.* RCMP, but also from provincial police forces cases that led to prosecution at the federal level). Since virtually any police officer or prosecutor in Canada can become involved in a criminal case that gives rise to forfeiture, it was surprising there was not a more coordinated national approach to forfeiture efforts or training.

Statistics

307. The confiscation statistics provided by Canada are incomplete (clearly some provincial data was not captured as noted by prosecutors interviewed by the assessment team). Canada has not provided an accurate picture of what all agencies or provinces in Canada seize or forfeit in any given year, but instead has given statistics from various different sources in somewhat incompatible formats and seemingly focused only on "proceeds of crime and money laundering" cases. The scope of Recommendation 3 is slightly broader than that. Under the Vienna and Palermo Conventions possession of criminal proceeds offences relating to covered offences can be characterized as money laundering offences. However, it is highly unlikely that the bulk of Canada's "possession of criminal proceeds" cases resulted from either the organized criminal offences or the drug offences covered by those two treaties. What percentage of Canada's forfeiture involved drug cases, stolen property cases, fraud or organized crime cases can not be determined from the statistics provided by Canada. One thing is certain; Canada has a mostly conviction-based forfeiture system and had only 21 Section 462.31 money laundering convictions in 5 years. In the same five year period the charge and conviction figures show that Canada had 10 150 convictions for the possession of property derived from criminal offence, which could cover a range of different underlying offences.

308. The property manager reports that it managed or supervised the management of CAD572.8 million in seizures between 2000 and 2007. It further reports that it realized CAD203.93 million from forfeitures. Finally it reports that as of September 25, 2007 it currently manages or supervises assets having a value of CAD325.5 million. The amount of property under management by Public Works and Government Services in Table 13 does not help explain what is actually being forfeited in any one year, nor does it explain the actual value of the assets "added" in any one year as it is likely assets are managed for more than one year. Arguably, the steady growth in the amount of property under government management while forfeiture numbers are stabilizing or even decreasing over that time period actually suggests that such property is not being efficiently forfeited, but, instead, is held for long period of times. It would be interesting to see if criminal cases involving substantial amounts of forfeitable assets take longer than similar cases without such forfeitable assets considering the ability to access restrained proceeds of crime for legal fees and other expenses.

RCMP's Integrated Proceeds of Crime Program								
	2000-2001	**2001-2002**	**2002-2003**	**2003-2004**	**2004-2005**	**2005-2006**	**2006-2007**	**Total**
# Cases Opened	239	231	256	226	256	228	204	1 640
Value of Seizures	19 946 000	23 795 000	36 582 000	16 015 000	39 220 000	18 982 000	26 064 321	CAD180 604 321
# Closed Cases	213	198	211	253	289	199	206	1 569
Value of Forfeitures	7 643 504	7 387 364	11 024 119	14 494 264	10 200 981	15 116 644	16 524 728	309. CAD82 391 60 4

Seized Property Management Directorate										
Gross Seizures from RCMP's IPOC Units										
Fiscal Years 2000-01 to 2006-07										
			Asset Count by Type							
Year	Case Count	Total Value (CAD'000)	Cash	Fin. Instr.	Hydro	Aircraft	Vehicle	Vessel	Other	Real Est.
00-01	239	19 946	322	67	26	0	96	6	260	20
01-02	231	23 795	311	45	16	7	176	11	551	53
02-03	256	36 582	374	43	9	1	178	9	219	47
03-04	226	16 015	293	28	8	0	89	2	48	26
04-05	256	39 220	429	136	28	0	162	4	86	82
05-06	228	18 982	265	5	16	0	97	6	65	42
06-07	204	26 064	265	16	24	1	125	8	71	56
Total	**1 640**	**180 604**	**2 259**	**340**	**127**	**9**	**923**	**46**	**1 300**	**326**

Value of the seized property managed by Public Works	
Fiscal Year	**Value of property**
2000-01	CAD152.0 million
2001-02	CAD172.7 million
2002-03	CAD216.3 million
2003-04	CAD235.6 million
2004-05	CAD286.8 million
2005-06	CAD324.5 million

Value of property forfeited in Money Laundering cases		
Fiscal Year	**Value of property forfeited**	**Number of Cases**
2000-01	CAD19.03 million	1 686
2001-02	CAD19.01 million	2 127
2002-03	CAD29.01 million	3 216
2003-04	CAD33.68 million	4 405
2004-05	CAD36.4 million	5 350
2005-06	CAD35.13 million	5 180
2006-07	CAD31.4 million	9 953
Total	CAD203.93 million	

2.3.2 Recommendations and Comments

310. Canada should improve its mechanisms for collecting, maintaining and analyzing confiscation data. It should consider authorizing a study to identify why the IPOC Unit seizures and forfeiture numbers are decreasing, and why there is a large gap between the amount of property seized for forfeiture and the amount of property actually forfeited. Canada should consider ways to combat the dissipation of criminal proceeds and offence-related property to criminals for use as legal, business and living expenses even in non-victim cases. The Criminal Code should provide a specific process to properly obtain income tax information in the investigatory stage that is not limited to investigations of drug, organised crime, terrorist and money laundering offences with a drug, terrorist or organised crime predicate.

311. Canada should consider increasing funding to its IPOC units as they have some difficulties handling both major case responsibilities and every-day forfeiture responsibilities with the current resources allocated. Canada should consider creating mandatory specialized one or two day forfeiture and financial investigation training programs for all new law enforcement personnel and Crown counsel. Canada should create national or provincial entities that sets confiscation policies and standards and can develop and manage any training programs, as well as generally encourage the use of forfeiture in any criminal case in which an economic benefit was obtained by the accused by promoting confiscation.

2.3.3 Compliance with Recommendation 3

Rec.	Rating	Summary of factors underlying ratings

R.3	LC	▪ The fine in lieu forfeiture provision does not fully and effectively meets the requirement for equivalent value provisions and does not apply to property held by third parties. ▪ Based on the limited quantitative and qualitative information available, it does not seem that the confiscation and seizure regime is fully effective, particularly with respect to value based confiscation.

2.4 Freezing of funds used for terrorist financing (SR.III)

2.4.1 Description and Analysis

General

312. Canada's United Nations Act and its related regulations enable the Canadian government to implement the decisions contained in the resolutions of the United Nations Security Council. The United Nations Al-Qaida and Taliban Regulations (UNAQTR), and the Regulations Implementing the United Nations Resolutions on the Suppression of Terrorism (RIUNRST), were enacted under the authority of Canada's United Nations Act. These regulations allow Canada to list a terrorist individual or entity for the purpose of freezing the funds or assets owned or controlled by that individual or entity or its associates. A third listing mechanism exists under the Criminal Code for threats to Canada's domestic security. The Criminal Code explicitly defines a "terrorist group" and listed individual or entities are determined on the basis of this definition. In combination, these mechanisms allow Canada to list either domestic and foreign terrorist individuals or entities.

313. The decision to list a terrorist entity ultimately lies with the Governor-in-Council, with the exception of those entities listed by the UN 1267 Committee. UNSCR 1267 and successor resolutions are implemented in Canada through the United Nations Al-Qaida and Taliban Regulations (UNAQTR) which automatically incorporate into Canadian law, by direct reference, the list of individuals and entities who are designated by the 1267 Committee. Paragraph 4(b) of UNSCR 1267 is implemented in accordance with s. 4, 4.1, 5 and 5.7 of the UNAQTR. The primary difference between listing an entity pursuant to regulations under the United Nations Act and the Criminal Code is the evidentiary threshold required to support the listing. To list an individual or entity using the UNAQTR, there must be "reasonable grounds to believe" that the individual or entity is involved in terrorist activity. The evidentiary standard is stronger with respect to Criminal Code listings as the Governor-in-Council must have "reasonable grounds to believe that the entity was knowingly" involved in a terrorist activity.

Procedures to freeze terrorist funds or other assets in accordance with S/RES/1267(1999)

314. The United Nations Afghanistan Regulations (1999) gave effect to S/RES/1267(1999). Amendments were made to these regulations on 23 June 2006 and these regulations are now referred to as the United Nation Al-Qaida and Taliban Regulations (UNAQTR).

315. These regulations prohibit persons in Canada and Canadians outside Canada from having financial dealings with the Taliban and Usama Bin Laden and his associates or persons acting on their behalf (Section 4 of the UNAQTR). This includes all funds or assets that are directly or indirectly used, or intended to be used, by these designated individuals or entities. Persons designated by the United Nations 1267 Committee are automatically covered by the regulations.

Procedures to freeze terrorist funds or other assets in accordance with S/RES/1373(2001)

316. The Regulation implementing the United Nations Suppression of Terrorism Regulations (RIUNRST) gives effect to S/RES/1373(2001). The RIUNRST provides a list of individuals or entities for which there are reasonable grounds to believe they are involved in or associated with terrorist activities and prohibits persons in Canada and Canadians outside Canada from having financial dealings with these individuals or entities.

Listing procedures under the Criminal Code

317. The Criminal Code listing mechanism was developed in 2001 as part of the omnibus Anti-terrorism Act. The Anti-terrorism Act was developed to combat terrorism, while ensuring that human rights, such as the right to privacy, are respected. Part II.1 of the Criminal Code has provisions that prohibit the financing of terrorism which are designed to address threats to Canadian security. These provisions include the listing of individuals or entities for which there are reasonable grounds to believe that the individual or entity has knowingly carried out, attempted to carry out, participated in or facilitated a terrorist activity; or the entity is knowingly acting on behalf of, at the direction of or in association with an entity involved in a terrorist activity (Section 83.05 of the Criminal Code).

318. Listing under the Criminal Code allows assets to be frozen and subject to seizure, restraint and forfeiture through the automatic statutory authority in Section 83.08 of the Criminal Code.

Laws and procedures to examine and give effect to the actions initiated under the freezing mechanisms of other jurisdictions

319. The UNAQTR, the RIUNRST and the Criminal Code listing mechanisms provide Canada with the ability to respond to international listings through the United Nations, undertake joint listings and list both domestic and foreign individuals and entities.

320. In the case where intelligence relating to a proposed listing is received from another country, it is the responsibility of CSIS and/or the RCMP to determine the credibility of the information received. Both CSIS and the RCMP work with their international counterparts when collecting intelligence relating to a potential listing.

321. The process of listing under the Criminal Code begins with criminal and/or security intelligence reports on an entity disclosing the reasonable grounds to believe that the entity has knowingly carried out, attempted to carry out, participated in or facilitated a terrorist activity; or the entity is knowingly acting on behalf of, at the direction of or in association with an entity involved in a terrorist activity. The legislation provides for the Governor in Council to establish by regulation a list on which the Governor in Council may place any entity, on the recommendation of the Minister of Public Safety and Emergency Preparedness Canada.

322. The criminal and/or security intelligence reports are submitted to the Minister of Public Safety and Emergency Preparedness Canada for consideration. If the Minister has reasonable grounds to believe that the above test is met, the Minister may make a recommendation to the Governor in Council to place the entity on the list.

323. If the Governor in Council is satisfied that there are reasonable grounds to believe that the above test has been met, the entity may be placed on the list of individuals or entities. The listing of an individual or entity is published in the Canada Gazette and on the Public Safety and Emergency Preparedness Canada website under “Currently listed entities”. As of 31 December 2006, there were 40 entities listed pursuant to section 83.05 of the Criminal Code.

Funds subject to freezing actions

324. The freezing mechanism in place at Section 4 of the RIUNRST prohibits any person in Canada and Canadians outside Canada, to knowingly:

(a) Deal directly or indirectly in any property of a listed person owned or controlled directly or indirectly by that perso.
(b) Enter into or facilitate, directly or indirectly, any transaction related to a dealing referred in (a).
(c) Provide any financial or other related service in respect to the property referred in (a).

(d) Make any property or any financial or other related service available, directly or indirectly, for the benefit of a listed person.

325. Property is defined at Section 1 of the regulations and includes property of every description and documents relating to or evidencing the title or right to property, or giving a right to recover or receive money or goods, and includes any funds, financial assets or economic resources. This is in line with the FATF definition of "funds and other assets".

326. Section 4 and 4.1 of the UNAQTR have basically the same provisions for individuals and entities listed by the UN 1267 Committee, specifically the Taliban or a person associated with them, acting on their behalf or at their direction, Usama bin Laden or his associates, or by persons acting on their behalf or at their direction. In addition, a breach of either the UNAQTR or the RIUNRST gives rise to a criminal offence in Section 3 of the United Nations Act, which upon a summary conviction, can lead to fines of up to CAD100 000 and/or imprisonment up to one year. Imprisonment of up to 10 years can result on conviction on indictment.

327. The prohibitions outlined above, combined with the criminal offences of dealing in assets controlled or owned by listed individuals or entities, freezes all that individual or entity's assets within Canada and prevents Canadians outside of Canada from dealing with such property. Although the legal underpinnings are sound, the effectiveness of the freeze mechanisms are impacted by the degree to which information on the listed persons and entities is communicated to Canadians in general and the financial sector and other potential holders of assets of listed persons in particular.The names of listed persons are published in the Canada Gazette and on the Public Safety and Emergency Preparedness Canada website, and a range of financial intermediaries are required to conduct monthly checks for a "listed entity" in section 83.11. This covers a significant amount of assets but is not exhaustive of the persons who can "deal, directly or indirectly, in property." The assessment team believes that the enforcement provisions in the criminal code, the RIUNSRT, the UNAQTR and the United Nations Act are relatively difficult to enforce as they require that the Crown prove "knowledge" of a listing, and this is likely to be even more difficult for entities and persons that are not required to undertake monthly checks .

328. Section 83.08(1) and s. 83.03 of the Criminal Code have basically these same provisions for entities defined as a terrorist group or for terrorist activity. The definition of a terrorist group as it applies to the Criminal Code is defined as: (i) an entity that has as one of its purposes or activities facilitating or carrying out any terrorist activity, or (ii) a listed entity, and includes an association of such entities. For the purposes of the Criminal Code provisions property is defined at Section 2 of the Criminal Code and includes real and personal property, funds, financial assets and their substituted property.

329. In addition to the freeze provision, Sections 83.13 through 83.17 permit Canada to seize and forfeit property owned or controlled by Section 83.05 listed entities and property that has been or will be used to facilitate terrorist activity. These provisions can be used cases where assets slip through the section 83.08 freezing net, naturally assuming that the relevant Canadian officials are aware of the forfeitable property and the requisite terrorist nexus. The procedure set forth in Sections 83.13 through 83.17 is a judicial process that very much mirrors the processes set out in forfeiture matters under the Proceeds of Crime provisions located in Part XII.2 of the Criminal Code. This terrorist property seizure and forfeiture regime appears to be in rem and is not conviction-based. The standard of proof in terrorist property forfeitures under Part II.1 is a "balance of the probabilities" test, which is a civil standard. For violations of the RIUNRST and the UNAQTR regulations, the United Nations Act also provides for forfeiture of property dealt with in violation of that Act, and the conviction-based forfeiture scheme set forth in Part XII.2 of the Criminal Code appears to apply to such assets.

Communicating actions taken under the freezing mechanisms and guidance

330. There are several processes that are used to ensure that financial institutions and other individuals and entities are properly notified of a new listing or change to the UNAQTR, the RIUNRST and the Criminal Code. The listing of an individual or entity is published in the Canada Gazette (the official newspaper of the federal government) in conjunction with a press release issued by the Minister of Public Safety and/or the Minister of Foreign Affairs. The Regulations themselves require a continuing monitoring and determination of the existence of property in the possession or control of the institutions. And a failure to undertake the required monitoring is a criminal offence under the regulations and the United Nations Act.

331. To assist financial institutions to search against these listed terrorist names, OSFI, in cooperation with the Department of Public Safety and Emergency Preparedness and the Department of Foreign Affairs and International Trade maintains on its website a database, in various formats, of all terrorist names subject to Canadian laws, including known identifiers for those terrorists. Each time a new terrorist name is listed under Canadian law, or there are changes to existing information, OSFI notifies financial institutions by posting a notification to its website and also notifies all its e-mail subscribers. At the same time OSFI updates the databases with the listing or changes. Since October 1, 2001 OSFI has posted over 90 letters informing financial institutions and the public of updates to the terrorist lists.

332. OSFI also issues a monthly written reminder to federal financial institutions, as well as provincial regulators and SROs that financial institutions are required to file (by the 15th of the following month) a report with OSFI or the appropriate provincial regulator showing, in aggregate, the number of accounts and the dollar value of terrorist property frozen and reported to law enforcement.

333. FINTRAC provides advice and assistance to reporting entities through its website and through the efforts of its Compliance Officers in attending meetings with reporting entities and industry associations. During these outreach sessions and on its website, in particular in its Guideline 5 on Submitting Terrorist Property Reports, FINTRAC refers all reporting entities to OSFI's website, which contains a consolidated list of names.

334. Federally regulated financial institutions, and some other categories of financial institutions[37] are required to determine on a continuous basis whether they are in possession of terrorist property and must report to their regulator on a monthly basis on whether they are in possession of frozen assets. Nil reports are also required. OSFI reminds financial institutions of this obligation every month including their obligations to continuously search their customer names against the OSFI Consolidated List.

335. In addition, federally regulated financial institutions are expected to search their client names against newly listed terrorist names as soon as possible after those new names are posted. If a financial institution discovers terrorist assets it is required to report to the RCMP and CSIS immediately. Reporting entities to FINTRAC must also submit a Terrorist Property Report to FINTRAC if the assets are those of an entity listed under the Criminal Code. It is a criminal offence (section 83.12 of the Criminal Code) to fail to report to RCMP or CSIS.

336. The monitoring systems put in place by financial institutions vary considerably and proper screening against existing lists may take place in some institutions on a monthly basis only. The assessment team believes that this raises some issues of effective implementation of the freezing requirement. In addition, although OSFI provides guidance to federally regulated financial institutions (and forwards its Guidance to provincial regulators and SROs such as IDA in that area, no equivalent measures are in place for other financial institutions, e.g. MSBs, and the DNFBPs (in addition to outreach initiatives and advices and limited guidance provided by FINTRAC). For these entities, the

[37] This does not include MSBs as these entities are not authorised to offer accounts in Canada.

existing communication and guidance is insufficient. This may have an impact on Canada's ability to freeze terrorist funds or other assets without delay.

Publicly-known procedures for considering de-listing requests and for unfreezing the funds of de-listed persons

337. Any Canadian or person in Canada may apply to be delisted. There are clear processes for delisting those entities listed pursuant to the UNAQTR, the RIUNRST and the Criminal Code; (1) on application in writing by a listed individual or entity to the appropriate Minister; and, (2) an applicant may apply to a judge for judicial review of the Ministerial decision.

338. The Minister shall notify the petitioner, within 60 days after receiving the petition, of his or her decision on whether to consider the petition. Within 60 days after the date of receipt of the Minister's decision, the petitioner may apply to a judge for judicial review of the Minister's decision. The regulations or the Criminal Code provide more details of the procedure that has to be followed by the judge when reviewing the Minister's decision.

339. There is a two-year review process for Criminal Code listings by the Minister of PSEPC to ensure accuracy. Delisting procedures for each mechanism are set out in Sections 5.3 and following of the UNAQTR; Sections 2.1 and following of the RIUNRST; and Section 83.05(1) of the Criminal Code. Such procedures are in line with the FATF requirements.

Publicly-known procedures for unfreezing the funds or other assets of persons or entities inadvertently affected by a freezing mechanism

340. Section 5.6 of the UNAQTR, section 10 of the RIUNRST and section 83.07 of the Criminal Code allow for a person or entity to apply for a certificate stating that it is not a listed entity. If it is established that the applicant is not the person or entity referred to under the listing, the Minister has 15 days after receiving the application to issue a certificate.

341. Canadian law enforcement and intelligence agencies have procedures in place to verify identifiers. Verifying identifiers is done through open and classified sources. Full identifiers accompany all domestic listings. Identifiers for individuals may include date of birth, place of birth, country of residence, and address; whereas for entities, a fulsome description is made of the type of activities it engages in and its country of origin. Attempts are made to clarify aliases and alternative spellings of names especially when another country requests that Canada make an addition to its list.

Authorising access to funds or other assets

342. Under the UNAQTR and the RIUNRST, a person whose property has been affected by the freezing, may apply to the Minister for a certificate to exempt property from the freezing procedures if such property is necessary for basic or extraordinary expenses.

343. The Minister shall issue a certificate if the necessity of that property is established with Security Council Resolution 1452 (2002) of December 20, 2002: a) in 15 days after receiving the application if the property is necessary for basic expenses, if the Committee of the Security Council (or the CSC established under Resolution 1267 (19990 OF October 15, 1999, for property frozen pursuant to the UNAQTR) did not refuse the release of the property; and b) in 30 days after receiving the application if the property is necessary for extraordinary expenses, if the release of the property was approved by the Committee of the Security Council. This is set out in Section 5.7 of the UNAQTR and Section 10.1 of the RIUNRST.

344. It is different for property frozen pursuant to the Criminal Code. Pursuant to Section 83.09 of the Criminal Code, the Minister may authorise any person in Canada or any Canadian outside Canada to carry out a specified activity or transaction prohibited by the freezing under the Criminal Code. The authorisation may be subject to any terms and conditions that are required in the opinion of the Minister, including amending, suspending, revoking or reinstating the authorisation. In theory it is

possible to apply to the court to actually seize or restrain the same property. Such an application has never occurred since the provisions amount to an automatic statutory freeze. If the property was seized or restrained pursuant to an order issued under Section 83.13 of the Criminal Code, any person with an interest in the property may apply to have access to it to pay for reasonable living business and legal expenses. However subsection 462.34(6) (b) applies in such cases. The court considering the application must be satisfied that the property is not required for any proceeding. In light of section 83.08 the property is, in fact and law, required for another proceeding, namely the statutory freezing obligation in the criminal law. As a result the section 462.34 process has never been used in a terrorist property case.

Right to challenge freezing measures

345. Sections 5.4 and 5.5 of the UNAQTR, Sections 2.3 and 2.4 of the RIUNRST and provisions in Section 83.05 of the Criminal Code allow for listed entities to apply to a judge for judicial review if the Minister has given it notice that it will remain a listed entity. The judicial review process is stated in these sections and requires that the judge examine the application without delay and provides the applicant with a reasonable opportunity to be heard.

346. If the property was seized or restraint pursuant to an order issued under Section 83.13 of the Criminal Code, any person with an interest in the property may apply to have the property or part of it returned to him/her. In the case of a restraint order, the judge may revoke or vary the order or make the order subject to such reasonable conditions as the judge thinks fit. However no such property has ever been seized or restrained pursuant to a section 83.13 order.

Freezing, Seizing and Confiscation in other circumstances

347. The seizing and confiscation mechanisms as stated in Section 2.3 of the report also apply to cases of FT and terrorist-related funds. In addition to the civil seizure, restraint and forfeiture provisions described above, the normal seizure and restraint provisions for evidence, offence related property and proceeds of crime applies to all terrorist offences established in Part 11.1 of the Criminal Code.

348. For all offences in the Criminal Code, including all terrorism offences in Part 11.1, instrumentalities or, as the concept is described in Canada, “offence related property” provisions apply with the result that all instrumentalities of a terrorist offence are included in the definition. The Criminal Code definition of proceeds of crime, found in section 462.3, also applies to terrorism offences, under either the Criminal Code or as indictable offence in the United Nations Act. Those offences fall within Criminal Code section 462.3’s definition of a designated offence. Finally, it is relevant to consider, for both offence related property and proceeds of crime as they relate to terrorist offences, that the broad definition of “property” in s. 2 of the Criminal Code applies to the search, seizure, restraint and forfeiture provisions.

Rights of bona fide third parties

349. As described above, the UNAQTR, the RIUNRST and the Criminal Code have procedures in place for any person, to make an application to be delisted or to have their property unfrozen.

350. In addition, if the property was seized or restrained pursuant to an order issued under Section 83.13 of the Criminal Code, any person with an interest in the property may apply to have access to it to pay for their reasonable living business and legal expenses, to have the property or part of it returned to him/her. In the case of a restraint order, the judge may revoke or vary the order or make the order subject to such reasonable conditions as the judge thinks fit.

351. Before the forfeiture hearing of property seized or restraint pursuant to the Criminal Code, a judge may require notice to be given to any person who appears to have an interest in the property. Such person shall be entitled to be added as a respondent to the application (par. 83.14(7). If the judge

is satisfied that the person has an interest in the property and has exercised reasonable care to ensure that the property would not be used to facilitate or carry out a terrorist activity and is not a member of a terrorist group, the judge shall order that the interest is not affected by the forfeiture. The order shall declare the nature and extent of the interest in question (par. 83.14(8).

352. There are specific provisions to protect bona fide third party if the property was seized or restraint as proceeds of crime or offence related property.

Monitor compliance with the obligations under SR III and sanctions

353. Federal, provincial and municipal law enforcement authorities are responsible for enforcing the Criminal Code, UNAQTR and RIUNRST. Persons committing offences under these regulations are liable upon conviction to the penalties set out in the United Nations Act.

354. Reporting entities are required to submit Terrorist Property Reports to FINTRAC if they have property in their possession or control that they know is owned or controlled by or on behalf of a terrorist or a terrorist group. FINTRAC refers all reporting entities to the OSFI website, which contains a consolidated list of names. Reporting entities must also put in place policies and procedures that incorporate the verification of lists of terrorists and terrorist entities published in Canada. FINTRAC is responsible to ensure that all reporting entities comply with their AML/CFT obligations under the PCMLTFA and its associated regulations.

355. Section 74 of the PCMLTFA outlines the sanctions that can be imposed on reporting entities on conviction of a summary offence for non-compliance. Reporting entities are subject to fines of up to CAD500 000, imprisonment up to 6 months, or both[38]. Should the same entity be charged with any subsequent summary offence, that entity is liable for a fine up to CAD1 000 000, imprisonment up to 1 year, or both[39]. The PCMLTFA also provides sanctions for a person or entity charged for with an indictable offence for failure to adhere to compliance measures. If a person or entity is charged with an indictable offence for failing to meet compliance obligations, that person or entity is liable for a fine not more than CAD2 000 000, imprisonment for not longer than 5 years, or both[40].

356. Pursuant to section 78 of the PCMLTFA, any officer, director or agent of a reporting entity who directed, authorised, assented to, acquiesced in or participated in the commission of an offence is a party to and guilty of the offence and liable on conviction to the punishment provided for the offence, whether or not the reporting entity has been prosecuted or convicted.

357. Federal and provincial regulators are responsible for ensuring that their regulated financial institutions have procedures in place to continuously monitor and take action against designated entities. Except for OSFI, on-site inspections do not systematically include checks on financial institutions measures to comply with the regulations containing obligations to freeze funds or other assets as well as the prohibition on making funds available to the groups and individuals listed, and the monitoring measures generally are insufficient.

Additional elements

358. Canada has in place some of the measures set out in the Best Practices Paper for SRIII. In particular, there is appropriate communication and co-operation with foreign governments. However, the communication to the private sector, including monitoring of compliance is not sufficient and should be enhanced (with the exception of federally regulated financial institutions supervised by OSFI).

38 PCMLTFA, Section 75 (1)(a)(i).
39 PCMLTFA, Section 75 (1)(a)(ii).
40 PCMLTFA, Section 75 (1)(b).

359. As of December 2006, there has not been a request to free up frozen funds for basic or extraordinary expenses under the RIUNRST or the UNAQTR.

Statistics

360. This table shows the number of Listed Persons and Entities (as of December 2006):

UNAQTR	477
RIUNRST	36
Criminal Code	40

361. This table shows the number of Terrorist Assets Frozen in Accounts:

Date	N° of accounts	Total CAD
November 2001	28	360 000
February 2002	44	460 000
June 2002	16	350 000
September 2002	17	355 000
December 2002	15	335 000
April 2003	17	340 000
September 2003	17	340 000
March 2004	13	181 000
October 2004	14	144 000
April 2005	15	126 000
September 2005	7	68 800
August 2006	10	186 300

2.4.2 Recommendations and Comments

362. There needs to be more communication on listed persons provided to certain categories of financial institutions and other potential asset holders as well more clear and practical guidance to reporting entities (including DNFBPs and MSBs) that may be holding targeted funds or other assets concerning their obligations in taking action under freezing mechanisms. This would assist the private sector to understand the process to follow and the action to take in such cases (this does not apply to those types of institutions that already receive specific guidance, as noted above).

363. Canada should enhance the existing measures to monitor the compliance with the legislation governing the obligations under SRIII (except for federally regulated financial institutions supervised by OSFI).

2.4.3 Compliance with Special Recommendation III

Rec.	Rating	Summary of factors underlying ratings
SR.III	LC	▪ The actions taken to communicate the names of listed persons or entities do not cover all types of financial institutions and the lists are not effectively communicated to other types of asset holders. ▪ With the exception of guidance given to federally regulated financial institutions (and copied to provincial regulators/SROs), Canada has issued insufficient guidance to other financial institutions and DNFBPs that may be holding funds of other assets concerning their obligations in taking action under freezing mechanisms. This may have an impact on Canada's ability to freeze terrorist funds or other assets for such entities without delay; ▪ The existing measures to effectively monitor the compliance with the legislation governing the obligations under SRIII are insufficient (except for federally regulated financial institutions supervised by OSFI).

2.5 The Financial Intelligence Unit and its functions (R.26 & 30)

2.5.1 Description and Analysis

Recommendation 26

Functions and responsibilities of the FIU

364. *General.* Canada has established the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC) as a national centre for receiving, analyzing and disseminating information concerning suspected money laundering or terrorist financing. The Canada FIU was created in 2000 under the Proceeds of Crime (Money Laundering) Act. FINTRAC's mandate was expanded to include the detection and deterrence of the financing of terrorism and other threats to the security of Canada in 2001 when FINTRAC's enabling legislation was amended and became the PCMLTFA.

365. FINTRAC is an 'administrative' FIU, meaning it does not have investigative powers. FINTRAC is an independent agency that acts at arm's length (it receives no explicit direction) from the recipients of its information and reports its activities to the Parliament of Canada through the Minister of Finance.

366. In addition to its core FIU functions, FINTRAC has a mandate to ensure compliance among financial institutions and other reporting entities with Canada's AML/CFT legislation and regulations (see Section 3.10 of the Report) and promote public awareness of money laundering and terrorist financing issues.

367. *Receiving disclosures of STRs and other types of reports*. FINTRAC receives from reporting parties the following types of reports:

- Suspicious transaction reports related either to money laundering or to terrorist activity financing regardless of dollar value (STRs).
- Terrorist property reports that report the existence of terrorist property in their possession or control, or information about a transaction or proposed transaction in respect of such property (TPRs).
- Large international electronic funds transfer reports involving CAD10 000 or more (EFTRs)[41].
- Large cash transaction reports of CAD10 000 or more (LCTRs).

368. In addition, CBSA provides the following reports to FINTRAC on behalf of individuals, and any entity who is importing or exporting currency or monetary instruments of CAD10 000 or more:

- Cross-border currency or monetary instruments reports (CBCMIRs) involving movements of CAD10 000 or more in currency or monetary instruments.
- Cross-border currency seizure reports (CBCSRs).

[41] Only financial entities, MSBs and casinos are required to report EFTRs.

369. In addition to the reports received from obligated reporting entities, FINTRAC receives information concerning suspicions of money laundering or terrorist financing voluntarily from the general public and various other sources, including law enforcement agencies, CSIS, CBSA, CRA and foreign FIUs. This additional information, referred to as 'voluntary information' or 'VIR', is included in FINTRAC's data holdings and is available to assist in its analytical work. FINTRAC provides acknowledgement of voluntary information received from law enforcement, CBSA, CRA and CSIS within approximately four weeks of its receipt through the delivery of response letters[42]. FINTRAC has received and continues to receive a significant amount of voluntary information from law enforcement and CSIS relating to both money laundering and terrorist activity financing (more than 2,500 voluntary reports since 2001).

370. *Conducting analysis of disclosures of STRs and other types of reports*. To assist in the analytical process, FINTRAC has developed policies and procedures, which identify criteria to be considered in the selection of cases for further analysis and provide guidance in determining that cases have met the legally prescribed disclosure threshold.

371. Once a case has been assigned to an analyst, that person will review and assess the information available to all the analysts (transactions, voluntary information, data from commercial and law enforcement databases, registries of companies, registries of personal property, business profile and open sources[43]) to identify and verify linkages between transactions, people and entities that may be indicative of money laundering and terrorist financing.

372. Once analysis demonstrates that there are reasonable grounds to suspect that the financial activity would be relevant to a money laundering or terrorist activity financing investigation (see below description in "*Disclosing intelligence*"), the analyst prepares the following: (1) an 'analytical report' that provides a description of the case, the analysis that took place, and sets out the rationale for disclosure; (2) a link analysis chart, a visual depiction of the linkages between key transactions, individuals and businesses; (3) a compilation of all relevant publicly available information that the analyst has used in developing the case; and (4) a 'disclosure statement' which sets out the 'designated information' that will be provided to the disclosure recipient. Additional detail on the 'designated information' that FINTRAC is able to disclose is provided below in '*FINTRAC disclosures'*.

373. The analytical report and disclosure statement go through a series of vetting and management approvals before a recommendation is presented to the FINTRAC Disclosure Committee, a FINTRAC Committee consisting of senior management representatives[44] that makes a recommendation to FINTRAC's Director concerning whether cases should be disclosed (*i.e.* whether the case meets the disclosure threshold) and if so, to whom (*i.e.* what is the appropriate police force or other agency in each case). Ultimately, it is the Director that approves disclosures. This review and approval process ensures that, prior to disclosing information, FINTRAC is satisfied that it has met two fundamental criteria. First, that the legislative threshold to disclose has been met and, second, that the information provided is what is allowed under the legislation. This threshold and the list of information that may

---

[42] If FINTRAC's preliminary analysis of the information shows that there is insufficient information to warrant a more comprehensive analysis, FINTRAC issues a letter indicting that FINTRAC is not currently in a position to communicate designated information and provides confirmation that the voluntary information has been incorporated into FINTRAC's database. If the preliminary analysis shows that there is sufficient information to warrant a more comprehensive analysis, FINTRAC will advise the provider, in writing, that FINTRAC is proceeding with the analysis of the information. If FINTRAC meets its threshold for disclosure following a more comprehensive analysis, it will disclose information to the provider of the voluntary information. If the threshold is not met, FINTRAC will follow up by sending the information provider a 'negative response' letter.

[43] 'Open source' refers to information that is available from sources that can be accessed by everyone such as the Internet, media articles etc.

[44] Currently, FINTRAC's Disclosure Committee consists of: the Director, all Deputy Directors, Assistant Directors (some on a rotational basis), Legal Counsel (in an advisory role) and any other persons appointed by the Director.

be provided are set out in sub-Sections 55(3), and 55(7), 55.1(1), 55.1(3), 56.1(1) and 56.1(5) of the PCMLTFA. However given the variety of circumstances seen in money laundering and terrorist financing schemes, FINTRAC makes its decision to disclose on a case-by-case basis.

374. All cases that culminate in a disclosure are coded and entered into a disclosure database. This also allows for the maintenance of a running tally of disclosures made to disclosure recipients. In addition, analysts entering case information check the original disclosure information for any inconsistencies or errors in logging or detailing case information. The assessment team was told that this database is also queried on every case opened by an analyst, which allows FINTRAC to link new cases to previous disclosures and potentially provide secondary or "follow-up" disclosures to law enforcement.

375. The time required to complete a disclosure will vary based on the complexity of the case. For complex disclosures that include thousands of transaction reports, more time is obviously necessary for FINTRAC to complete analysis of such cases. The assessors were told that FINTRAC has disclosed urgent cases in less than 48 hours (see further comments on effectiveness).

376. FINTRAC's case analysis can have a variety of starting points. In most cases, the initiator for a case to be developed is one particular information source. The majority of FINTRAC cases disclosed have been built with information contained in voluntary information provided by law enforcement, CSIS, or the public. In 2005/2006, queries submitted by foreign FIUs (FIUQs) were also frequent case originators. It is cross-referenced against all financial transaction and other data held by FINTRAC to identify transactions or patterns of transactions that may be indicative of money laundering or terrorist financing. Cases also originate from other sources such as STRs or open source information. However, the number of these types of cases has declined as the number of voluntary information reports from law enforcement have increased (see comments below on effectiveness).

377. *Disclosing intelligence*. Under the PCMLTFA, FINTRAC is authorised to disseminate financial information to domestic authorities for further action when it has reasonable ground to suspect that the information would be relevant and useful to the investigation or prosecution of a money laundering or terrorist activity offence. The following summarizes the various agencies that FINTRAC discloses to, and under what circumstances:

- Where FINTRAC has reasonable grounds to suspect that designated information would be relevant to investigating a money laundering or a terrorist activity financing offence, FINTRAC must disclose this information to the appropriate police force[45].
- Where there are reasonable grounds to suspect that designated information would be relevant to threats to the security of Canada[46], FINTRAC must disclose designated information to CSIS.
- FINTRAC also discloses to the CRA or the CBSA under certain circumstances. For these disclosures, FINTRAC must meet a dual test. First, FINTRAC must suspect that the designated information will be relevant to investigating or prosecuting money laundering or terrorist activity financing offence and then, for example, if FINTRAC also determines that the information is relevant to tax evasion, FINTRAC must disclose to CRA. Similarly, once the first test is met, and FINTRAC also determines that the information is relevant to determining if a person is inadmissible or relevant to certain offences under the *Immigration and Refugee Protection Act* or to the evasion of customs taxes or duties, FINTRAC must disclose to the CBSA.
- When FINTRAC has reasonable grounds to suspect that designated information would be relevant to the investigation or prosecution of a money laundering or terrorist financing

[45] PCMLTFA, 55(3).

[46] 'Threats to the security of Canada' is defined in the *Canadian Security Intelligence Service Act*, Section 2.

offence or a substantially similar offence, FINTRAC also has the authority to disclose information to foreign financial intelligence units with which it has entered into a Memorandum of Understanding (MOU) to govern such exchanges (see additional information about FINTRAC's international cooperation in Section 6.5 of the report).

378. FINTRAC analysts use a variety of indicators from a number of sources to determine whether a transaction is related to money laundering or terrorist financing (including indicators developed by the reporting entities themselves). FINTRAC has developed a reference guide of indicators with input from law enforcement units. However, the assessment team was told that these indicators are solely based on typologies and indicators issued by the FATF; the Egmont Group as well as AML guidelines issued by a number of FIUs to their reporting entities. They are not based on ML/TF trends developed by FINTRAC itself. Furthermore, a list of 13 of these indicators has been disclosed to the assessment team. In the assessment team's views, this list spots relatively basic and unsophisticated indicators.

379. During the on-site visit, the assessors were told by a law enforcement agency that FINTRAC may occasionally disclose ML/CF cases to the wrong police authority, which may delay the course of the investigation though FINTRAC indicated that it had never heard of such a case.

FINTRAC Disclosures

380. As stated previously and as set out in sub-Sections 55(7), 55.1(3) and 56.1(5) of the PCMLTFA, the information that FINTRAC can provide to a disclosure recipient is referred to as "designated information". The designated information includes key details that identify individuals or entities and their financial transactions. Designated information provided in FINTRAC's case disclosures includes any or all of the following:

- Name and address of company(ies) involved in the transaction(s).
- Name, address and type of business where the transaction(s) occurred.
- Location, date and time of the transaction(s).
- Type and value of the transaction(s) including the amount and type of currency or monetary instruments involved.
- Transaction, transit and account number(s).
- Name of importer or exporter, in the case of importation or exportation of currency or monetary instruments.
- Name and alias of person(s) involved in the transaction(s).
- Address of person(s) involved in the transaction(s).
- Date of birth.
- Citizenship.
- Passport, record of landing or permanent resident card number.

381. Disclosures may also contain publicly available information about transactions, persons or entities contained in the report as well as a visual display highlighting relevant linkages and money flows.

382. The decision to provide police and other recipients with designated information only when FINTRAC reaches its threshold, rather than to provide unrestricted access to FINTRAC's data holdings, reflects the fact that FINTRAC receives a large amount of varied financial information on persons and entities, the vast majority of which is legitimate and not relevant to any investigation or prosecution. By having FINTRAC disclose designated information, under specific circumstances (reaching the disclosure threshold), the assessors were told that lawmakers have struck a balance between the needs of police and other recipients to pursue ongoing and new investigations, and the privacy rights of Canadians guaranteed under the Canadian Charter of Rights and Freedoms. Instead of providing direct access to its data holdings, FINTRAC discloses cases that provide new leads to law enforcement authorities and other partners, either in support of ongoing investigations or in support of other intelligence related to new investigative targets.

383. Although delineating designated information assists in protecting the privacy of Canadians, the 2004 Report of the Auditor General of Canada and the Year Five Evaluation of the National Initiatives to Combat Money Laundering and Interim Evaluation of Measures to Combat Terrorist Financing, stated that the effectiveness of FINTRAC disclosures was limited by legislative restrictions that constrain the information that can be disclosed. This was seen to have a direct impact on law enforcement ability to effectively investigate ML and TF cases.

384. The two above-mentioned reports encouraged the government to re-examine the list of designated information and identify potential additions to the list with the objective of expanding the information available in FINTRAC disclosures while continuing to respect the privacy and Charter rights of Canadians. Designated information was enhanced as a result of amendments to the PCMLTFA which came into force on June 30, 2007. Since that date, FINTRAC may disclose the following, in addition to the original list of designated information identified above:

- The existence of pending criminal charges or of criminal records of the parties involved in or related to any transaction.
- The relationship or association of any person or entity to a corporations or any other entity referred to in the disclosure, if the transaction was/were made on behalf of a corporations or other entity.
- The name, address and telephone number of each partner, corporate director or officer of a corporation or other entity, its business number and its place of business, or principal location of activities.
- Whether the parties referred to in the disclosure have any beneficial or financial interest in the partnership, corporation or other entity.
- In disclosures where more then one person is involved in, associated with, or related in any manner to the money laundering and/or terrorist financing activity, the principal or controlling entity or individual involved in or related to the money laundering and/or terrorist financing activity.
- The number and type of reports or types of information a disclosure is based on.
- The number and type of reporting entities who filed the reports.
- A summary of indicators (*e.g.* rapid movement of funds and transactions inconsistent with customer profile).
- The reporting entity's reason for submitting a suspicious transaction report to FINTRAC.

385. *Production Orders*. When law enforcement or CSIS want additional information from FINTRAC that is not included in a case disclosure of designated information, they may seek a court order, which requires FINTRAC to provide them with additional information. In most cases, a production order will be served on FINTRAC after an initial disclosure has been made; however, under the Act, a disclosure of designated information is not a precondition to a production order.

386. A production order may include the transaction reports (STRs, LCTRs, etc,) and the case analysis report, which contains the facts on which the analysis is based, the detailed reasons for suspecting money laundering or terrorist financing (the rationale for disclosure), and any other information named in the order. These facts are gathered from the financial transaction reports received and publicly available information, among other sources. To get a production order, the police must satisfy a judge that there are reasonable grounds to believe that a money laundering or terrorist-activity financing offence has been committed by the person in respect of whom the police are seeking information or that that person has benefited from such an offence. In addition, the police must satisfy the judge that the information that they are seeking is likely to be of substantial value to the investigation of the offence. The judge may then issue a production order requiring FINTRAC to permit the police officer named in the order to examine, or be provided certified copies of, all information and documents described in the court order, subject to conditions the judge considers advisable in the public interest.

387. To date, FINTRAC has been served with only 14 production orders from law enforcement. Law enforcement authorities cite two basic reasons for the reluctance to apply for production orders. One is that the legislative threshold is high, the same as for a search warrant: the applicant must satisfy the court that there are "reasonable grounds to believe" an offence has been committed. A search warrant is preferable because it provides direct access to target information that could be used as evidence. Second, the information contained in FINTRAC disclosure is generally considered below the legislative threshold that a production orders requires.

Guidance on reporting

388. FINTRAC provides comprehensive guidance to reporting entities regarding the manner of reporting and the procedures that should be followed when reporting. FINTRAC has defined very structured reporting forms for STRs, LCTRs, EFTRs and CBCMIRs.

389. In order to ensure that FINTRAC is able to receive and process large volumes of reports quickly and efficiently, a mandatory requirement was established in the PCMLTFA Regulations, requiring reporting entities to submit reports electronically to FINTRAC when the sender 'has the capacity to do so'[47]. Today, approximately 99.9% of all reports are submitted electronically.

390. Given the IT requirements for submitting reports, FINTRAC works very closely with reporting entities, particularly the larger ones, with respect to the development and implementation of technical specifications. To assist with this, FINTRAC has created and hosts regular meetings of a technical support group for technology specialists within some of the major reporting sectors, to act both as a consultative body and to ensure that technical questions and issues on reporting to FINTRAC are addressed and communicated within the group. FINTRAC also developed and provided the software to reporting entities to allow them to encrypt and transmit batch files to FINTRAC.

391. In February 2006, FINTRAC launched an updated secure online report capture system, F2R, that provides reporting entities with a reliable mechanism to file reports through the Internet. This tool further facilitates the reporting of financial transactions for the many individuals and businesses that are obliged to do so under the PCMLTFA. This newly implemented reporting system has also been designed to increase data quality through new functions which return LCTRs and EFTRs to reporting entities for revision (*RRFA: Reports Return for Further Action*) when the required information is not included in the report. The new reporting system also has built in controls to ensure that more complete reports are provided to FINTRAC through the implementation of automatic, immediate error messages that go to reporting entities concerning any errors made in specific fields of their submitted transaction reports. The system does not accept the reports if certain key fields are not completed.

392. The assessment team believes that such IT tools can generate positive outcomes. However, during the on-site visit, the assessors were told on several occasions by reporting entities that the format of reporting forms is somewhat too rigid and reduces the capacity to communicate a maximum level of information. FINTRAC indicated to the assessment team that reporting entities were consulted during the development of the new reporting system in order to offer a product that meets reporting entities expectations and needs as well as FINTRAC's requirements. FINTRAC has also worked closely with reporting entities to explain the importance of including a clear and complete description of events and reasons for suspicion in the narrative portion of the form (section G), which has no space limitation.

[47] A reporting entity needs only have basic information technology infrastructure, such as a PC and connection to the Internet in order to be able to report electronically to FINTRAC.

Access to information

393. FINTRAC now has over 45 million reports in its data holdings, and data holdings continue to grow at the rate of approximately 15 million reports each year. All of the data on these reports is available for analysis within FINTRAC.

394. FINTRAC analysts have ongoing, direct access to many different commercially and publicly available databases (*e.g.* Registries of companies, Registries of Personal Property, and Business Profiles), as well as the Internet.

395. Under the PCMLTFA, FINTRAC has authority to collect information from databases maintained for law enforcement or national security purposes and in respect of which an agreement is entered into. FINTRAC currently has access to two major national police databases.

396. The first database is a computerized system that provides tactical information about crimes and criminals. It is an integral part of the RCMP's National Police Services (NPS) as it is the only national information-sharing system that links criminal justice and law enforcement partners across Canada and internationally. This database is responsible for the storage, retrieval and communication of shared operational police information to all accredited criminal justice and other agencies involved with the detection, investigation and prevention of crime. This database has been operational since 1972, and is located in the RCMP Headquarters complex in Ottawa, Ontario. It allows for over 80 000 law enforcement officers to connect to the central computer system within 3 185 police departments, RCMP detachments, and federal and provincial agencies across the country. This system has four data banks, Investigative, Identification, Intelligence and Ancillary (containing information not found in the other categories), which includes files and information such as: vehicles, persons and property.

397. The second database is the RCMP's automated information management system used to store, update and retrieve information on operational case records/occurrences being, or having been, investigated. This electronic indexing system is used by the RCMP operational units, some municipal police agencies, by Firearms Officers (FO) across Canada, and by other federal partners. The database captures data on individuals who have been involved in investigations under the Criminal Code, federal and provincial statutes, municipal by-laws and territorial ordinances. According to the RCMP, in addition to details of an event in a brief synopsis, the database contains limited information relating to investigations and criminal histories. Unlike the first database, which essentially contains factual information (*e.g.* charges and convictions), this database may also contain information provided by witnesses, victims and other associated subjects that can be highly subjective, as well as the names of the witnesses, victims, and acquaintances of the accused individual. It also contains information on occurrences and incidents that never resulted in charges.

398. FINTRAC continues to work with law enforcement and national security partners to identify databases, assess FINTRAC's interest in their content and if appropriate develop agreements for access.

399. FINTRAC has dedicated staff (Law Enforcement Liaison Officers) that are responsible for liaising and maintaining a relationship with FINTRAC's law enforcement partners. These liaison officers are responsible for delivering FINTRAC's disclosures to and obtaining feedback about these disclosures from law enforcement. They also facilitate law enforcement's provision of voluntary information to FINTRAC.

400. FINTRAC does not have access to information on the income of suspects of money laundering or terrorism financing activities. FINTRAC has no authority under the PCMLTFA to collect information from the CRA. FINTRAC has no direct or indirect access (i.e. cannot query) to databases maintained by the CSIS, which can provide information on suspects of terrorism financing activities, nor to databases maintained by the Canadian Customs Agency. However the assessment team was told that CSIS provides FINTRAC with general analysis of threats to the security of Canada that can help FINTRAC to analyze the reports it receives.

401. FINTRAC must rely on voluntarily information provided by the law enforcement authorities to carry out the analysis of the reports it receives. When receiving and analysing such reports, FINTRAC does not ask information directly or via its liaison officers to specific or local law enforcement agencies but limits itself to collect information from the two available law enforcement databases that are not fully integrated and not entirely complete.

Additional information from reporting parties

402. FINTRAC is not allowed by the PCMLTFA to ask additional financial information from reporting entities at the analytical stage. FINTRAC can return STRs to reporting entities because of missing information or other errors (*e.g.* some fields in the electronic form are not completed. Since the adoption of the secure online report capture system (F2R), this process has become more formalized and systematic under the "Reports Returned for Further Action" or RRFA. RRFAs are returned by FINTRAC to reporting entities that must complete insufficient data. Once the reporting entity has made the corrections required (*i.e.* has completed the missing field(s)), the STR is forwarded back to FINTRAC. However, at this stage, no substantive analysis of the report has been made yet. Therefore FINTRAC can only ask reporting parties to supplement an incomplete report but cannot obtain from the reporting entities additional information during the analytical process (for instance, FINTRAC cannot ask the reporting entity about other financial operations carried out in that institution by the same person which are not covered by the report but knowledge of which could help in fully understanding the ML mechanisms they might be using). Canada has advised that Section 8 of the Charter that sets out that "everyone has the right to be secure against unreasonable search and seizure" would not allow FINTRAC to request additional financial information to the reporting entities.

403. The assessment team was told that the legislated reporting requirements were developed in such a way as to ensure that FINTRAC has a broad and detailed amount of transaction information to link suspect transactions and develop intelligence products for the police forces and others. FINTRAC also relies on additional information from reporting entities it can get through other types of reports than STRs (*i.e.* its compliance work as well as from commercial databases and publicly available information).

404. The Suspicious Transaction Report includes a wide range of fields to be complete by the reporting entities (certain fields are mandatory – for all other fields the reporting entity has to make reasonable efforts to get the information). The report has been built by FINTRAC to oblige the reporting entities to provide FINTRAC with as many information as possible on the suspicious financial transactions (multiple suspicious transactions can be reported simultaneously) and the suspects of money laundering or terrorist financing activities. Amongst other things, mandatory fields on how the transaction was initiated (where the money came from) and on the disposition of the funds (where the money went) are included in the report. With respect to STRs, special attention is given to the section of the report dealing with the description of the suspicious activity regarding a transaction (Section G). The ideal response clearly and completely describes the factors or unusual circumstances which led the reporting entity to a suspicion of money laundering or terrorist financing, and provides as many relevant details as possible.

405. However, the assessment team does not consider such mechanisms sufficient to meet the FATF requirement. The current legal framework does not permit FINTRAC to go back at reporting entities to ask for additional potentially relevant information available within the financial sector. As FINTRAC has no authority to obtain additional financial information from the reporting entities, law enforcement authorities may be provided with incomplete pictures of the suspicious ML/TF cases, *i.e.* a partial description of the financial information.

Operational independence and autonomy

406. The PCMLTFA established FINTRAC as an independent agency and, as such, FINTRAC has a high level of operational independence and does not take direction concerning day-to-day operations from any external parties. The Director is appointed for a 5-year term, has supervision over, and direction of, FINTRAC's work and employees, and may exercise any power and may perform any duty or function of FINTRAC.

407. The Minister of Finance is responsible for FINTRAC and may direct FINTRAC on its strategic direction or matters that affect public policy. Similarly, the Director is required to keep the Minister informed of any matter that could materially affect public policy or the strategic direction of FINTRAC. The PCMLTFA prohibits the Director from disclosing any information to the Minister that would directly identify an individual who provided a report or information to FINTRAC, or a person or entity about whom a disclosure was provided by FINTRAC under the PCMLTFA.

408. In addition, FINTRAC is mandated to operate at arm's length from those to whom it discloses information and FINTRAC cannot take direction from police forces or other agencies that it discloses to.

Protection of the information

409. Information held by FINTRAC is securely protected and is disseminated only in accordance with the PCMLTFA. FINTRAC has a legislated mandate to ensure that personal financial information in its possession is protected and remains confidential. This piece of its mandate guides every aspect of FINTRAC's operations.

410. The PCMLTFA upholds the principles outlined in the Canadian Charter of Rights and Freedoms and the Privacy Act, and contains significant provisions specifically designed to protect the privacy of individuals.

411. FINTRAC employs a robust integrated security program that incorporates state of the art technology including both smart cards and biometric technology to control physical and computer access. Continuous improvement and vigilance of physical and electronic security systems ensure that FINTRAC maintains a high standard of information protection[48].

412. When delivering domestic disclosures, all information is handled in a highly secure manner. A FINTRAC Law Enforcement Liaison Officer hand delivers all outgoing disclosures to the appropriate law enforcement or intelligence agency recipient. The disclosure package is presented in both paper and electronic format to facilitate use by the receiving agency. All disclosure activity is logged, whereby the recipient signs for receipt of disclosures and both parties retain a receipt for their records. This process is practiced on a consistent basis and adheres to the Government of Canada's "Security Policy".

413. The protection of information is a paramount consideration in the decision to enter into an agreement with a foreign FIU for the exchange of information. As required by the PCMLTFA, these agreements contain specific provisions that commit those organizations to protect the information, to use it only for purposes related to the investigation or prosecution of money laundering or terrorist activity financing offences (or substantially similar offence), and to treat the information in a confidential manner. Further disclosure of the information to a third party is done only with FINTRAC's explicit consent. Disclosures to foreign FIU are made via the Egmont Secure Web (a

[48] For instance, all employees must obtain 'Top Secret' security clearance as a condition of employment. Staff operate under the 'need to know' principle, meaning that staff has access only to information they require in order to perform their specific duties. Measures to control physical access to FINTRAC offices include security staff, high security locks, electronic access control, closed circuit monitoring, electronic intrusion detection and monitoring.

secure communications channel used by most Egmont-member FIUs) or more secure means, if necessary.

Periodic reports

414. Part of FINTRAC's mandate is to enhance public awareness and understanding of matters related to money laundering and terrorist financing activity. Subsection 72(1) of the PCMLTFA requires the Director to prepare and submit on or before 30 September of each year an annual report on the operations of FINTRAC for the preceding year to the Minister of Finance. Subsequently, the Minister tables the report in Parliament.

415. FINTRAC's Annual Report contains a range of information regarding financial transaction reporting statistics, agency highlights, staffing matters, future priorities and performance summaries. FINTRAC has released Annual Reports since 2002. FINTRAC's Annual Report has evolved over its five publications. In the 2005 Annual Report, FINTRAC provided a sanitized money laundering case in an effort to further enhance the public's understanding of money laundering and FINTRAC's role in detecting it. In 2006, before Parliament, FINTRAC provided detailed televised testimony, on FINTRAC's business flow and how it produces financial intelligence. This material has subsequently been published on FINTRAC's website and replicated in the 2006 Annual Report, in order to reach a wider audience.

416. The Annual Report 2006 provides the following statistical tables: reports received by fiscal year and type; suspicious transaction reports by sector; disclosures and value of transactions; number of reporting entities represented in disclosures; percentage of case disclosures supported by each type of report; regional distribution of money laundering case disclosures; and agreements with foreign FIUs. With regard to ML/TF trends, it describes trends that FINTRAC has observed with respect to drug and fraud-related cases. One complex sanitized case is also presented that includes: description of the facts; a brief summary of the result of the case (such as number of arrests); where appropriate, a description of the inquiries made by the FIU; and, lessons learned. However, the assessment team believes that the FINTRAC Annual Reports could provide more statistical information (such as for instance the number of STRs sent to law enforcement authorities), typologies and ML/TF trends related information considering the number of ML/FT cases FINTRAC annually deals with and the amount of information FINTRAC at its disposal (out of 45 pages of the annual report 2006, only 12 pages are dedicated to statistical information, typologies and ML/TF trends). This is to be linked to the need for FINTRAC to improve its capacity to produce typologies works and studies on ML/TF trends in Canada.

Egmont Group membership

417. FINTRAC became a member of the Egmont Group in June 2002. Since that time it has participated actively in many of its activities, committees and working groups. Currently, FINTRAC's Director holds a seat on the Egmont Committee as Vice-Chair and is Chair of the Information Technology Working Group.

Egmont Group Statement of Purpose and its Principles for Information Exchange Between Financial Intelligence Units for Money Laundering Cases

418. FINTRAC takes into account both the Egmont Group Statement of Purpose and its Principles for information Exchange between Financial Intelligence Units[49].

[49] The Egmont principles stipulate that FIUs should be able to exchange information freely with other FIUs on the basis of reciprocity or mutual agreement and consistent with procedures understood by the requested and requesting party.

Recommendation 30 (Resources)

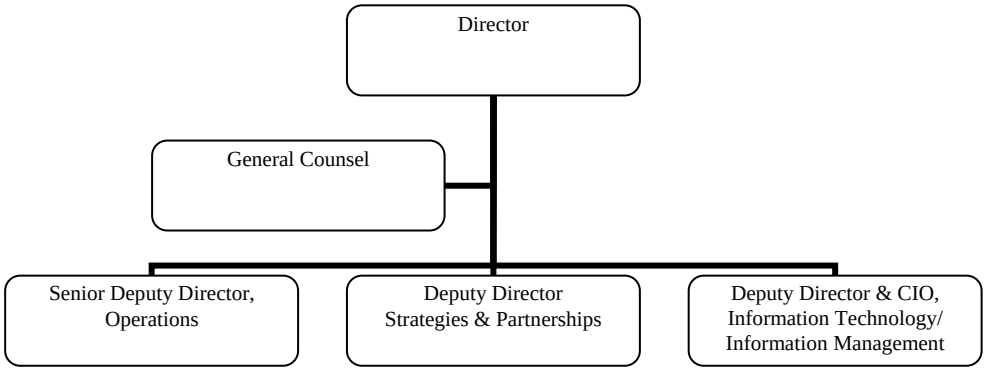
General

419. In 2000, FINTRAC was established as Canada's FIU with an initial annual budget of approximately CAD18 million and 70 employees. In 2001, FINTRAC was given additional responsibilities for combating terrorist financing as part of the Anti-terrorism Act, and the budget was increased to CAD42 million. In the 2006 Budget, the Government announced its priority to bolster existing capacity to combat money laundering and terrorist financing by providing incremental resources to the AML/CFT regime, including an additional CAD16.2 million and 102 employees to FINTRAC. The following table outlines FINTRAC's past, current and planned annual budget.

	2000-01	**2001-02**	**2002-03**	**2003-04**	**2004-05**	**2005-06**	**2006-07**	**2007-08**
Full-Time Employee (FTE)	70	135	150	189	184	180	265.4	271
Total Funding FINTRAC (CAD '000)	17 985	36 093	42 158	33 255	32 003	33 973	51 081	49 839

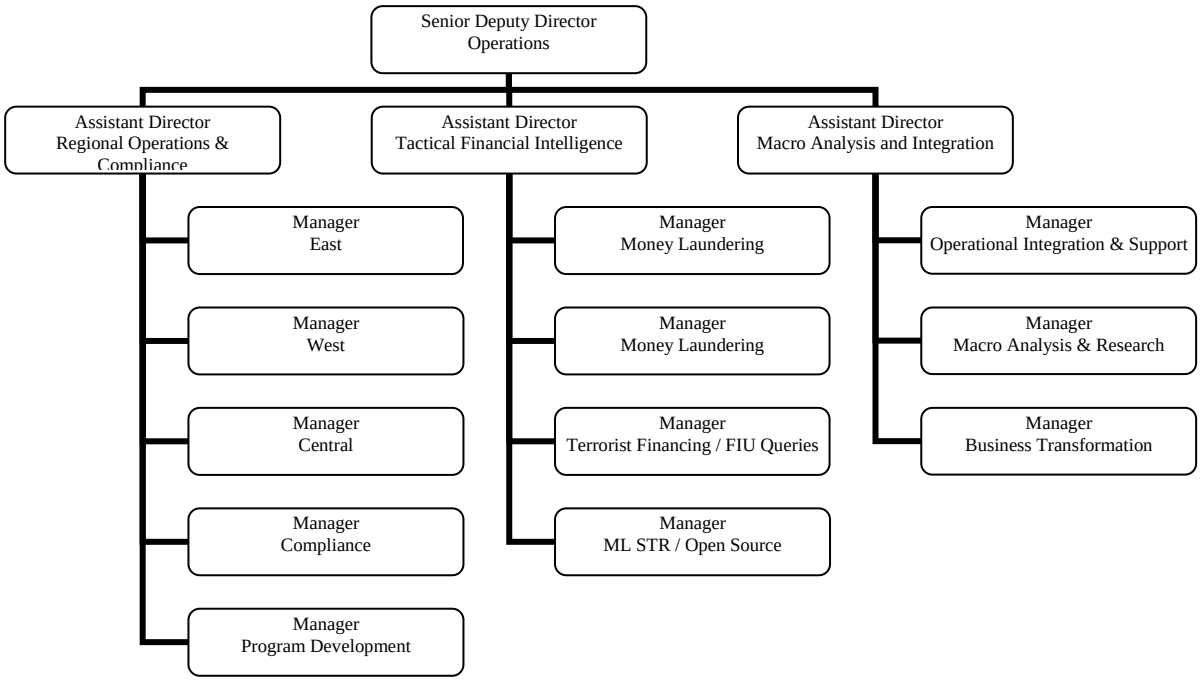
420. FINTRAC has three regional offices (Western, Central, and Eastern)[50] of approximately ten staff each with responsibilities for the various aspects of the national compliance program (policy interpretation, reporting entity assistance, risk assessment and examinations, data quality, timing and volume, reporting entity feedback and disclosures of non-compliance to law enforcement) as well as for liaison with law enforcement agencies (delivery of disclosures, receipt of voluntary information, and relationship management).

FINTRAC's Organizational Chart



421. *Operations Sector*. The Operations Sector (117 employees) is responsible for detection and deterrence activities with the support of the following three functions: Regional Operations and Compliance (ROC), Tactical Financial Intelligence (TFI) and Macro Research and Integration (MAI).

[50] Western – located in Vancouver, covers British Columbia, Alberta, Saskatchewan, and the Yukon; Central – located in Toronto, covers Ontario Manitoba, the Northwest Territories and Nunavut; Eastern – located in Montreal, covers Quebec, New Brunswick, Nova Scotia, Prince Edward Island and Newfoundland and Labrador.

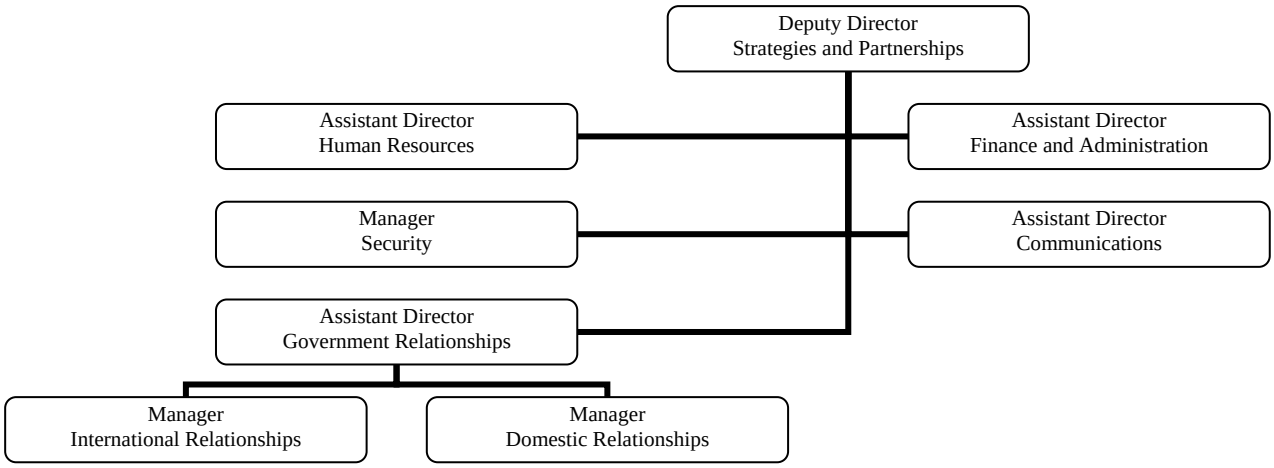


422. Regional Operations and Compliance (49 employees) is responsible for interpreting policy and regulations, providing advice and assistance to reporting entities; conducting risk assessment and examinations; monitoring data quality and volume; providing feedback to reporting entities; making disclosures of non-compliance to law enforcement; conducting regional liaison with disclosure recipients; and developing and implementing new programs.

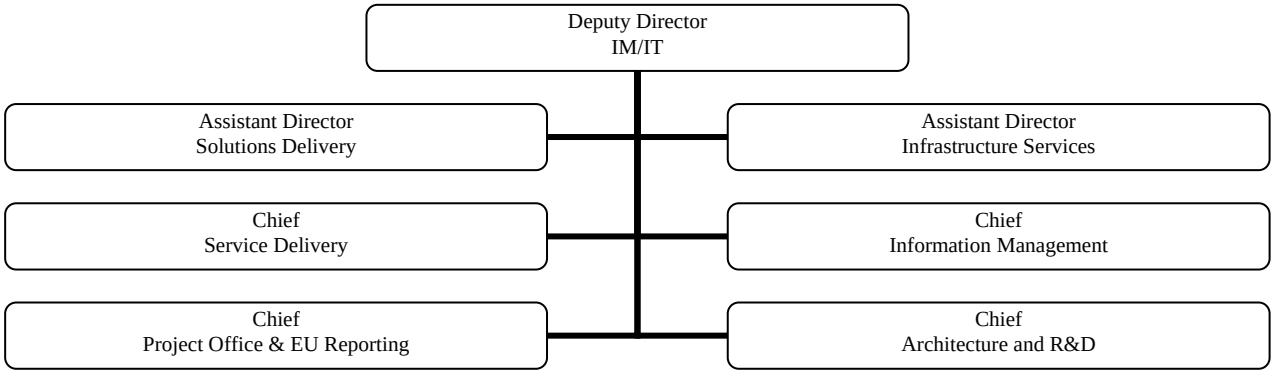
423. Tactical Financial Intelligence (36 employees) is responsible for developing cases and FINTRAC's disclosures. The Tactical Financial Intelligence Unit comprises four units. Three units are dedicated to the analysis of ML cases and the fourth unit deals with terrorist activity financing cases as well as FIU queries. The three ML units are structured to ensure FINTRAC's disclosures are provided in a most timely fashion. For example, one ML unit is set up to deal with the less complex cases. These cases often have fewer transactions and can be analysed within a short time frame and disclosed quickly. The second ML unit deals with more complex cases. This allows analysts to spend the necessary time on the preparation and analysis of these cases to ensure they are worked on immediately and disclosed in a timely manner. The third unit is set up to deal with cases generated by STRs and open source or media articles. The TF unit deals entirely with terrorist activity financing and threats to the security of Canada cases as well as with any queries FINTRAC receives from other FIUs. There is a manager in charge of each unit and a total of 36 analysts handle the workload.

424. Macro Analysis and Integration (29 employees) is responsible for operational integration and support (including handling of Voluntary Information and disclosures, and support on production orders), macro analysis and research (statistics and reports to support FINTRAC's operations, research and exploit available macro level information sources) and business transformation (i.e. development and review of business processes within Operations Sector and the development of user requirements in support of new systems development).

425. *Strategies and Partnerships Sector*. The Strategies and Partnerships Sector (63 employees) manages the key relationships that FINTRAC has with domestic and international partners, and is the primary conduit for ensuring that FINTRAC's views are put forward in the development of public policy and international standards and is responsible for establishing, maintaining and nurturing positive and productive relationships with critical partners such as law enforcement, other government departments and foreign FIUs relationships. This sector also supports corporate needs, including human resources, finance and administration, facilities management, and security. The Communications group is responsible for internal and external communications and public awareness.



426. *Information Management/Information Technology Sector*. The Information Management and Information Technology Sector (75 employees) provides support to FINTRAC's operations in five key areas: the receipt and processing of financial transaction reports, the provision of high quality financial intelligence products, the production of insightful strategic intelligence, compliance and the protection of personal information. This sector develops and applies information management and information technology methodologies that support and advance all of FINTRAC's objectives. It designs, maintains, implements, secures and supports IT infrastructure and system solutions to meet internal and external end user requirements.



427. *Legal Services*. FINTRAC's Legal Services unit is staffed by Department of Justice Canada lawyers who provide advice to FINTRAC on legal questions pertaining to FINTRAC's mandate and operations.

428. *Conclusion*. Canada decided to establish an FIU that would make maximum use of advanced technologies in its analytical and compliance work, allowing FINTRAC to effectively manage a very important and growing database and to analyse incoming reports within a short time frame. FINTRAC's analysts certainly benefit from support from advanced technologies as well as from many experts in the agency. As such, FINTRAC's analysts are significantly focussed on conducting analysis and developing cases for disclosure recipients. Much of the work done outside of the Tactical Financial Intelligence (TFI) unit directly supports this analytical work.

429. Taken into account the above-mentioned considerations and while the total number of staff seems more than adequate, the assessment team has concerns with regard to the number of staff dedicated to the analysis of potential ML/FT cases. Only 36 analysts out of 271 employees (13%) are responsible for developing cases and elaborating FINTRAC disclosures. It seems very challenging for these staff to deal with the amount of reports coming in (15 million reports in 2005-2006, including

nearly 30 000 STRs). Having regard to total resources, FINTRAC should review its internal resource allocation and use, and consider the best and most effective results are being achieved.

Professional standards

430. FINTRAC staff is a diverse group with relevant experiences and skills from both the public (41.7%) and private sectors (58.3%) such as the financial industry, accounting, law enforcement, customs, justice, and public safety. Also, FINTRAC relies upon, and leverages a multidisciplinary team of analysts with backgrounds in various reporting entity sectors, other government departments and international organizations.

431. Employees in the Operations sector bring a varied background of education, including undergraduate and graduate degrees as well as affiliations with professional associations such as Chartered Accountants, Certified Fraud Examiners, International Association of Crime Analysts, and International Association of Law Enforcement Intelligence Analysts.

432. More specifically for the Tactical Financial Intelligence sector, FINTRAC seeks analysts that have sound knowledge and understanding of complex financial manipulations, and a degree from a recognized university. FINTRAC analysts also have experience in using software to analyse data and previous experience in the Canadian or international sector in banking, securities, intelligence analysis, law enforcement, or law.

Standards concerning confidentiality

433. FINTRAC has implemented enhanced security measures and employees participate in security awareness sessions. A robust and effective security program, and a full suite of policies and procedures to protect privacy, and prevent unauthorised disclosures of information, are in place and are vigorously upheld. As mentioned above, FINTRAC employees must obtain a 'Top Secret' security clearance as condition of employment.

Training

434. Employees are able to undergo training and attend conferences on ML/TF issues. FINTRAC provides ongoing internal and external training opportunities to enhance analysts' skills and development. New analysts complete a two-day Operations Orientation Session that covers the operational working and structure of FINTRAC including its legal framework and domestic and international relationships. Entry level analysts also take part in pertinent courses offered regularly, such as courses relating to tactical and strategic intelligence analysis, international AML/CFT standards, effective use of the Internet, and report writing.

Statistics

435. FINTRAC keeps a broad set of statistics, including statistics relating to the number and type of reports received by sector and other relevant information. FINTRAC also maintains statistics on disclosures, in order to track the amount, type, recipient, and foundational information such as the types of financial transaction reports that supported disclosures and the number of reporting entities represented in disclosures.

Effectiveness

436. The following table shows, by report types, the total reports submitted to FINTRAC, by fiscal year, since beginning to receive reports in November 2001:

Report Type	2001-2002[1]	2002-2003	2003-2004	2004-2005	2005-2006	2006-2007[2]	Total
CBCSRs/CBCMIRs	--	650	29 369	75 821	54 506	19 914	**180 260**
LCTRs	--	226 918	2 792 910	3 658 462	6 003 493	3 119 156	**15 800 939**
EFTRs	--	1 859 237	6 689 626	7 077 675	8 887 097	4 814 423	**29 328 058**
STRs	3 772	17 358	14 794	19 113	29 367	18 431	**102 835**
Terrorist Property Reports	--	19	6	6	1	--	32
Total	3 772	2 104 182	9 526 705	10 831 077	14 974 464	7 971 924	45 412 124

[1] For the period of November 2001 to March 2002 (FINTRAC became operational in November 2001 and fully operational in March 2003).
[2] Fiscal year 06-07 statistics include only the first two Quarters (up to September 30, 2006).

437. The number of FINTRAC disclosures since 2001 is as follows:

	2001/2003	2003/2004	2004/2005	2005/2006	2006/2007*	**Total**
Number of disclosures	104	197	142	168	92	**703**

* Fiscal year 06-07 statistics include only the first two Quarters (up to September 30, 2006).

438. The following table breaks down FINTRAC disclosures, by recipient and fiscal year. The RCMP has received the largest number of FINTRAC disclosures. FINTRAC discloses to the RCMP both as the national police force, but also as the provincial police service for all Canadian provinces except Ontario and Quebec. Foreign financial intelligence units, CSIS, and other police forces, (including provincial services for Ontario and Quebec, and municipal services) all receive FINTRAC disclosures.

Disclosure Recipient	2001-2003	2003-2004	2004-2005	2005-2006	2006-2007[1]	Total	%
Royal Canadian Mounted Police	88	163	97	111	63	522	56%
Canadian Security Intelligence Service	23	38	22	21	9	113	12%
Foreign Financial Intelligence Unit	10	22	22	28	17	99	11%
Other Government Agency	3	1	2	4	3	13	1%
Other Law Enforcement Agency	28	66	34	38	27	192	20%
Total	**152**	**290**	**177**	**202**	**119**	**939**	**100%**

[1] Fiscal year 06-07 statistics include only the first two Quarters (up to September 30, 2006).

439. The number of disclosures to 'Other Government Agency' (CRA, CBSA) is reflective of the dual test that must be satisfied in order to disclose to these agencies. As a recipient of information from multiple law enforcement agencies, international counterparts and reporting entities, FINTRAC often identifies links between reports and other information, and this means that disclosures are sometimes made to more than one recipient (*i.e.* multiple police forces in one province, different levels of domestic law enforcement, domestic and international agencies at the same time).

440. The following table shows the number of STRs used in disclosures since 2001:

	2002-2003	2003-2004	2004-2005	2005-2006	2006-2007[1]
Disclosures including STRs	89	117	78	108	62
Total disclosures made	104	197	142	168	92
Number of STRs in these disclosures	5 814	3 080	1 040	1 368	787
Total STRs received	**17 358**	**14 794**	**19 113**	**29 367**	**18 431**

[1] Fiscal year 06-07 statistics include only the first two Quarters (up to September 30, 2006).

441. The total number of STRs used in the cases disclosed has strongly decreased from 5 814 in 2002/2003 (33.5%) to 1 368 (4.6%) in 2005/2006.

442. The following table provides an overview of disclosures by fiscal year, in terms of numbers of disclosures made, the relative dollar amount and the number of transactions contained in the disclosure.

Fiscal Year	Number	CAD Amount	Transactions
2001-2003[1]	104	471 359 543	12 571
2003-2004	197	696 434 493	12 235
2004-2005	142	2 048 445 054	19 263
2005-2006	168	5 004 349 860	43 771
2006-2007[2]	92	2 265 046 135	25 706

[1] Too few disclosures were made in 2001-2002 to present separately. FINTRAC became operational (November 2001).

[2] Fiscal year 06-07 statistics include only the first two Quarters (up to September 30, 2006).

443. The above-mentioned tables indicate a very low number of disclosures in comparison with the total number of reports that FINTRAC receives. In 2005/2006, out of 14 974 464 reports received and out of 29 367 STRs, only 168 disclosures were sent to law enforcement authorities for further investigations (out of these 168 disclosures, 108 included STRs and these disclosures related to more than 43 000 transactions and contained 1 368 STRs). FINTRAC believes that the large number of transactions being disclosed is a positive indicator of the amount of financial data that FINTRAC delivers to law enforcement authorities.

444. FINTRAC disclosures are essentially based on cases generated by law enforcement authorities. The assessors were told that 80% of the cases disclosed by FINTRAC resulted from voluntary information from law enforcement or another recipient[51]. The remaining 20% of the disclosed cases concern new cases that are not already under investigation by law enforcement. This raises serious concerns with respect to the capability of FINTRAC to generate new ML/TF cases (as opposed to positively contributing to existing investigations) on the basis of the STRs it receives (*i.e.* the financial information provided by the private sector).

445. FINTRAC initiated a case disclosure feedback framework in November 2005, which was developed in cooperation with law enforcement agencies throughout Canada. The objective was (1) to enhance FINTRAC's understanding of how law enforcement uses its intelligence product; (2) to initiate steps to strengthen FINTRAC's disclosure process and product; and (3) to be able to report publicly, as a performance measure, the results of FINTRAC's disclosures to law enforcement.

446. Of the feedback forms received as of the end of September 2006, 85% of the responses indicate that the FINTRAC disclosure related to persons, businesses or entities of interest to their current investigation and 60% indicate that the FINTRAC disclosure provided leads on previously unknown persons, businesses or entities of interest. Overall, close to half of the responses indicate that the FINTRAC disclosure provided a major contribution to an ongoing investigation, while about 15% indicate that a FINTRAC disclosure triggered a new investigation. Approximately 15% of the responses also indicated that a FINTRAC disclosure had contributed to an investigation that is expected to be prosecuted.

[51] More than 2 500 voluntary reports were sent to FINTRAC since 2001 (the RCMP provides the majority of these reports).

447. The general view of some organizations that receive FINTRAC disclosures and that were met by the assessment team during the on-site visit is that the balance has been so far too strongly in favour of privacy concerns. The approach that prevailed until the amendment of the PCMLTFA in June 2007 – characterized as too "conservative" or "risk-averse" by some –led to insufficient information in disclosures, which reduced the usefulness for investigations (in particular, for new cases), and difficulty in obtaining production orders for more information.

448. In addition, law enforcement partners have expressed a need for more details (*i.e.* a narrative) on the analysis and rationale underlying FINTRAC disclosures in addition to the factual information that must be provided under the PCMLTFA (as revised). They argue that if more details were provided, this would reduce unnecessary duplication of intelligence effort (*i.e.* there would be no need to redo the analysis already conducted by FINTRAC), enhance availability of timely information, improve the usefulness of disclosures for investigations, and ultimately enhance the effectiveness of the AML/CFT regime.

449. A number of recipients initially indicated that the timeliness of disclosures should be improved to increase relevance to ongoing investigations. The assessors were told that FINTRAC has worked to decrease the time it takes to build a case and make a disclosure, and feedback since April 2006 has indicated an increasing satisfaction with timeliness of disclosures.

450. FINTRAC has an obligation to disseminate financial information to domestic authorities for further action when it has reasonable ground to suspect that the information would be relevant to the investigation or prosecution of a money laundering (Section 462.31) or terrorist activity offence seems to be too strictly implemented using a higher threshold that the one required by law. The assessors have concerns about the interpretation that is made by FINTRAC of the "threshold to disclose" level that might be reached to disclose. Assessors understood during the on site visit that certain financial transactions are not disclosed because they considered as not important enough to be investigated, even if law enforcement information is available. FINTRAC indicated however that all relevant transactions are transmitted to law enforcement as soon as the legal threshold is reached.

451. Based on all of these factors, the assessment team has serious concerns with regard to the added value of the information generated by FINTRAC on ML/TF cases. Importantly, during the on-site visit, the assessors were advised that since the creation of FINTRAC, no conviction for ML or TF has resulted from a FINTRAC disclosure[52]. Although FINTRAC has no role in investigation, prosecution or conviction of ML, TF and the predicate offences, the assessment team believes that this is an additional factor to consider when looking at FINTRAC's ability to produce intelligence that is able to be used in criminal investigations and prosecutions.

2.5.2 Recommendations and Comments

452. FINTRAC should be authorised to develop a more proactive approach for collecting data on suspicious cases of money laundering or terrorist financing and should consider more actively employ its liaison officers to interact with the law enforcement authorities. FINTRAC should be authorised to have access to more intelligence data from CSIS, CRA and the Canadian Customs Agency to reinforce its analytical work. FINTRAC should envisage employing liaison officers from these agencies.

453. FINTRAC should be able to obtain additional financial information from the reporting entities, especially during the analytical process.

---

[52] On 23 January 2008, Canada informed the assessors that one investigation resulted in a conviction for money laundering and was initiated as a result of a STR-driven FINTRAC disclosure case. In addition, FINTRAC indicated that in 22 cases, its disclosures supported investigations that resulted in convictions for ML, proceeds of crime, fraud and other offences.

454. While it will always take a certain level of judgment to decide what constitutes "reasonable grounds" for suspicion, an explicit framework helps produce consistent decisions among analysts and over time. Such indicators should be developed based on ML/TF trends elaborated by FINTRAC. FINTRAC should improve its capacity to produce typologies works and studies on ML/TF trends in Canada.

455. Canada should ensure that the format of reporting forms developed by FINTRAC provides some flexibility and allows the reporting parties to enter all the information in their possession (including annexes such as banking records) that could be relevant for further investigation.

456. Canada should clarify on what basis and criteria FINTRAC decides to which law enforcement authority disclose ML/TF cases. FINTRAC should timely provide law enforcement authorities with more comprehensive and clearer narratives of the cases it discloses.

457. So far, the number of disclosures made by FINTRAC to the CRA has been rather low. It is important that FINTRAC provide information to the CRA because often where cases do not meet the threshold for criminal prosecution, civil liability for unpaid taxes may be possible. FINTRAC and CRA seem to work on developing indicators that would allow FINTRAC to more readily determine whether the information it has in its possession would meet the test of being relevant to an offence of evading or attempting to evade taxes.

458. Canada should ensure that FINTRAC has sufficient analysts that are in charge of developing ML/TF cases and processing disclosures to law enforcement authorities for further investigations.

459. Canada should examine FINTRAC effectiveness in disclosing ML/TF cases to law enforcement authorities including whether all relevant information in FINTRAC possession is disclosed within the restrictions imposed by law, whether this information positively and timely participates in prosecuting ML and TF and whether FINTRAC discloses cases strictly in the circumstances imposed by law. Canada should also consider the use made of STRs and other forms of reports when disclosing cases and consider the current disproportionate reliance on voluntary information reports.

2.5.3 Compliance with Recommendation 26

Rec.	Rating	Summary of factors underlying ratings
R.26	PC	▪ FINTRAC has insufficient access to intelligence information from administrative and other authorities (especially from CRA , CSIS and Customs). ▪ FINTRAC is not allowed by the PCMLTFA to gather additional financial information from reporting entities. ▪ Effectiveness: (1) the number of staff dedicated to the analysis of potential ML/FT cases is low especially in comparison with the amount of reports coming in, which may have an impact on the number of cases that FINTRAC generate; (2) feedback from law enforcement authorities outlines the relatively limited added value of FINTRAC disclosures in law enforcement investigations; (3) the timeliness of FINTRAC disclosures to law enforcement authorities was raised as an issue at the time of the on-site visit; (4) 80% of the disclosures made by FINTRAC result from voluntary information from law enforcement; only 20% result from STRs which raises serious concerns with respect to the capability of FINTRAC to generate ML/TF cases on the basis of STRs or other reports it receives from the private sector; (5) so far, very few if any convictions for ML or TF have resulted from a FINTRAC disclosure which is an additional factor to consider when looking at FINTRAC's ability to produce intelligence to be used in criminal investigations and prosecutions.

2.6 Law enforcement, prosecution and other competent authorities – the framework for the investigation and prosecution of offences, and for confiscation and freezing (R.27, 28 & 30)

2.6.1 Description and Analysis

Recommendation 27

Law Enforcement authorities

460. Canadian efforts to combat organized crime and terrorism are shared by law enforcement agencies throughout the country. As such, Canadian law enforcement authorities are tasked with enforcing federal, provincial, territorial and municipals laws. Statistics indicate that in 2005, there were 229 police forces in Canada, with a total of 61 050 peace officers to enforce various statutes throughout the country. Canada has one national police force (RCMP), two provincial police forces in Ontario and Quebec (Newfoundland's provincial police force is focused largely in St. John's), 169 municipal, and 56 First Nations police forces.

461. While all Canadian police forces can investigate money laundering and terrorist financing offences, the Royal Canadian Mounted Police (RCMP) and, to a lesser extent, the provincial law enforcement authorities in Ontario (the Ontario Provincial Police) and Québec (Sûreté du Québec) undertake virtually all money laundering and terrorist financing investigations. While all police services in Canada are potential recipients of FINTRAC disclosures, the majority of disclosures are made to the RCMP, then CSIS and the Ontario Provincial Police (see table in Section 2.5).

RCMP

462. The RCMP is unique as it is a national, federal, provincial and municipal policing body. The RCMP is organized under the authority of the RCMP Act and is headed by a Commissioner. The RCMP is an agency of the PSEPC. It is divided into four regions and 15 Divisions plus the headquarters located in Ottawa.

463. The Royal Canadian Mounted Police enforces throughout Canada laws made by, or under the authority of the Canadian Parliament. Administration of justice within the provinces, including enforcement of the Criminal Code, is part of the power and duty delegated to the provincial governments. The RCMP provides police services under the terms of policing agreements to all provinces (except Ontario and Quebec), Yukon, the Northwest Territories and Nunavut, and under separate municipal policing agreements to 197 municipalities.

464. *Money Laundering and Proceeds of Crime*

465. The RCMP Proceeds of Crime Program falls under the Federal Policing Services program, which coordinates the RCMP's components in combating money laundering in relation to two federal government initiatives targeting money laundering and criminal proceeds of crime: the Integrated Proceeds of Crime Initiative (IPOC) and the AML/CFT regime.

466. The goal of the IPOC initiative is to contribute to the disruption and dismantling of targeted organized criminals and crime groups (see Section 1.2 of the report for more information on the IPOC Units). The IPOC initiative is currently comprised of 14 units located across Canada and has a total of 257 regular member police officers, 19 civilian members, 59 public servants and approximately 30 seconded provincial and regional police officers.

467. The AML/ CFT regime is led by the Department of Finance. The RCMP coordinates its activities through its Money Laundering Program and currently operates 12 money laundering units, located across Canada and within either Integrated or non-Integrated Proceeds of Crime Sections. The Money Laundering Program has a current workforce of 28 regular member police officers and four civilians.

468. The assessment team believes that the Integrated Proceeds of Crime Units (IPOCs) have demonstrated an ability to enforce proceeds of crime and ML offences and are effective at investigating proceeds of crime and ML offences despite insufficient resources (see also comments in relation to Recommendation 30).

National Security/Terrorist Financing

469. The RCMP has an integrated model for responding to National Security Investigations (NSI), which forms part of the overall Public Safety Anti-Terrorism (PSAT) initiative. The NSI centrally coordinates and directs all national security investigations, intelligence and policy. At the operational level in each province of Canada, NSI serves as the policy centre for the Integrated National Security Enforcement Teams (INSETs) and the National Security Investigation Sections (NSIS).

470. The NSI includes a unit in Ottawa called the Anti-Terrorist Financing Team which consists of the RCMP and CRA. The team is responsible for (1) monitoring and coordinating major ongoing investigational projects related to terrorist organizations focusing primarily on their financial and procurement infrastructures and (2) liaising on a routine basis with partner agencies such as FINTRAC, CSIS and CRA Charities Directorate. The unit has also hosted terrorist financing courses in 2005 and 2006.

471. National Security Operations Branch (NSOB) supports and coordinates all national security field operations by reviewing, analyzing and disseminating information from all sources, including international partners, the CSIS, third parties and RCMP field investigations. NSOB also prepares subject profiles, case briefs and briefing notes for senior management, ensures compliance with RCMP policy, and tasks RCMP liaison officers in support of RCMP National Security investigations.

472. The Anti-Terrorist Financing Team (ATFT) supports counter-terrorism strategies with respect to financial intelligence investigations, enforcement, and the listing process in respect to Terrorist Entities.

473. Using existing resources from NSIS, and complemented by PSAT funding, the RCMP created new Integrated National Security Enforcement Teams (INSETs). INSETs have two mandates: to increase the capacity for the collection, sharing and analysis of criminal intelligence among partners; and to enhance enforcement capacity with respect to criminal activities relating to national security.

474. Supplemented by several other agencies (*e.g.* Canada Border Services Agency, CSIS and Transport Canada), partners work closely in the collection and sharing of intelligence relating to the activities of terrorist groups or individuals. INSET units are located in Vancouver, Toronto, Ottawa and Montreal and total approximately 300 staff. In 2005/2006, the INSET Units concluded approximately 2 900 files.

Provincial Police Forces

475. *Ontario Provincial Police (OPP).* The OPP is comprised of over 5 500 uniformed members, 2 000 civilian employees and 850 Auxiliary members.

476. The OPP established the Ontario Provincial Police Asset Forfeiture Unit (AFU) as the group responsible for the application of all asset forfeiture legislation and the coordination of asset forfeiture initiatives within Ontario. The main activities of the AFU include the identification, investigation, and seizing of offence-related property and proceeds of crime, including the investigation of money-laundering activities resulting from the commission of designated offences found in Part XII.2 of the Criminal Code. The AFU also identifies assets as proceeds of crime, instruments, or conspiracies as defined under the Civil Remedies for Illicit Activities Act (Ontario). The AFU supports local investigative units with their investigation of the substantive criminal offence(s) by providing investigative expertise, training, case management, asset management, expert witness, and external agency liaison.

477. The AFU has developed a core of specialized investigators who investigate asset forfeiture to carry out these activities. To assist in the investigations, the AFU has a full-time forensic accountant. Also, the AFU uses a Currency Reading and Tracing System (CRATS) for searching and tracing seized Canadian or U.S. currency to determine its involvement in criminal offences.

478. With the expanding and changing criminal activity in Ontario, there is a parallel need for substantive investigations and related asset forfeiture investigations. The AFU reviews new trends in crime and law enforcement and adapts their specialized investigative resources accordingly.

479. *Sûreté du Québec*. The Sûreté du Québec (usually translated as "Quebec Provincial Police") is the provincial police force of Quebec, employing approximately 5,200 officers. The primary function of the Sûreté du Québec is to enforce provincial laws, some municipal bylaws, the criminal code, and many other laws throughout Quebec and to assist municipal police forces when needed. The Sûreté du Québec created the first team of investigators specialized in proceeds of crime in 1996. Until 2003, some 12 investigators were specifically assigned to proceeds of crime investigations. Since then, the Sûreté has adopted an integrated approach to organized crime investigations by incorporating a proceeds of crime focus in each major investigation.

480. In the last five years, the Sûreté has initiated or completed approximately 20 major investigations that had a significant proceeds of crime component. Overall in these five years, over CAD20 million dollars have been forfeited as a result of the work of the Sûreté du Québec and a number of criminal organizations have been dismantled.

Prosecution

481. The attorney general of Canada is the chief litigator for the Government of Canada. The Criminal Code establishes jurisdiction to undertake criminal prosecutions in Canada. Criminal prosecution responsibility is divided, by tradition and the law of criminal procedure, between the attorney general of Canada and provincial attorneys general. Generally the attorney general of Canada is responsible for undertaking money laundering prosecutions whenever the offences giving rise to the property being laundered are derived directly or indirectly from offences under criminal law other than the Criminal Code. The provincial attorneys general have the jurisdictional responsibility for money laundering prosecutions for offences found in the Criminal Code. The attorney general of Canada and the provincial attorneys general have concurrent jurisdiction over all terrorist financing prosecutions.

482. The attorneys general prosecute through public prosecution offices established under the authority of their federal or provincial departments. Public prosecutors, known as Crown counsel, are distributed throughout Canada and prosecute on the basis of the jurisdiction to prosecute set out in the Criminal Code. Each province and the attorney general of Canada has a delegated head of criminal prosecutions. Those heads of prosecution meet regularly to coordinate prosecution issues and help each other develop prosecution policies. Money laundering is a regular topic of discussion within the heads of prosecution group. The group has established a subcommittee, the National Liaison Committee on Proceeds of Crime, to coordinate prosecutions issues on money laundering.

483. Counsel for attorneys general have the authority to take over private prosecutions, issue stays of prosecution and generally manage the prosecution function in the Criminal Code. That function includes authority to approve charges. Under the money laundering prosecution authority, only the attorneys general – through their prosecution counsel – may apply for special search warrants, restraint orders, forfeiture orders and wiretap authorisations. Additional responsibilities associated with the PCMLTFA include attorney general applications for production orders and prosecutions related to new offences created within that Act, such as failure to report suspicious transactions.

484. There are 2 349 prosecutors, known as Crown Counsel, working for the ten provincial Attorneys General departments or in a provincial Director of Public Prosecutions office in the province. These prosecutors work in cities or towns throughout their provinces and they are assisted by other legal counsel, acting as standing agents, as the prosecution volume requires. Each of the provincial prosecution services has their own crown counsel prosecution manual and the distribution of money laundering or organized crime cases is managed within the operational structures of the provincial Attorneys General departments of Director of Public Prosecution office.

485. In addition, there are 411 federal prosecutors, now under the supervision of the Director of Public Prosecution in the Public Prosecution Service of Canada (PPSC). These prosecutors work in 13 regional prosecution offices and sub-offices, strategically distributed across Canada. There are also 800 standing agents working for the PPSC who are widely scattered across Canada and operating under the local supervision of the thirteen regional prosecution offices.

486. The federal prosecutor complement includes 70 prosecutors working on proceeds of crime and money laundering litigation in Canada. These include the federal prosecutors assigned to the 12 IPOC units in the RCMP as well as counsel who prosecute the cases generated by the IPOC units. The 70 PPSC prosecutors are dedicated to POC prosecution. They do not prosecute cases generated by NSIS or IBETS. In the larger provinces (Ontario, Quebec, British Columbia and Alberta, as well as in New Brunswick) special teams of crown counsel work with provincial investigative units that are assigned to undertake money laundering investigations.

487. *Measures to postpone or waive the arrest of suspected persons*

488. There is no specific legislative measure in place that allows a law enforcement official to postpone or waive the arrest of suspected persons and/or the seizure of the money for the purposes of identifying persons involved in such activities or for evidence gathering. Rather, the competent authorities have discretionary powers to determine when such enforcement action will be taken. It is important to note, that this power brings with it the responsibility to ensure that the discretion complies with the internal policies of the authority and is in the best interest of Canadians.

Additional elements

489. In Canadian law, there is no separate legislative framework that applies to special investigative techniques (SITs). Law enforcement is covered under the general legal framework of criminal law, as well as under legislation governing the establishment and conduct of police forces and other enforcement agencies. Within this framework, specific kinds of SITs are subject to specific legal requirements. It should be emphasized, as well, that laws providing for SITs, and law enforcement activity in using SITs, are subject to review by the courts under the Canadian Charter of Rights and Freedoms and in respect of compliance with other general requirements, such as those that govern abuse of process.

490. Some SITs, such as general undercover police operations, non-intrusive police observation techniques, and use of informants are not subject to specific provisions of statutory law addressing when and how they can be used. Nevertheless, general legal standards and common law requirements apply. Common law standards, such as the abuse of process doctrine, also come into play: police conduct which is unacceptable as an abuse of process is that which violates a community's sense of decency and fair play and police use of such techniques may lead to a judicial staying of proceedings against the accused. It should be noted that the use of SITs such as undercover operations are also governed by internal police policy and procedures. Comprehensive administration and accountability provisions addressing law enforcement activity is provided by laws addressing the establishment and organization of police forces, codes of conduct, and internal discipline (deontology), and public complaints.

491. Certain other SITs do have detailed provisions in law requiring prior judicial authorisation. These include, for example, interception of private communications and searches. Judicial authorisation requirements also apply to additional special procedures such as the taking of DNA samples, installation of tracking devices and installation of devices recording telephone numbers dialled (and the numbers from which calls are received).

492. In respect of SITs in which police would engage in illegal conduct, the Supreme Court of Canada has ruled that police have no inherent immunity from liability for unlawful conduct committed in good faith during the course of an investigation. The Supreme Court further noted that if immunity

were necessary, it was for Parliament to provide for it. On its face, this restrictive principle could apply, depending on the circumstances, to certain SITs. Parliament has, however, adopted provisions allowing law enforcement officers to engage in conduct that would otherwise be illegal for the purpose of investigations and enforcement, subject to controls and limitations. For example, measures under the Criminal Code provide a limited justification for designated law enforcement officers – and others acting at their direction – for acts and omissions that would otherwise be offences. The justification includes a fundamental requirement of "reasonable and proportional" conduct. Three factors are set out as relevant to determining reasonableness and proportionality: the nature of the act or omission, the nature of the investigation, and the reasonable availability of other means for carrying out enforcement duties. Certain conduct that would otherwise be an offence is justified only if a public officer has the prior written authorisation of a senior official responsible for law enforcement or in exigent circumstances. Certain other conducts, such as the intentional causing of death or bodily harm, obstruction of justice, or conduct that would violate the sexual integrity of an individual, are not justified.

493. Certain other exemptions and exceptions for specific law enforcement SITs that would otherwise be illegal are provided by separate legal provisions. For example, the Controlled Drugs and Substances Act (Police Enforcement) Regulations governs the use of controlled deliveries and reverse stings in drug investigations.

494. In the proceeds of crime context, provisions of the Criminal Code provide exceptions, respectively, for possession of property obtained by crime and for money laundering where this is done by a law enforcement officer – or a person acting under the direction of a law enforcement officer – for the purpose of an investigation or otherwise in the execution of the law enforcement officer's duties.

495. Canadian law enforcement undertakes co-operative investigations with appropriate authorities in other countries, especially with the US. Canadian authorities actively participate with foreign jurisdictions in both money laundering and criminal proceeds investigations. During these co-operative investigations, compliance with Canadian legislation is ensured. The participation of Canadian authorities is limited to its domestic legislative parameters, most notably with respect to the use of special investigative techniques.

Recommendation 28

496. Through authority in criminal law, law enforcement has the ability to compel production, to search persons or premises and seize or obtain documents, information or data while conducting ML, TF and underlying predicate offence investigations. The accessible information includes bank account records, customer identification records, and other records maintained by financial institutions and other persons through lawful process, as necessary, to conduct investigations of money laundering, terrorist financing and predicate offences.

497. Most of the procedures allowing law enforcement to compel production of, to search persons or premises and seize or obtain documents, information or data are found in the Criminal Code. The following list is describes several of the procedures frequently used by the police:

- Search warrant under s. 487 of the *Criminal Code* – search and seizure of evidence.
- Special search warrant seizures under s. 462.32 of the *Criminal Code* – search and seizure of proceeds of crime.
- Search warrant under s. 11 of the *CDSA* – search and seizure of evidence for a drug offence.
- Production order under s. 487.012 of the *Criminal Code* – production of documents or copies or preparation of a document.
- Production order under 487.013 of the *Criminal Code* – for financial and commercial information.
- General warrant under s. 487.015 of the Criminal Code.

- Order for gathering evidence under s. 83.28 of the *Criminal Code* (for terrorist offence only) – order the examination on oath or not of a person, order the person to bring any thing in their possession or control.
- Order for disclosure of information in respect of FINTRAC – for money laundering or terrorist activity financing offences only – for information or documents obtained by or on behalf of the Director of FINTRAC.
- Order for disclosure of income tax information under 462.48 of the *Criminal Code* – for a money laundering or possession of proceeds of crime offence, for a designated drug offence or a terrorism offence – tax information from Canada Revenue Agency.

498. Pursuant to paragraph 34(2) of the Interpretation Act, these procedures can be used while investigating suspected money laundering, terrorist financing, and all other offences of federal legislation, except if the legislation otherwise provides.

499. These procedures are issued by either a judge of the peace, a Provincial Court judge or a Superior Court judge. Before making an order, the justice or judge must be satisfied, on the basis of an ex parte application containing information on oath in writing, that there are reasonable grounds to believe that (a) an offence against this Act or any other Act of Parliament has been or is suspected to have been committed; (b) the documents or data will afford evidence respecting the commission of the offence; and (c) the person who is subject to the order has possession or control of the documents or data.

500. During the on-site visit, the assessment team was told that such threshold is difficult to reach in practice, especially under Article 487.013 of the Criminal Code for collecting financial and commercial information. The law enforcement authorities met were also unanimous with regard to the difficulty to get valuable information from FINTRAC (limited data contained in “designated information” (although new PCMLTFA requirements in force since June 30, 2007 address this issue), lack of narrative information, delays in responding - see conclusions in relation to Recommendation 26 in Section 2.5 of the report). The law enforcement authorities met during the on-site visit also identified other types of impediments to the conduct of ML/TF investigation including access to information in possession of lawyers and access to ownership information on legal persons.

501. The RCMP has demonstrated an advanced capability in terms of using special investigative techniques for money laundering and proceeds of crime investigations. An example is the 'store front' operation referred to as Project Eldon, which involved establishing and operating an import / export business that provided money laundering services to organized crime. This investigation was conducted over several years, including the time that it took to establish the business and technical infrastructure, and to infiltrate and dismantle an international organised crime group with extensive involvement in money laundering offences. The investigation relied primarily on undercover policing techniques and was supported, among other things, by electronic surveillance and computer crime investigation capability. The RCMP has indicated that further covert money laundering investigations will be conducted based on the experiences learned from Project Eldon.

502. Law enforcement agencies in Canada have a wide range of investigative powers and capabilities for use against organized and serious crime, including for the investigation of ML, TF and predicate offences. The evaluation team noted that while the Canadian undercover policing programme was used for the investigation of money laundering, to attack the upper most levels of organised crime, there is no provision for protecting the true identity of the undercover police officer - instead, the true identity of the officer must be revealed to the accused person. This situation arises due to there being no dedicated legislative regime for conducting undercover policing operations. When compared with internationally equivalent jurisdictions, this was considered to be a weakness for special investigative techniques that may be used for money laundering investigations.

503. Competent authorities have the powers to take witness statements for use in investigations and prosecutions of ML, TF, and other underlying predicate offences and related actions.

504. In money laundering and terrorist financing cases, witness statements are taken voluntarily in accordance with the Charter of Rights and Freedoms and the Canada Evidence Act. However, in terrorist financing investigations, witnesses are bound to provide a statement. There are legislative provisions outlined under Part II.1 of the Criminal Code (Terrorism) whereby an investigative hearing can take place for the purposes of gathering evidence, including the questioning of persons, in respect to a terrorism offence. Those offences are outlined under Section 2 of the Criminal Code and include the financing of terrorism offences (Sections 83.02, 83.03 and 83.04 of the Criminal Code).

Recommendation 30 – structure, staff and resources

Law Enforcement

505. The RCMP provides federal policing services in all provinces and territories and provincial/municipal policing services in three territories, eight provinces (except Ontario and Quebec), more than 200 municipalities, 165 Aboriginal communities, three international airports and numerous smaller airports. In total, the RCMP employs approx. 23 466 employees, of which 16 327 are peace officers.

506. One of the RCMP's division or directorate that is particularly relevant for combating criminal activity and money laundering is the Federal and International Operations (FIO) group. This group works to ensure the safety and security of Canadians and their institutions, domestically and globally, through intelligence-based prevention, detection, investigation, and law enforcement measures taken against terrorists, organized criminals, and other criminal activity. The strategic priorities are: (1) effective support of international operations; (2) reducing the threat and impact of organized crime and (3) effective delivery of federal programs.

507. FIO works closely with other activities for the national delivery of federal programs. The assistance of Criminal Intelligence Directorate is crucial to timely, effective and efficient service delivery. Technical Operations provides specialized investigative supports services which encompass and enhance research and development on techniques and tools to ensure FIO's ability to conduct high level investigations. Under the FIO umbrella is Drugs and Organized Crime, Border Integrity, International Policing and Financial Crime.

508. *Drugs and Organized Crime* focuses on combating Organized Crime as well as drug related social and economic harm to Canadians. It works to reduce supply of and demand for illicit drugs using an integrated approach involving measures for prevention, education, enforcement, counseling, treatment and rehabilitation.

509. *Border Integrity* is responsible for enforcement issues related to Canada's borders, and enforcement of more than 250 federal statutes in a variety of areas. It also builds partnerships with stakeholders throughout all segments of Canadian society to provide the best response(s) to policing concerns, whether by investigating criminal offences, assisting federal government departments, informing and seeking input from general community and implementing problem oriented policing.

510. *International Policing* enhances international cooperation at strategic and tactical levels between RCMP and foreign police and law enforcement agencies. It provides support and assistance, through the liaison officers, to Canadian law enforcement agencies in the prevention and detection of offences to Canadian federal laws, liaises with foreign criminal police agencies and related institutions, and coordinates activities related to Interpol. In accordance with Canada's foreign policy, it selects, trains and deploys Canadian police personnel on UN civilian police missions and provides logistical support to them and their families.

511. *Financial Crime* contributes to the security of the Canadian economy and seeks to protect Canadians and their governments from financial crimes perpetrated by organized crime and others. It reduces, controls and prevents business-related or white-collar crime, including fraud, false pretenses, and offences against the Government of Canada, corruption of public officials, insolvency process,

counterfeiting and others. It also oversees RCMP's contribution to the Integrated Proceeds of Crime (IPOC) partnerships against money laundering.

Proceeds of Crime Program

512. The Proceeds of Crime Program coordinates the RCMP's components in combating money laundering and terrorist financing in relation to 2 federal government initiatives targeting Money Laundering and Criminal Proceeds of Crime, being the IPOC and the AML/CFT regime (see comments above under Recommendation 27). The following table provides the funding available for the RCMP's Proceeds of Crime Program as a result of the IPOC and AML/CFT regime.

Funding arrangements for the RCMP Proceeds of Crime Program			
Year	**IPOC**	**AML/CFT regime**	**TOTAL**
2005-2006	CAD40 796 662	CAD4 900 000	CAD45 696 662
2004-2005	CAD38 838 869	CAD4 900 000	CAD43 738 869
2003-2004	CAD38 693 000	CAD4 900 000	CAD43 593 000
2002-2003	CAD36 848 960	CAD4 900 000	CAD41 748 960

513. In addition to the resources identified above that are directly linked to the Proceeds of Crime Program, the program has access to other technical investigational support from within the RCMP. These resources include police undercover operations, source/agent operations and support, electronic and physical surveillance, and forensic science support to name a few.

514. Further statistics in relation to the resources available to the RCMP were provided to the assessment team. The first table identifies resources available to the RCMP in the context of the National Initiative to Combat ML (NICML) established in 2000. In that context, the RCMP got 12 extra staff in December 2006. The second table makes inventory of the resources of IPOC Units in 2007.

RCMP Resources in the context of the National Initiative to Combat ML (NICML)					
YEAR	FUNDING	REGULAR MEMBERS	PUBLIC SERVICE	Civilian Member	TOTAL POSITIONS
2002-2003	CAD4 900 000	30	1	4	35
2003-2004	CAD4 900 000	30	1	4	35
2004-2005	CAD4 900 000	30	1	4	35
2005-2006	CAD4 900 000	30	1	4	35
2006-2007	CAD4 900 000	30	1	4	35
2007-2008	CAD6 962 000	42	1	4	47

IPOC Units Resources				
Proceeds of Crime RCMP DIVISIONS 2007	Regular Member	Civilian Member	Public Service	**Total**
A Division (Ottawa)	10	1	3	**14**
B Division (Newfoundland)	5	0	3	**8**
C Division (Quebec)	62	5	16	**83**
D Division (Manitoba)	10	1	2	**13**
E Division (British Columbia)	39	3	12	**54**
F Division (Saskatchewan)	10	2	2	**14**
G Division (Northwest Territories)	1	0	0	**1**
H Division (Nova Scotia)	9	0	2	**11**
J Division (New Brunswick)	11	1	2	**14**
K Division (Alberta)	27	2	6	**35**
L Division (Prince Edward Island	0	0	0	**0**
N Division (HQ Ottawa)	11	1	3	**15**
O Division (Ontario)	56	2	12	**70**
TOTAL	251	18	63	**332**

515. As far as IPOC Units are concerned, RCMP has the same level of resources as of 1996 when the Units were set up. RCMP representatives insist on the fact that the type of investigations they carry out are more complex and require more time and resources than it was the case in the 1990's. In addition, the increase allowed in December 2006 (plus 12 staff) brings the resources to their level before the budget cuts that took place in the late 1990's. The evaluation team was informed that the RCMP received funding for an additional 1 000 positions to restore staffing in several programs where gaps had been identified: commercial crime; drug enforcement; federal enforcement services; customs and excise; immigration and passport, criminal intelligence; and technical operations. Initiatives, such as IPOC, were not identified for additional funding and positions could not be reallocated outside of the programs targeted.

516. Following September 11, 2001, the Government of Canada enhanced its terrorism response capabilities and improved the legislative framework for terrorist threats. The RCMP received funding to enhance analytical, intelligence sharing and operational technology; support protective operations; enhance security activities at airports, ports and borders; and focus on human resourcing for activities targeting cross-border criminal activities. The following enforcement units and funding were put in place to address National Security enforcement:

- Integrated National Security Enforcement Teams (INSETs) – CAD64M over 5 years.
- Integrated Border Enforcement Teams (IBETs) – CAD125M over 5 years.
- Financial Intelligence – CAD1M.
- Investigative Operations Support – CAD25M.
- Police Reporting and Occurrence System – CAD10M.
- Marine Security – CAD115M.
- National Ports Enforcement Teams – CAD11.5M over five years.
- Integrated Immigration Enforcement Teams –CAD18.7M over five years.

517. Despite the increase of budget, the RCMP lacks the resources that would allow it to focus on a larger spectrum of ML/TF investigations. The RCMP acknowledges that, due to resources constraints, it is essentially dedicates its resources to large and complex ML investigations related to organised crime groups.

Marine Security

518. The marine sector supports a vital trade gateway, connecting Canada to the world. In 2000, Canadian international marine trade, including traffic between Canada and the US, was valued at more than CAD100B, equalling one-eighth of the country's total trade, and employing more than 30 000 people.

519. The role of Canada's marine security includes the investigation of occurrences dealing with national security, organized crime and other federal statutes, such as those involving smuggling, illegal drugs and immigration. They also work with various Government departments as part of its integrated response to marine security, to help deter and detect any illicit and/or terrorist activity, cargo or people within Canadian waters. Budget 2004 included CAD115M for marine security issues and improvements to Canada's marine security.

National Ports Strategy

520. Through its National Ports Strategy, the RCMP strategically and tactically addresses criminal activities and terrorism at Canada's major marine ports. The objective is to take an intelligence-led, multi-disciplinary and integrated approach to prevent, deter and detect any illicit and/or terrorist activity, cargo or people at major marine ports that may pose a threat to national, US and global safety and security. The RCMP enforce federal statutes dealing with issues such as migrant smuggling, illegal drugs, illegal firearms.

National Ports Enforcement Teams (NPETs)

521. NPETs were established in 2003 to conduct investigations of federal offences relating to Canadian seaports. Comprised of partners from federal, provincial and municipal law enforcement agencies, NPETs are complemented by local management teams to resolve conflicts and identify roles and responsibilities. There are currently 24 RCMP members dedicated to NPETs, centered at Canada's three major ports. Commencing in 2003/04, CAD11.5M in funding over five years will be used to position investigators in major ports; increase training for marine intervention (*i.e.* ASB); and, conduct records checks of port employees for Transport Canada.

Airports

522. Airport Federal Enforcement Sections (AFES) are mandated to combat organized crime and terrorism by providing enforcement of numerous federal statutes, as well as assistance to various federal programs and departments. Since the inception of the AEFS system in 1999 the Airport Federal Enforcement Sections have seized over CAD460M worth of contraband, including drugs and weapons. A funding strategy is under development to expand the program at the Toronto site, as well as include other airports (*i.e.* Calgary and Ottawa).

Smuggling and Trafficking of Persons

523. Canada's long border, with high volumes of people and goods passing across, provides opportunity for the smuggling of contraband and prohibited goods. Challenges are also posed by expanding global migration by land, sea and air. In June 2002, Canada introduced the Immigration and Refugee Protection Act, creating new offences that directly address trafficking in human beings. In addition, as of November 2005, three new *Criminal Code* offences came into effect relating to trafficking in persons.

524. The Immigration and Passport Program (IPP) is being regionalized to meet evolving expectations and demands. The roll-out of the program continues, with the reallocation of funded positions to six locations – Vancouver, Calgary, the Greater Toronto Area, Ottawa, Montreal and Halifax. The focus of these teams will be to combat and disrupt organized migrant smuggling and the trafficking of persons, with more recent emphasis on those individuals and/or organizations posing a threat to the security of Canada. As of June 2006, the CBSA gained responsibility for criminal investigations related to migrant smuggling.

525. In addition to these regional teams, a new trafficking unit will be co-located with the Ottawa Immigration and Passport Section, focusing on the coordination of domestic and international trafficking investigations; interacting with foreign law enforcement agencies in support of Immigration and Passport teams; and, advocating education, prevention and awareness of these global problems[53].

526. A federal interdepartmental working group, consisting of 16 departments and agencies, is developing Canada's position on the UN Trafficking Protocol. The working group is responsible for co-ordinating federal activities to address trafficking including the development, promotion and implementation of a comprehensive anti-trafficking strategy, in keeping with Canada's international commitments.

527. Specialists from the RCMP have developed training material for the recognition of fraudulent travel documents. A collaborative effort is underway between BCDE and Interpol forensic analysts to improve Interpol's central databank for lost and stolen passports – Canada was selected as one of the countries to participate in this important pilot project.

---

[53] This unit has been formed and is fully functional. Information about the Human Trafficking National Coordination Centre (HTNCC) can be found at http://www.rcmp-grc.gc.ca/imm_pass/htncc_e.htm.

Prosecution

528. Until December 12, 2006 the Federal Prosecution Service of Canada was an integral branch of the Attorney General of Canada's function as part of the Canadian Department of Justice. On December 12, 2006 the Director of Public Prosecution Act came into force, resulting in the seamless transition of the Federal Prosecution Service into an independent public prosecutions office that reports to the Parliament of Canada through the Attorney General of Canada. The new Public Prosecution Service of Canada (PPSC) assumes carriage and control of all prosecution functions previously undertaken by the Federal Prosecution Services and the PPSC is tasked with all of the consultation and coordination responsibilities previously undertaken by the Federal Prosecution Service. The federal prosecutor complement includes 70 prosecutors working on proceeds of crime and money laundering litigation in Canada. These include the federal prosecutors assigned to the 12 IPOC units in the RCMP as well as counsel who prosecute the cases generated by the IPOC units. The 70 PPSC prosecutors are dedicated to POC prosecution

529. The provincial heads of prosecution manage and supervise all provincial crown prosecutors. As a result, this group of prosecution heads regularly meets to discuss and coordinate common prosecution issues. In the area of money laundering and proceeds of crime, there are two committees that have been created. The National Liaison Committee comprised of money laundering prosecutors, selected by and reporting to the heads of prosecution, meets yearly or more frequently to coordinate common issues relevant to money laundering prosecutions. The second committee is the Coordinating Committee of Senior Officials (CCSO) on Proceeds of Crime. It is also comprised of money laundering prosecutors and criminal law policy lawyers and reports to the Justice Deputy Ministers Committee (Federal, Provincial and Territorial).

530. The PPSC is also a partner in a national memorandum of understanding with the RCMP for the Integrated Proceeds of Crime Program. This integrated program includes a significant number of full time prosecutors, who are PPSC prosecutors, assigned to be members of the 12 IPOC investigative units. In addition, the program also funds PPSC prosecutors to actually prosecute the money laundering cases investigated by the IPOC units and general law enforcement. There is a regular series of meetings between the RCMP's national Proceeds of Crime program and the PPSC on money laundering and proceeds of crime. In addition, the PPSC has quarterly meetings with RCMP Federal Police Service to discuss and plan for investigative and prosecution issues, both in the proceeds of crime and general prosecution area.

531. There are also regional IPOC unit and PPSC regional office meetings, as mandated in the existing Memorandum of Understanding with the RCMP. These meetings resolve local problems and concerns that may develop in the proceeds of crime program. In addition, the PPSC will carry on the Federal Prosecutions Service's Cross Border Crime Forum meeting with law enforcement and the United States Attorneys Office. The Forum works on common prosecution issues, including proceeds of crime, with counterparts in the United States. The PPSC is a member of the International Association of Prosecutors and it attends that organization's annual meetings. Finally, the PPSC has counsel in its headquarters assigned to coordinate all proceeds of crime issues. That counsel conducts a quarterly video conference with all counsel in the IPOC units and the IPOC unit counsel have an IPOC common electronic mail room that is used daily to discuss money laundering and proceeds of crime issues between counsel.

Recommendation 30 – staff professional standards

Law Enforcement

532. Municipal, regional, and federal policing agencies conduct activities in accordance with the laws of Canada. To ensure enforcement and adherence to the laws and values of Canadian society, policing agencies have established professional and ethical codes of conduct. These matters are monitored through both internal and external processes, and may result in criminal judicial proceedings and/or internal disciplinary action.

533. The RCMP employs both regular (peace officers) and civilian members, who are subject to the provisions of the RCMP Act. The RCMP Act is a Federal statute, which governs the structure, operations, and ethical conduct of the membership. Members must pledge an Oath of Allegiance and an Oath of Secrecy pursuant to their engagement with the RCMP. The RCMP also employs public servants who take oaths of office and secrecy pursuant to the Public Service Act.

534. The Proceeds of Crime/Money Laundering investigative sections are integrated units tasked with conducting complex financial investigations. Professionals from the legal, accounting, asset management and taxation fields work with police investigators, from the RCMP and Regional/Municipal police services to conduct proceeds of crime/money laundering investigations. Each person assigned to the investigative unit is bound by the professional and ethical standards established by their respective organizations.

535. The Security of Information Act permanently binds all RCMP employees, which includes those assigned to the Proceeds of Crime/Money Laundering units and the National Security, who have access to special operational information to secrecy. Sensitive information obtained through the day-to-day operations of the Proceeds of Crime/ Money Laundering Units is classified using the RCMP security classification system. Access to this information is limited to those persons with the appropriate security clearance and who have an operational requirement to access the said information. Breaches with respect to classified, sensitive and or private information can be dealt with through criminal or internal disciplinary proceedings.

Prosecution

536. Prosecutors, as opposed to standing agents, are all full time appointment positions within the public service of Canada or a province. Each prosecutor must sign an oath of office and maintain their legal duty relative to solicitor client privilege. Just as full time prosecutors maintain privileged communications the same professional obligation applies to every standing agent. There are strong conflict of interest obligations and prohibitions against accepting outside work as legal counsel.

537. Every prosecutor, whether they work for a provincial Attorney General, director of public prosecutions or the federal Director of Public Prosecution, must be a full member of a provincial or territorial law society who is in good standing with that professional society. In addition they all operate independently of law enforcement and separate from the judiciary. Every prosecutor fully appreciates their responsibility as a quasi minister as described by Supreme Court of Canada and courts of appeal decisions. This role is best seen in the following excerpts from two cases: R. v. 1353837 Ontario Inc. and R.. v. Boucher[54].

Recommendation 30 – training

Law Enforcement

538. Since the inception of the Proceeds of Crime Program, the RCMP has taken the lead role in training investigators who specialize in these investigations.

---

[54] *The tradition of Crown counsel in this country in carrying out their role as "ministers of justice" and not as adversaries has generally been very high (R. v. 1353837 Ontario Inc., et al, February 24, 2005, C42378, at par. 34, per Laskin J.A. (Ont. C.A.)).* It cannot be over-emphasized that the purpose of a criminal prosecution is not to obtain a conviction; it is to lay before a jury what the Crown considers to be credible evidence relevant to what is alleged to be a crime. Counsel have a duty to see that all available legal proof of the facts is presented; it should be done firmly and pressed to its legitimate strength, but it also must be done fairly. The role of prosecutor excludes any notion of winning or losing; his function is a matter of public duty than which in civil life there can be none charged with greater personal responsibility. It is to be efficiently performed with an ingrained sense of the dignity, the seriousness and the justness of judicial proceedings. (R.. v. Boucher [1955] S.C.R. 16, at pp. 23-24; 100 C.C.C. 263, at p. 270.).

539. Specific eligibility requirements have been established in an effort to ensure that qualified and motivated personnel are hired by the RCMP. These requirements include specific language, education, physical and age restrictions. Upon completion of an extensive recruitment process which includes medical, physical and psychological testing the successful candidate attends the RCMP Training Academy situated in Regina, Saskatchewan for a five month training program. This training program is comprised of a number of courses including: Criminal Law, Firearms training, Driver training, Police Incident Reporting procedures, and witness/suspect interviewing techniques. This training provides the foundation for all aspects of policing within the RCMP.

540. Subsequent to the successful completion of this basic training, the candidate is given the legal authority to enforce the criminal laws of Canada. Human Resources Department will assess the needs of the RCMP and assign the new police officers to detachments throughout Canada. These police officers will further develop their policing skills through work experience and additional work related training. The "Proceeds of Crime" units seek experienced investigators who have developed their skills from both front line uniform and plain-clothes aspects of policing. To further enhance the skills of these investigators, the RCMP developed two training courses specific to "money laundering".

541. The RCMP currently offers a "Basic" and "Advanced" proceeds of crime investigators course. These courses, based at the RCMP's Centralized Training Facilities in Regina, Saskatchewan, follow the adult based learning model. Training is targeted primarily around RCMP proceeds of crime/money laundering personnel as well as employees of the initiatives partner agencies. Positions on these courses are based on the operational requirements of units and whenever possible, training is also given to non-program related investigators in order to increase both awareness and understanding of the program, while developing expertise for potential future proceeds of crime/money laundering investigators.

542. The Basic Proceeds of Crime course is offered to members of the RCMP assigned to the Proceeds of Crime program as well as employees of partner agencies. This course is seven days in length and concentrates primarily on the basic structure and methods used to investigate money laundering offences. A combination of experienced facilitators and a "problem base" method of instruction, allows participants to share their work experiences and explore different strategies in conducting these complex investigations.

543. In addition, municipal and provincial police partner agencies representatives have participated in these courses. The RCMP has also made efforts to educate other agencies, at both the federal and provincial levels. Federal agencies such as FINTRAC and the Competition Bureau have received training, while provincial agencies such as Revenue Quebec, have also been given the opportunity to partake in these courses. Internationally, the RCMP has trained six international law enforcement officers and continues to field requests from countries for this training.

544. The Advanced Proceeds of Crime Course is offered primarily to investigators, with approximately three years of proceeds of crime/money laundering experience and who have received the Basic Proceeds of Crime Course. Candidates are primarily from within the Proceeds of Crime/ Money Laundering Program and partner agencies. In addition, this training is also offered to seconded policing partners, both provincial and municipal, who have developed their expertise within their respective units. The course is also offered to other RCMP investigators. From January, 2001 to December, 2005, the RCMP has presented 20 Basic Proceeds of Crime courses and 8 Advanced Proceeds of Crime courses to close to 775 candidates.

545. To further meet the needs of the more complex investigations within the mandate of the RCMP, the RCMP has developed training programs which concentrated primarily on complex investigative techniques including wiretaps, search warrants, human source development and undercover police operations. The instructors for these training courses include police investigators and lawyers who are specialists in these areas. These techniques are used traditionally in drug investigations. With the

evolution of money laundering investigations, the RCMP has modified this training to demonstrate the application of these techniques within these types of investigations.

546. Within the money laundering/proceeds of crime investigators program, there are approximately 30 investigators who form an "Expert Witness Program" and provide "expert testimony" in criminal court pertaining to money laundering offences. To further supplement their experience, the RCMP provides a bi-annual expert and senior investigator's training workshop where these investigators share their knowledge on money laundering investigative techniques, trends and typologies.

Prosecution

547. All prosecutors must maintain their status as members of their relevant provincial or territorial law society. Every law society has a continuing legal education obligation for its members. In addition every Attorneys General department, including the federal Attorney General of Canada, and the Office of the Director of Public Prosecutions has a continuing legal education policy and extensive training courses in their manuals and procedures. In the case of federal prosecutors working for the Office of the Director of Public Prosecutions each must have an annual performance review report, which includes a specific component on continuing legal education.

548. Every year, the Director of Public Prosecution organizes the School for Prosecutors and the Advanced School for Prosecutors. Each school is an intensive seven-day training course on substantive law, policies and practice. Every year, approximately 30 prosecutors attend each school. Each provincial prosecution service has similar training obligations and programs.

549. The federal Department of Justice and the Office of the director of Public prosecutions has a formal Continuing Legal Education Policy, which requires each of its lawyers to take a minimum of 12 hours of training, or to teach for at least four hours, every year. The policy is based on a number of principles, one of them being that "Crown counsel are expected to maintain a high level of expertise by keeping abreast of developments in the law." The policy may be found on the Department's intranet site, under the heading Continuing Legal Education. Finally, every prosecutor's mandatory annual performance review includes a detailed consideration of the prosecutor's successful completion of their training obligations and their training plans for the next year.

550. Training initiatives dedicated to combat ML and TF seem limited in practice.

Additional elements

551. The National Justice Institute is dedicated to the development and delivery of educational programs for all federal, provincial and territorial judges.

552. The Institute has conducted a Criminal Law Seminar in March 2007 that has focused on financial Crimes. One of the agenda items dealt specifically with money laundering issues.

553. In addition, an RCMP senior investigator and a Department of Justice prosecutor traveled to Ottawa in 2004 and 2005 to provide training on money laundering investigations and prosecutions to the CBSA's Adjudications Division. Also, a senior investigator of the RCMP made a money laundering presentation to the Osgoode Hall Law School continuing development program on February 11, 2006.

Statistics

554. The following table provides an overview of the investigative work at the IPOC units in recent years.

Trends in All Files Opened, by Year and Predicate Offence								
	2002		2003		2004		2005	
Predicate Offence	**#**	**%**	**#**	**%**	**#**	**%**	**#**	**%**
Drug related	643	39.7%	606	35.7%	1288	42.1%	1511	45.3%
Proceeds of crime /Money laundering	476	29.4%	552	32.5%	1329	43.5%	1481	44.4%
Customs related	54	3.3%	51	3.0%	87	2.9%	101	3.0%
National security	17	1.0%	5	0.3%	7	0.2%	1	0.1%
Other Criminal Code offences	68	4.2%	54	3.2%	155	5.1%	240	7.2%
International requests	178	11.0%	161	9.5%	54	1.7%	0	0.0%
Predicate undetermined	185	11.4%	267	15.7%	137	4.5%	0	0.0%
TOTAL	**1621**	**100%**	**1696**	**100%**	**3057**	**100%**	**3334**	**100%**

2.6.2 Recommendations and Comments

555. Canada should ensure that additional resources are allocated to law enforcement authorities to allow them to carry out a larger number of ML/TF investigations (including at provincial level) in addition to the biggest ML cases they can actually tackle.

556. Canada should also collect more data on current ML investigations (especially in Ontario and Quebec).

557. Canada should consider reviewing the possible existing impediments to ML/TF investigations (including access to information in possession of lawyers and access to ownership information on legal persons). Access to tax information, while provided for, could also be enhanced.

558. Canada should improve the educational and training programmes provided for judges and courts concerning ML and TF offences.

2.6.3 Compliance with Recommendations 27 & 28

Rec.	Rating	Summary of factors underlying ratings
R.27	LC	▪ The RCMP lacks the resources that would allow it to focus on a larger spectrum of ML/TF investigations.
R.28	C	▪ The Recommendation is fully met.

2.7 Cross Border Declaration or Disclosure (SR.IX)

2.7.1 Description and Analysis

Declaration system

559. Canada's mandatory cross-border currency reporting regime came into force in January 2003. Under Part II of the PCMLTFA, any person or entity is required to report to Canada Border Services Agency (CBSA) officers the importation or exportation of currency and monetary instruments of an amount of CAD10 000 or more. The requirements apply whether the currency or monetary instruments are brought across the border by the importer or exporter themselves, (*e.g.* carried in baggage) or imported or exported by mail, courier, rail or by any other means. This reporting requirement applies to the physical movement of money, not to funds transferred electronically.

560. Section 12 of the PCMLTFA establishes the requirement to report the cross-border movement of currency or monetary instruments over a set amount. The Cross-Border Currency and Monetary Instrument Reporting Regulations set out the reporting threshold and other modalities of the reporting obligations.

561. The regulations define the term "monetary instruments" as including, among other things, stocks, bonds, bank drafts, traveller's cheques or any other financial instruments in bearer form or in such form as title to them passes on delivery, and set the reporting threshold at CAD10 000 or its

equivalent in a foreign currency. The report must be made in writing using the forms designed by the CBSA – the Cross-Border Currency or Monetary Instrument Report (CBCMIR). Limited provisions exist to allow for reporting from remote locations. If there is no CBSA office in the vicinity, reporting may be done by telephone. The CBSA officer could request that the importer or exporter present themselves at a specified place for examination of the currency or monetary instruments.

562. The regulations also provide for certain exceptions from reporting, such as when currency or monetary instruments are brought into Canada aboard a commercial passenger conveyance (airplane, charter bus, cruise ships or ferry), and where Canada is a transit point rather than the final destination. It does not apply where the passenger disembarks and reports to CBSA. Also exempt are movements of currency by or on behalf of the Bank of Canada that the Bank is manufacturing for other jurisdictions, as well as stocks, bonds and debentures imported into Canada by courier or as mail, if the importer is a financial institution or a securities dealer as defined in section 1(2) of the PCMLTFA.

563. In practical terms, the system used to detect the physical cross-border transportation of currency varies among the modes of transportation as well as whether individuals are coming to or leaving Canada. For example, in the case of incoming flights to Canada, all passengers must complete a CBSA Declaration Card where they declare if they are in possession of currencies and monetary instruments of a value equal or greater than CAD10 000 and hand over this declaration to a CBSA officer who may ask additional questions. For outgoing flights, CBSA will use a mix of intelligence information and random searches to target flights where passengers will be asked whether they are transporting CAD10 000 or more.

Failure to declare

564. Subsection 12(4) of the PCMLTFA imposes an obligation to any person arriving or leaving Canada to answer truthfully any questions from CBSA officers in respect of the reporting of currency or monetary instruments. The PCMLTFA provides for a maximum fine of CAD500 000 and a maximum jail term of five years for failure to report or for failure to cooperate with the border services officer when a report is submitted. This would include refusing to answer questions posed by the border services officer or failing to open packages or containers.

565. The CBCMIR form requires individuals to report the value of currency and monetary instruments being exported or imported, the country from which the funds are being exported or imported and key identifying information. If an individual fails to report the currency or monetary instruments whose value is equal to or greater than the CAD10 000 threshold CBCMIR, the CBSA officer may seize the currency. The individual CBCMIR can recover the currency or monetary instruments on payment of a monetary penalty ranging from CAD250 to CAD5 000. If the CBSA officer believes there are reasonable grounds to suspect that the funds are the proceeds of crime or linked to terrorist activities, the funds cannot be recovered.

Stop or restrain currency or bearer negotiable instruments

566. When an individual fully complies with the requirement to report on currency above the threshold, a CBSA officer who has reasonable grounds to suspect that information contained in the report or any other information may be relevant to the investigation or prosecution of a money laundering or terrorist financing offence is permitted to immediately disclose this information to law enforcement authorities. The CBSA officer may also provide information to FINTRAC where the information could be useful in the detection, prevention or deterrence of money laundering or terrorist financing.

567. Section 18 of the PCMLTFA grants authority to CBSA to seize unreported currency or monetary instruments. All seizures are reported to FINTRAC. If the border services officer suspects the seized money to be proceeds of crime or funds for use in financing a terrorist activity, it is forfeited to the Crown. Otherwise the CBSA will release the funds upon payment of a penalty ranging from

CAD250 to CAD5 000. The PCMLTFA allows the person from whom the funds were seized, or their owner, to appeal the seizure.

568. Under section 14 of the PCMLTFA, when an individual or entity does not have all the information needed to complete a report, the CBSA can temporarily retain the money until a border services officer is satisfied that they have been reported or the importer/exporter has decided not to proceed with the importation/exportation. If CBSA is not provided further information for seven days (30 days for mailed or items sent by courier), the money is forfeited to the Crown.

Retention of information

569. Every person or entity is obliged to complete a CBCMIR on the importation or exportation of currency or monetary instruments of a value equal to or greater than CAD10,000 in Canadian dollars or its equivalent in foreign currency. CBSA sends the reports to FINTRAC, which incorporates them into its database for analysis. The schedules to the Cross-Border Currency and Monetary Instrument Reporting Regulations set out the information that must be provided in the mandatory reports, including identifying information on the person transporting, mailing or shipping the currency or monetary instruments, as well as information on the person or entity on behalf of which the importation or exportation is made. Information on the amount and type of currency or monetary instruments must also be provided.

570. When unreported currency or monetary instruments are seized, a seizure report is prepared by CBSA officials and forwarded to FINTRAC. The seizure report includes, among other things, identifying information on the importer or exporter, the funds seized and the circumstances of the seizure.

Information accessible to the FIU

571. CBSA forwards all Cross-border Reports submitted by importers or exporters as well as seizure reports to FINTRAC electronically. FINTRAC analyzes this information in conjunction with other reports in order to identify potential money laundering and terrorist financing activities. The border services officer will report through the Occurrence Reporting System (ORS) an explicative summary of the circumstances and detailed information on the occurrence, the individual or any other information that the officers evaluate to be of importance for the intelligence community. This report is submitted to the Intelligence Directorate by the Regional Intelligence Officer for analysis. The relevant information is then disclosed to FINTRAC.

Co-ordination among customs, immigration and other related authorities

572. Domestic authorities co-ordinate their activities to stop and restrain the illegal cross-border transportation of currency and other monetary instruments through a variety of different mechanisms: the IPOC Units, Integrated Border Enforcement Teams (IBETs), and the sharing of cross-border reporting information by CBSA.

573. Within IPOC units, CBSA Regional Intelligence Officers provide expertise and intelligence on CBSA matters linked to the border concerning proceeds of crime investigations. CBSA Regional Intelligence Officers also provide a service to border services officers by responding at the ports of entry to incidents related to forfeitures of currency that may be associated to organised criminal groups. In return, CBSA receives expert advice and intelligence information from the IPOC partners to assist in CBSA matters.

574. Integrated Border Enforcement Teams (IBETs) are a Canada/U.S. initiative set out in the Smart Border Accord. These Teams combine the intelligence and law enforcement expertise of various agencies (Canada Border Services Agency, Royal Canadian Mounted Police, U.S. Customs and Border Protection, U.S. Immigration and Customs Enforcement and U.S. Coast Guard) and use a coordinated approach to identify and stop the high-risk movement of people and goods between the

ports of entry on the Canada - United States border. The CBSA and RCMP jointly operate IBETs. They share the responsibility for collecting critical information to develop criminal intelligence to assist in investigations relating to national security or criminality such as organized crime and human smuggling.

575. In addition, the CBSA sends Cross-border Reports and Seizure Reports to FINTRAC for analysis (see description above).

International co-operation and assistance amongst customs, immigration and other related authorities

576. Section 38 of the PCMLTFA allows the CBSA to enter into information sharing agreements with other countries that impose similar requirements in respect of reporting the importation or exportation of currency or monetary instruments. The CBSA is currently negotiating with the United States to enter into such an agreement.

577. Canada has a partnership agreement with the United States under the Shared Border Accord, allowing the governments of both countries to better manage the flow of refugee claimants at their shared border. This agreement allows for exchange of information between the two countries on:

- Advance Passenger Information and agreed-to Passenger Name Records on flights between Canada and the United States, including in-transit flights in order to identify risks posed by passengers on international flights arriving in each other's territory.
- Data related to Customs fraud, and agreed upon customs data pursuant to NAFTA, as well as any additional commercial and trade data, for national security purposes.
- Advance information on designated individuals and organizations for the purpose of freezing of terrorist assets.
- Refugee and asylum claimants in order to ensure that applicants are thoroughly screened for security risks.
- Marine in transit containers arriving in Canada and the United States.
- Anti-terrorism efforts through the Cross-Border Crime Forum and Project Northstar.

578. Canada entered into a trilateral agreement with the U.S and Mexico called the Security and Prosperity Partnership (SPP) in June 2005. The Partnership is a trilateral effort to increase security and enhance prosperity among the three countries through greater cooperation and information sharing. It includes efforts to develop and implement a comprehensive North American strategy for combating transnational threats to the three countries, including terrorism, organized crime, illegal drugs, migrant and contraband smuggling, and human trafficking.

Sanctions

579. Section 74 of the PCMLTFA provides for a maximum criminal fine of CAD500 000 and a maximum jail term of five years for failure to report or to cooperate with the border services officer when a report is submitted, such as falsely or not answering questions posed by border services officers or failing to open packages or containers as requested.

580. Part II of the PCMLTFA also provides that non-reported currency or monetary instruments is seized. Where there is no suspicion that the funds are linked to money laundering or terrorist financing, the owner may retrieve the forfeited funds after payment of penalties from CAD250 to CAD5 000 set out in the regulations. The funds cannot be retrieved when such a suspicion exists. Under section 18 of the PCMLTFA, unreported currency or monetary instruments in respect of which a border services officer has reasonable grounds to suspect are related to money laundering or the financing of terrorist activities are seized and forfeited and cannot be retrieved by the importer or exporter, subject to the appeals provisions.

581. In instances where a CBSA officer intercepts a foreign national or non-Canadian citizen suspected of involvement in money laundering or terrorist financing activities, they are instructed to

forward the file to CBSA's Organized Crime Section (OCS) at National Headquarters. OCS then analyzes the file based on in-house databases and research tools, and will request, if necessary, support from the appropriate units of partner agencies in law enforcement and intelligence, as well as FINTRAC. Once a portfolio-wide analysis has been completed, OCS contacts the originating officer with an assessment to assist that officer in deciding upon the proper course of enforcement action, possibly in concert with law enforcement partners, depending on the specific details of the case.

Confiscation, freezing and seizing measures

582. Generally, the provisions in Canada in respect of the confiscation, freezing and seizing of proceeds of crime or funds for terrorist activities also apply to the cross-border movements of currency or monetary instruments. When there is suspicion that the funds may be related to money laundering or terrorist financing, the various provision described in Section 2.3 of this report apply, in respect of the restraining of funds through criminal or civil procedures. Provisions under the PCMLTFA, the Criminal Code and other criminal or civil procedures for the confiscation, freezing and seizing of terrorist funds also apply to the cross-border movements of currency or monetary instruments. The measures are described in detail in Section 2.4.

Unusual cross-border movement of gold, precious metals or precious stones

583. Section 110 of the *Customs Act* gives CBSA officers the authority to seize goods where he or she has reasonable grounds to believe that the *Customs Act* or regulations have been contravened with respect to those goods. Gold, precious metals and stones are goods that are required to be declared upon importation. In cases where they are not properly declared, the CBSA can seize them with terms of release. In addition, section 101 of the *Customs Act* gives officers the authority to detain goods until he or she is satisfied that they have been dealt with in accordance with the *Customs Act* or any act of Parliament that prohibits, controls or regulates the importation or exportation of goods. This provision would apply to rough diamonds that are dealt with under the *Export and Import of Rough Diamonds Act*. CBSA officers also have authority under s.489(2) of the *Criminal Code* to seize goods where he or she has reasonable grounds to believe that the goods have been: obtained through the commission of an offence; used in the commission of an offence; or, will afford evidence of an offence under the *Criminal Code* or any other Act of Parliament.

Data protection

584. Section 36 of the PCMLTFA prohibits the unauthorised disclosure by a customs officer of information contained in a Cross-border currency and monetary instrument report or other information obtained in the course of enforcing the reporting requirement. Information forwarded to FINTRAC is subject to the privacy safeguards applicable to other information received by FINTRAC under the PCMLTFA. The CBSA sends the completed reports electronically, in a secure manner, to FINTRAC (see also comments in relation to FINTRAC detention of information in Section 2.5 of the report).

Additional elements

585. Canada has implemented the measures outlined in the Best Practices Paper. A number of these measures have been described earlier. In addition, the following measures are also in place:

- The threshold that triggers the reporting requirement is less than the threshold suggested by the FATF (CAD10 000 is roughly equal USD10 000 or EUR6 600).
- CBSA uses canine units, scanners and other sophisticated equipment to detect currency.
- The Bank of Canada stopped issuing the CAD1 000 bank notes in 2000. The largest note in active circulation is the CAD100 note.
- CBSA performs risk assessments and uses intelligence information to target all modes of transportation and travellers.
- CBSA officers are trained to detect suspicious behaviour by identifying indicators that are taught in various training courses.
- CBSA regularly performs examinations of passengers, vehicles, cargos, etc.

586. The Canada Border Services Agency (CBSA) uses a variety of technological tools to help stop the entry of contraband and dangerous goods into Canada. The use of detection technology tools enables CBSA officers to conduct effective, non-intrusive inspections, allowing them to focus on high-risk individuals and goods.

587. In the past, the CBSA's detection tools were developed primarily for the identification of contraband commodities (*i.e.* narcotics, weapons, child pornography, etc.). Recently, new legislation, policies, and programs initiated in support of fighting terrorism placed greater focus on border security. An integral part of Canada's plans in the fight against terrorism includes providing the necessary resources to purchase detection equipment. The CBSA has spent over CAD70 million in the last few years on new technology to improve border security.

588. Some of key interdiction technologies are: Gamma-ray Imaging Program (VACIS – Vehicle and Cargo Inspection System); the Remote Operating Vehicle (ROV), X-Ray Program and Ion Mobility Spectrometry (IMS) Technology. The CBSA also utilizes many smaller handheld tools. For example, the Snake Eye Camera is a self-contained, lightweight video inspection system. The Merlin Density Meter is a hand-held non-intrusive detection device that can indicate the presence of hidden contraband by measuring the density of a surface or an object. Videoprobes are used to inspect narrow spaces for hidden contraband in the air and land modes. The CBSA utilizes Contraband Outfitted Mobile Examination Truck, Chemical Biological Radiological Nuclear (CBRN) Detection Teams as well as Detector Dog Service.

Resources

589. The CBSA is part of the Public Safety and Emergency Preparedness (PSEPC) portfolio and is an integral component of Canada's national security approach along with other portfolio partners such as the RCMP, CSIS, etc. The CBSA integrates complementary business lines to protect public security and facilitate and control the movement of people and goods. Employing approximately 10 000 public servants, for which 7 500 are border services officers, the CBSA operates at 1 369 service points across Canada and nearly 40 locations abroad.

590. The 7 500 border services officers located at Canada's point of entry, among many other duties, are responsible to enforce the reporting requirement of Part II of the PCMLTFA. CBSA Intelligence officers located either in the regions or at Headquarters provide information or intelligence concerning individuals and organizations suspected of involvement in money laundering or terrorist financing activities to the officers. Then, senior program officers located at Headquarters coordinate and provide functional guidance on the program policies and procedures and address any issues relevant to the program's enforcement or administration.

591. The CBSA's current budget for the Cross-Border Currency Reporting Program is CAD2.43M yearly. CBSA will receive an additional CAD3.5M yearly in order to expand its intelligence mandate, cross border currency reporting, currency dog teams and deal with the seizure appeals. This will bring the CBSA's allocation to CAD5.93M yearly.

592. CBSA employees have relevant experiences and skills in sectors such as the law enforcement, customs, immigration, justice, and public safety as well as backgrounds in other government departments and international organizations.

593. The CBSA has implemented enhanced security measures and employees participate in security awareness sessions. A security program, and a range of policies and procedures to protect privacy, and prevent unauthorised disclosures of information, are in place and are upheld. They include the application of the need-to-know principle, guiding principles for the handling of sensitive and classified information and application of measures surrounding the analysis and disclosure processes. In addition, the clearance level required for CBSA employees involved in these issues demonstrates

the importance attached to the confidentiality of sensitive financial and personal information that is obtained and analyzed by its employees.

594. New CBSA officers graduate from the Port of Entry Recruit Training program at the CBSA training facility in Rigaud, Québec. Among other things, they are taught how to recognize and investigate based on key indicators, intelligence information, and suspicious activities and are provided with a web-based training for cross border currency related infractions as well as information related to money laundering and terrorist financing. Adjudicators working on behalf of the Public Safety Minister receive a half-day training course from the RCMP and Crown Prosecutor on money laundering and terrorist financing activities. A handout of the RCMP indicators as well as a booklet prepared by the RCMP on Money Laundering is provided at the training session.

Statistics

595. Statistics are available on the number of CBCMIRs involving movements of CAD10 000 or more in currency or monetary instruments.

Effectiveness

596. The number of CBCMIRs and seizure reports since 2002/2003 is as follows:

Report Type	2002-2003	2003-2004	2004-2005	2005-2006	2006-2007[1]	Total
Cross Border Currency Report	631	28 289	74 103	52 626	19 289	174 938
Seizure Report	19	1 080	1 718	1 880	625	5 322
Total	650	29 369	75 821	54 506	19 914	180 260

[1] Fiscal year 06-07 statistics include only what was received from CBSA up to September 30, 2006. CBSA receives CBCMIRs, captures the information electronically and transfers it to FINTRAC.

597. In 2005-06, 18% of FINTRAC's case disclosures were supported by cross-border currency and seizure reports.

598. Since the program implementation in January 2003, there have been over 5 000 currency seizures totalling more than CAD132 million. Approximately CAD34 million has been forfeited to the Crown, and penalties have been assessed in excess of CAD2 million. Over 500 seizures have resulted in forfeiture as suspected proceeds of crime or funds for the use of terrorist activities. Border services officers have collected over 100 000 cross-border currency reports.

599. Seizures related to cross-border currency transportation are classified into four levels based on the degree of concealment, previous seizures and the source of currency or monetary instruments. In levels one to three, a fine must be paid prior to release of the seizure. When seizures are made based on the suspicion it stems from proceeds of crime or terrorist financing (the fourth level), there are no terms of release. The following table describes the four levels of seizure related to cross-border currency interdictions and the fines that must be paid prior to the release of the seizure.

Level	APPLICATION	FINE
I	Applied when an individual or entity • has not concealed the currency or monetary instruments, • has made a full disclosure of the facts concerning the currency or monetary instruments on their discovery, and • has no previous seizures under the Act;	CAD250
II	Applied when an individual or entity • has concealed the currency or monetary instruments, other than by means of using a false compartment in a conveyance, or who has made a false statement with respect to the currency or monetary instruments, or • has a previous seizure under the Act, other than in respect of any type of concealment or for making false statements with respect to the currency or monetary instruments; and	CAD2500
III	Applied when an individual or entity • has concealed the currency or monetary instruments by using a false compartment in a conveyance, or • has a previous seizure under the Act for any type of concealment or for making a false statement with respect to the currency or monetary instruments.	CAD5000
IV	Applied when • CBSA Officers, who suspect on reasonable grounds that non-reported currency or monetary instruments are proceeds of crime or terrorist finances.	No terms of release

600. Since 2003, the RCMP has been asked to provide investigational assistance in 147 Level IV seizures conducted by CBSA officials. The following table provides a yearly breakdown of requests from CBSA to the RCMP's Money Laundering Program for assistance in these seizures.

Reports of Canada Border Services Agency (CBSA) Callouts				
	2003	2004	2005	Total
Number of Callouts	72	53	22	**147**

601. Since 2003, the Adjudications Division has seen numerous challenges of these enforcement actions. Level IV forfeiture enforcement actions tend to be highly litigious. Since 2003, of the 6 007 enforcement actions taken by the CBSA (at September 30, 2006), 666 of those actions have been appealed to the Recourse Directorate. Of those 666 appealed actions, only 55 have been cancelled and all funds have been returned. There are currently 45 active cases before the courts.

602. In 2004, the largest number of currency and proceeds of crime seizures (732) were made at customs points of entry located in the Pacific region, representing 45% of all seizures made. Customs officers in the Greater Toronto Area made 367 seizures, while officers in the Québec region made 338, officers at Niagara Falls/Fort Erie made 85, those in Windsor/St. Clair made 39, Prairie region made 27, Northern Ontario made 24 seizures and the Atlantic region made 4 interceptions. Combined, the Pacific, Quebec and the three regions of southern Ontario intercepted the bulk of all unreported currency and proceeds of crime totalling CAD42 301 608 million, accounting for 96% of the national total. In most cases, currency and proceeds of crime interceptions involved citizens of Canada, China and the United States. Canadians were involved in 10% (165) of the seizures totalling CAD4.1 million; citizens of China accounted for 21% (345) of the seizures totalling CAD7.6 million, and citizens of the United States were involved in 25% (401) of the interceptions yielding CAD18.1 million.

603. The following table shows the number and value of seizures made by type of currency for the year 2004.

Currency Type Seized	Number of Seizures	Value of Currency
Banker's drafts	26	CAD919,046
Bonds	3	CAD141,456
Cheques	54	CAD2,503,720
Currency	1450	CAD39,062,887
Money orders	20	CAD350,494
Other instr. in bearer form	1	CAD1,360
Stocks	1	CAD12,300
Traveller's cheques	60	CAD998,874
Treasury bills	1	CAD24,180
TOTAL	**1,616**	**CAD44,014,317**

Source: Cross-Border Currency and Proceeds of Crime Report 2004, Canada Border Services Agency.

604. This table shows the interceptions made in 2004, by referral type. The final two columns indicate the value and percentage (relative to the total) of seizures that were related to proceeds of crime.

Referral Type	Number of Seizures	Total Value of Currency Seized CAD	Value of which are Level IV – Proceeds of Crime CAD	Percent of Total
Selective referrals	1 382	**34 635 545**	7 412 250	21.4%
Lookouts	75	**5 284 884**	4 343 478	82.2%
Random referrals	38	**956 416**	374 202	39.1%
Targeting	17	**292 124**	29 787	10.2%
Canine indicators (DDS)	29	**753 210**	224 538	29.8%
Export examinations	56	**1 589 496**	633 796	39.9%
U.S. Customs referrals	5	**197 818**	44 284	22.4%
Other	14	**304 825**	0	0.0%
TOTAL	**1 616**	**44 014 318**	**13 062 335**	29.7%

Source: Cross-Border Currency and Proceeds of Crime Report 2004, Canada Border Services Agency.

2.7.2 Recommendations and Comments

605. Canada has a comprehensive system to protect the physical cross border transportation of currency and monetary instruments of a value of CAD10 000 or more and the law enforcement authorities have a clear understanding of the procedures that are in place in Canada for implementing SRIX. A range of methods and technologies are employed at the border to enhance capability relating to cross border currency enforcement. The legal authority for this is supported by a strategic and operational response that demonstrates close cooperation between agencies, especially enforcement agencies from the United States.

606. The effectiveness of Canada's cross border currency enforcement is demonstrated in the significant volume and value of currency seizures – 5 130 currency seizures totalling more than CAD132 million since January 2003. Seizures have been result of a broad range of enforcement methods, across a broad range of monetary instruments and currency, at various entry points into Canada - all of which indicates a broad enforcement response by Canadian authorities.

607. The assessment team however believes that competent authorities should further invest in the detection and investigation of out-going cross-border transportations of cash or any negotiable bearer instrument.

2.7.3 Compliance with Special Recommendation IX

Rec.	Rating	Summary of factors underlying ratings
SR.IX	C	▪ The Recommendation is fully met.

3. PREVENTIVE MEASURES - FINANCIAL INSTITUTIONS

Overview of legal and regulatory framework

PCMLTFA and its Regulations

608. To combat money laundering, the Canadian federal government enacted the Proceeds of Crime (Money Laundering) Act which received Royal Assent on June 29, 2000. To help fight terrorism, it enacted the Anti-Terrorism Act (Bill C-36) which came into force on December 24, 2001 and amended the Proceeds of Crime (Money Laundering) Act, which became the Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA).

609. The basis for the AML/CFT preventive legislation in Canada is the PCMLTFA that consists of five parts:

- Part I sets out record keeping requirements and requires the reporting of suspicious and prescribed financial transactions.
- Part II creates the obligation to report to Customs the importing or exporting of currency or monetary instruments of a value equal to or greater than CAD10 000 or its equivalent.
- Part III establishes FINTRAC as an independent agency to collect, analyze, assess and disclose designated information on financial transactions to assist in the detection, prevention and deterrence of money laundering and the financing of terrorist activities, while protecting Canadian's privacy.
- Part IV authorises the Governor in Council to make regulations.
- Part V creates offences, including the failure to report suspicious financial transactions and the prohibited use of information under the control of FINTRAC.

610. The PCMLTF Regulations implement a portion of Part I of the Act by requiring the financial institutions and financial intermediaries that are subject to the Act to identify their customers, keep certain records, report large cash transactions and international electronic funds transfers of CAD10 000 or more to FINTRAC and develop an internal compliance regime.

611. The PCMLTF Suspicious Transaction Reporting Regulations implement the remainder of Part I of the Act by requiring financial institutions and financial intermediaries to report financial transactions where there are reasonable grounds to suspect that they are related to money laundering or terrorist financing activities.

Recent amendment of the PCMLTFA and its Regulations

612. The Department of Finance issued a consultation paper in June 2005 outlining policy proposals to enhance the AML/CFT regime. These proposals included a series of new requirement such as the obligation to identify beneficial owners of client entities and to conduct enhanced due diligence for correspondent banking relationships and politically exposed persons. The adoption of a new registration scheme for money services businesses and of an administrative monetary penalties scheme was also proposed.

613. In October 2006, the Minister of Finance tabled Bill C-25, which proposed amendments to the PCMLTFA to expand the customer due diligence and transaction reporting requirements for financial institutions and financial intermediaries, set out a framework for the registration of money services businesses and extend the list of information that FINTRAC may disclose to law enforcement and

intelligence agencies. This Bill received Royal Assent in December 2006. However, a series of successive regulations is due to be adopted for the PCMLTFA to be fully effective.

614. Some new provisions of the PCMLTFA came into force on February 10, 2007 including technical amendments and information sharing in respect of cross border reporting regimes, FINTRAC record retention time limits, information sharing on charities and terrorist financing and a review of the Act by Parliament and the Office of the Privacy Commissioner. A "carve out" for suspicious transaction reporting by legal counsel also took effect.

615. On March 10, 2007, in the format of a pre-publication in the Government Gazette, the Canadian Department of Finance opened two proposed regulations (*Proceeds of Crime (Money Laundering) and Terrorist Financing Registration Regulations* and *Regulations Amending Certain Regulations Made Under the Proceeds of Crime (Money Laundering) and Terrorist Financing Act*) to consultation[55]. The consultation period ended on April 9, 2007. Quite a large number of financial institutions, financial sector associations and professional associations sent representations regarding the feasibility of the proposed amendments and possible coming-into-force dates for the new provisions. Overall, the assessors were told that stakeholders were supportive of the proposed enhancements to Canada's regime. However, with regard to the proposed registration system, some of them have suggested modifications to the proposed amendments to reduce the compliance burden[56].

616. On June 27, 2007, the *Regulations Amending Certain Regulations Made Under the PCMLTFA* were enacted and published in the Canada Gazette (Part II). A second package of regulatory amendments, the *Proceeds of Crime (Money Laundering) and Terrorist Financing Registration Regulations* was published, which sets out a framework for the registration of MSBs.

617. Additional amendments are necessary for the regulations to implement fully the legislation. For instance, amendments to the PCMLTF Regulations and PCMLTF Suspicious Transaction Reporting Regulations were pre-published on June 30, 2007 to address some of the measures that still need to be adopted. The proposed amendments extend coverage of the PCMLTFA to three non-financial professions (see Section 4.1 of the report). A proposed PCMLTF Administrative Monetary Penalties Regulations also set out specific measures for an administrative monetary penalties scheme. These proposed amendments were open to consultation until August 2007[57].

---

[55] Draft regulations in Canada must be pre-published in Part I of the Canada Gazette, before they can be made. Pre-publication in Part I of the Canada Gazette gives various interested groups and individuals, as well as Canadians in general, a final opportunity to review and comment on a proposed regulation at the last stages of the regulation-making process, before it is enacted and published in Part II of the Canada Gazette. Pre-publication also gives interested parties, and those stakeholders previously consulted at the beginning of the regulatory process, the opportunity to see whether the final draft proposal is in keeping with previous consultation drafts and to comment on the implementation timeline.

[56] The regulatory impact analysis of the *Proceeds of Crime (Money Laundering) and Terrorist Financing Registration Regulations* of 7 June 2007 states the following: "for example, as requested by a group of money services businesses, amendments to the Regulations exempt the sector from customer due diligence requirements when they enter into a service agreement with a publicly traded company or public body. Other exemptions to the client identification and record-keeping requirements have been added to alleviate the compliance burden for securities dealers and other sectors. As proposed by banks and credit unions, the definition of politically exposed foreign persons has been limited to fewer family members and the timeframe for the identification of such persons has been extended. Following discussions with banks, the record-keeping requirements applicable to financial entities for funds transfers of CAD 1 000 or more have been limited to international electronic funds transfers and domestic SWIFT MT103 transfers. Likewise, the obligation to keep a record of the address of the beneficiary for such transfers has been removed from the amendments to the Regulations. Many sectors have expressed their concerns regarding the amount of information that would have to be collected on partnerships and other entities if the published amendments were to come into force. To reduce this compliance burden, the amendments to the Regulations no longer require persons and entities to obtain information on the partners or directors of an entity other than a corporation".

[57] The amendments were enacted on 26 December 2007 and come into force in December 2008, see http://www.fin.gc.ca/news07/07-105e.html.

618. The present report takes into account (for analysis and rating purposes) the amended version of the PCMLTFA dated February 10, 2007. The report also takes into account (for analysis and rating purposes) the provisions of the PCMLTF Regulations that have been in force since June 30, 2007 (*i.e.* in relation to correspondent banking relationships, shell banks and a broader set of information released in FINTRAC disclosures). However, the provisions of the PCMLTF Regulations and the PCMLTF Suspicious Transaction Reporting Regulations also published on June 27, 2007 that will enter into force on June 23, 2008 (such as information to collect on beneficiaries and the politically exposed foreign person's related requirements) have not been analysed by the assessors. However, the existence of such provisions has been taken into account when drafting the recommendations given to Canada to improve its AML/CFT regime. Annex 1 of the report provides an inventory of the changes brought to the Canadian AML/CFT regime since December 2006.

Enforceability of AML provisions issued by competent authorities

619. There are 14 legislative bodies in Canada: the Parliament of Canada, and the legislatures of 10 provinces and three territories. Statutes enacted by these legislative bodies are primary legislation. Regulations are made under a statute or an Act by the government department or ministry administering that Act (see Part IV of the PCMLTFA) and are another form of law. This is the generally-recognized hierarchy of authority: the Constitution, human rights legislation, other legislation, regulations, case law from higher courts, other case law, treaties/international law and doctrine.

620. FINTRAC (for all reporting parties), OSFI (for Federally Regulated Financial Institutions) and IDA (for securities dealers) have developed guidelines to assist reporting entities understanding their obligations under the Act and associated regulations. During consultations on the proposed Regulations, stakeholder groups have identified the need for guidelines to assist persons and entities understanding their obligations under upcoming regulatory changes.

621. Repeated reference is made in this section of the report to various types of guidance issued by regulatory agencies with respect to the financial sector's AML/CFT obligations and the regulators' approach to compliance. The extent to which such guidance can be deemed to be "other enforceable means" is central to the evaluation of the financial sector preventive measures and the following summary reflects the view taken by assessors on the main forms of guidance.

622. Within the FATF, "other enforceable means" refers to guidelines, instructions or other documents or mechanisms that set out enforceable requirements with sanctions for non-compliance, and which are issued by a competent authority (*e.g.* a financial supervisory authority) or an SRO. The sanctions for non-compliance should be "effective, proportionate and dissuasive".

OSFI guidance

623. In relation to AML/CFT issues, OSFI has issued two pieces of guidance. Firstly, there is the Guideline E-13 entitled "Legislative Compliance Management", dated March 2003, which is a general guideline on managing regulatory risk that "*conveys OSFI's expectations of federally regulated financial institutions regarding controls through which they manage regulatory risk inherent in their activities worldwide"*. Second, there is Guideline B-8 entitled "Deterring and Detecting Money Laundering and Terrorist Financing", published originally in April 2003 and amended in November 2004 after publication of the Basel Committee paper "Consolidated KYC Risk Management". B-8 is applicable to domestic and foreign banks, trust & loan companies and life insurance companies, referred to collectively as federally-regulated financial institutions (FRFIs) although the text focuses more on banking related matters. OSFI advised the assessors that B-8 is scheduled for update and amendment after the introduction of the new regulations.

624. Based on the definition of "other enforceable means", the assessors have given consideration to a number of basic requirements when considering whether OSFI Guideline B-8 can be considered as "other enforceable means". These requirements are as follows:

1) *A document or mechanism that sets out enforceable requirements addressing the issues in the FATF Recommendations.* Guideline B-8 only addresses a very limited range of AML/CFT issues (essentially Recommendation 15 and to a lesser extent Recommendations 5, 6, 9, 22, 18 and 29). In relation to customer identification for instance, the Guidance essentially addresses some enhanced due diligence situations and suggests that beneficial ownership identification is particularly important. The most comprehensive part of the guideline deals with internal control procedures to prevent ML and TF (role and position of the CAMLO, oversight by the Board, compliance reporting processes, self-assessment program, independent procedures testing, etc.) in relation to Recommendation 15. Finally, the Guideline refers FRFIs to the website of FATF, FINTRAC and BIS and encourages them to familiarise themselves with the various standards contained therein. Looking at whether OSFI Guideline B-8 sets out enforceable means, the assessment team has considered:

   - *The nature of the document*: OSFI itself defines the guidelines it publishes (see OSFI website) as "*essentially best or prudent practices that it expects financial institutions to follow. Guidelines are used to set standards to govern industry activities and behaviour*". OSFI has indicated that its guidelines aim at *promoting* the adoption of policies and procedures designed to control and manage risk. Based on these clarifications and looking at the current form of such guidelines, they appear to be more similar to general advice than mandatory obligations and there is no contrary indication that the guidelines place mandatory obligations on FRFIs.
   - *The language of the document*: OSFI has intentionally opted for a gradation of the language in the B-8 Guidance (from FRFIs "must" to FRFIs "should consider" or FRFIs "are encouraged". Except on four occasions where the wording of the guidance is assertive (using a "must"[58]) the guidelines are generally worded in a permissive manner (FRFIs "should" do or "should consider"; OSFI "encourages", OSFI "recommends", OSFI "suggests") which do not adequately substantiate OSFI's expectations of FRFIs and leaves a great deal of discretion in the hands of the FRFIs. So, even if OSFI addresses the FRFIs' compliance with the Guideline in its regular on-site assessments, it is not clear which provisions of these guidelines could be considered as "requirements", most of them being "recommendations" or "best practice".

2) *The document/mechanism must be issued by a competent authority (e.g. a financial supervisory authority) or an SRO.* OSFI regulates and supervises federally regulated financial institutions and administers financial institution governing statutes. As a financial supervisory body, it is a competent authority.

3) *There are sanctions for non-compliance, which should be effective, proportionate and dissuasive and there is evidence that effective and dissuasive sanctions have been applied in practice.* When reviewing the compliance of FRFIs with the AML/CFT regime, OSFI explicitly includes in its scope and objectives the assessment of compliance with OSFI Guideline B-8. Sanctions are available to OSFI based on a failure of the financial institution to conduct its business in a safe and sound manner in relation to AML/CFT failings and OSFI Guidelines are enforceable to ensure "safety and soundness" within a financial institution. To encourage financial institutions to implement the AML/CFT provisions (including OSFI Guidance), OSFI's related supervisory powers are very much focused on early intervention

[58] 1. "*To identify their level of exposure to potential MLTFA and the associated risks, FRFIs must understand the nature of the risks associated with the different parts of their operations*"; 2. "*With respect to introduced business, FRFIs must obtain the necessary customer information for their records prior to, at, or at a reasonable time after, the time that the business is accepted*"; 3. "*The board of directors and senior management must be strongly committed to ensuring that measures designed to address risks associated with these activities (that are risky) are implemented*" and 4. "*Front-line staff plays an essential role in implementing anti- MLTFA measures and, therefore, must receive appropriate training to understand problems associated with MLTFA, the financial institution's anti- MLTFA policies, and the proper application of procedures*".

and OSFI strongly relies on a remedial program through the normal supervisory process to address compliance failures.

- *Applicable sanctions*. OSFI has a range of supervisory tools and sanctions at its disposal, including written interventions, staging, directions of compliance, placing terms and conditions in the FRFI's Order To Commence And Carry On Business (operating licence) and imposing an Administrative Monetary Penalties (AMP) under the OSFI Act.

- *Sanctions that have been applied*:

  (a) OSFI issues supervisory letters after each AML/CFT assessment. The letters contain "required actions" on compliance issues or "recommendations". In most cases, interventions in the form of "recommended action" (vs. "required action") have been applied for failing to implement OSFI Guidance B-8 as a result of OSFI inspections. OSFI issues "Recommended actions" to address deficiencies in risk management controls or *other supervisory requirement not directly related to a legal requirement*. However, when OSFI feels it necessary to deliver a stronger signal to the financial institution, they may use the term "require" as more prescriptive language when dealing with deficiencies under B-8. This may be because the lack of compliance with the B-8 provision resulted in a markedly weaker AML program overall. So, for example, OSFI will sometimes say they "require" a self-assessment and at other times "recommend" it. OSFI claims that there is indeed no procedural difference applied to the terms "requirement" and "recommendation" and that FRFIs work to quickly implement the necessary changes, whether required or recommended.

  (b) Beyond the supervisory letters, OSFI has a range of supervisory tools (including sanctions) at its disposal. Staging is a supervisory measure implemented by the Supervisory Sector of OSFI based on its overall view of the level of risk in the FRFI balanced against the effectiveness of the risk controls. It results in progressively more and more intense oversight and detailed intervention by OSFI on the issues that led to the Staging. It also results indirectly in a financial charge to the staged deposit-taking financial institutions as it attracts a higher OSFI assessment fee and may attract a higher deposit premium by CDIC. Cumulatively, in the period 2004-2006 inclusive, OSFI staged 4 financial institutions for AML/CFT control deficiencies (2 of them on this sole basis). The AML/CFT deficiencies giving rise to the staging were a mixture of regulatory non-compliance and non-compliance with B-8 requirements. The amount of OSFI and CDIC surcharges ranged from CAD 45 000 up to CAD 500 000.

  (c) Supervisory tools such as direction of compliance or prudential agreements (see Section 3.10 for further details) are available but have never been used for a failure to implement OSFI Guidance or even for any AML deficiencies. OSFI considers that such actions have never been necessary, as weaknesses have always been adequately addressed with measures taken under (a) and (b) above.

  (d) OSFI can issue Administrative Monetary Penalties (AMPs) but these penalties only apply in case of a contravention of a provision of a financial institutions Act (such as the Bank Act) or of a direction of compliance, terms and conditions or a prudential agreement (see OSFI ACT, art. 25). They cannot be administered directly in case of non-compliance with the PCMLTFA, its regulations or a fortiori OSFI Guidance.

625. In conclusion, sanctions for non-application of OSFI Guideline B-8 do not appear to be sufficiently effective, proportionate and dissuasive. OSFI essentially use written recommendations as a main supervisory tool and in some limited occasions, closer monitoring (only staging (to stage 1) was used in a limited number of cases although very serious deficiencies were identified in a number of assessments). These supervisory tools have been the only ones that OSFI has used so far for failure to implement Guideline B-8. Looking at the language of the guidelines and the sanctions that have been applied by OSFI, the assessors' believe that OSFI Guidelines cannot be considered as "other enforceable means".

IDA guidance

626. The IDA is the national self-regulatory organisation of the securities industry in Canada and regulates the activities of investment dealers in terms of both their capital adequacy and conduct of business. The IDA is the front-line regulator of full securities dealers. A number of provisions in provincial securities regulations recognize IDA rules as an alternative to provincial regulations, generally by explicitly granting or allowing the granting of exemptions from the provincial rules to members who abide by IDA rules.

627. The IDA regularly publishes By-laws, Regulations and Policies that set out detailed requirements to be implemented by its members in carrying out their business (such as opening account rules, recordkeeping requirements, etc. that are applicable in the AML/CFT context). IDA By-laws, Regulations and Policies use prescriptive language (securities dealers "must" do). Penalties for breaches of the By-laws, Policies and Regulations include a wide range of sanctions for registered employees and member firms and have been used by IDA in the past (see section 3.10 of the report). The assessors took the view that IDA By-laws, Policies and Regulations are legally enforceable and can be considered as "other enforceable means".

628. In the AML area more specifically, the IDA published "*Deterring ML activity, A Guide for Investment Dealers*" in October 2002. This Guide is intended to highlight the key elements for a Canadian investment dealer to consider in developing an effective AML program. The language of the document clearly states that securities dealers are encouraged to take certain AML/CFT measures. There is no sanction directly applicable for a failure to comply with an AML/CFT measures contained in the Guide. For the purpose of this report, this Guide is considered as non-binding guidance which is neither law, regulation nor other enforceable means as defined by the FATF.

FINTRAC guidance

629. Under the PCMLTFA (Section 40(e)), FINTRAC has responsibility for ensuring compliance, reporting, record-keeping and client identification requirements of the reporting parties. FINTRAC has therefore developed a series of guidelines defined by FINTRAC as "'helpful hints"[59] that do not remove the responsibility for reporting entities to be familiar with or comply with the PCMLTFA and related Regulations. Such guidelines have therefore been developed by a competent authority that deals with AML/CFT issues. The language of the FINTRAC Guidance is direct, forceful and explicit with clear direction and requirements and points out how criminal sanctions exist to tackle breaches on record-keeping requirements set out by the PCMLTFA and the PCMLTF Regulations. However, FINTRAC Guidelines in themselves do not impose any mandatory requirements with sanctions for non-compliance, and indeed state in the preamble to each guidance note that "*it is provided as general*

[59] The list of FINTRAC Guidance is as follows (as of June 2007): 2 – Suspicious transactions; 3A – Submitting Suspicious transactions Reports to FINTRAC Electronically; 3B - Submitting Suspicious transactions Reports to FINTRAC By Paper; 4 - Implementation of a Compliance regime; 5 -Submitting Terrorist property Reports; 6-Record keeping and Client Identification; 7A – Submitting Large Cash Transaction Reports to FINTRAC Electronically; 7B - Submitting Large Cash Transaction Reports to FINTRAC By Paper; 8A – Submitting Non-SWIFT Electronic Funds Transfers Reports to FINTRAC Electronically; 8B - Submitting SWIFT Electronic Funds Transfers Reports to FINTRAC Electronically; 8C - Submitting Non-SWIFT Electronic Funds Transfers Reports to FINTRAC By Paper and 9 – Alternative to Large Cash Transaction Reports to FINTRAC.

information only. It is not legal advice and is not intended to replace the Act and Regulations". Furthermore, under the PCMLTFA, FINTRAC cannot impose penalties or sanctions but only has the option of referring cases to law enforcement (see Section 3.10). For the purposes of this report, the requirements of such Guidelines cannot be considered as "other enforceable means".

3.1 Risk of money laundering or terrorist financing (R.5 – 8)

Application of AML/CFT obligations to certain sectors

630. As described in the FATF Recommendations, a country may decide not to apply certain AML/CFT requirements, or to reduce or simplify the measures being taken, on the basis that there is a low or little risk of ML or TF in a given business sector. The country may decide the extent to which certain measures need to be applied on a systemic basis by each general category of financial institution, as well as by various subsets within each industry.

631. In Canada, certain financial institutions that undertake financial activities, as defined by the FATF Recommendations are not currently covered by the AML/CFT regime. These sectors or activities[60] are as follows (excluding entities that are caught because they also engage in financial activities under the regime): financial leasing; factoring; finance companies (*i.e.* entities specialized in consumer lending, credit cards, equipment financing and small business loans that are not loan companies); providers of e-money; Internet payment providers[61]; and cheque cashiers[62] when only cashing cheques issued to denominated persons[63]. Canada considers that these entities pose little or no threat of money laundering/terrorist financing. It is worth noting that these different activities represent a not insignificant part of the financial sector: for instance, the three finance companies that are members of the ACFC (Association of Canadian Financial Corporations) serve 1.74 million customers and have CAD 8 billion in assets. This is still smaller than the banking sector which has 1.5 trillion in assets.

632. Canada's AML/CFT risk-based approach was described to the assessment team as follows[64]: the starting point is that government first looks at ML/FT risks to determine whether particular parts of the financial sector should be covered by AML/CFT legislation. Based on that risk assessment, decisions are then made to regulate or not that sector for AML/CFT purposes. Canada indicated that this general approach has applied with the exception of finance companies which approached the Department of Finance in 2001 to clarify that their risk of AML/CFT was low and they should not be caught by the regime. Based on this, a decision was made not to regulate the sector but subsequent voluntary reporting of suspicious transactions has resulted in that sector remaining under monitoring by competent authorities in order to ensure that emerging risks are addressed if necessary.

633. When considering in more details the process that takes place to assess ML/TF risks, the assessment team was told that risk assessments are presented and discussed at meetings involving relevant departments and agencies, including the RCMP, the Department of Justice and FINTRAC. The assessment team was advised that the Department of Finance looks at the sector structure (types

60 That came to the knowledge of the assessors.

61 Internet payment and e-money providers are only subject to the Act if they also offer funds remittance or transmission services and, as such, would be considered money services businesses.

62 Cheque cashing businesses that also offer money remittance services are included in the definition of MSBs under the PCMLTFA and are therefore subject to the requirements of the PCMLTFA.

63 Credit card issuers are covered by the AML/CFT regime. The assessment team was advised that VISA, Mastercard and American Express are the only general purpose credit cards available in Canada. As a result of VISA and Mastercard internal rules, credit cards are only issued by regulated and supervised financial institutions, both for PCMLTFA and prudential purposes. Finance companies that are not caught under the PCMLTFA can also issue general purpose credit cards (in addition to stored value cards) but do so through subsidiaries that are regulated for AML/CFT and prudential purposes.

64 At the different stages of the evaluation process, the assessment team was provided with varying descriptions of processes in place in Canada to assess ML/TF risks. Some information in that Section was provided in January 2008.

of products and clients involved, etc.) and takes into consideration risk analysis carried out at national and international level. However, no formal minutes or documentation were kept in respect of the decisions to regulate or not a given sector for AML/CFT purposes and consequently the risk assessments underlying the decisions, if any, could not be obtained by the assessment team. Limited documentation was provided for a risk assessment conducted on financial leasing (see below). The following paragraph illustrates how sectors were not included within the coverage of the PCMLTFA.

634. Importantly, Canada subsequently clarified that its risk based approach is centred around the principle that financial sectors will be brought into the AML/CFT regime only if there is a proven risk of ML/TF.

635. Canada's approach to risk is not in line with the FATF approach to risk as defined in the Methodology where a list of activities and operations must be covered by the AML/CFT regime unless there is a proven low risk of ML of TF. Canada has taken the opposite approach to extend coverage of the PCMLTFA only to activities for which there is a proven ML/TF risk. This approach is even more problematic since the risk assessment process carried out by Canada to reach conclusions on the exposure of certain sectors to ML/TF risks is either non-existent or very fragmented and ad-hoc. In the cases where such a process has taken place, the risk assessment has provided clear indicators that certain sectors were at risk (based in particular on studies carried out by the RCMP). Despite this, the decision has been taken not to cover these sectors from the AML/CFT framework (this is the case for financial leasing, stored value cards and white label ABMs – see Section 4.4 of the report). In other scenarios, no proper risk analysis has been carried out or at least there is no evidence that such analysis has taken place. However, based on the general assumption that these sectors present low ML/TF risks or that ML or TF activities can be prevented and detected in these sectors through other entities subject to the PCMLTFA, the decision has been taken not to bring them under the PCMLTFA coverage (this applies to finance companies, factoring, cheque cashiers, Internet payment and e-money providers).

636. A clear example of the approach taken is provided by the financial leasing sector, as a distinct activity, "due to the relatively low money laundering and terrorist risks involved". The assessors were referred to a study undertaken by the Department of Finance ("Financial leasing industry in Canada and ML") but this was only an undated discussion draft. This paper clearly identifies the risks attached to financial leasing activities and suggests some options to regulate the sector to address its vulnerabilities vis-à-vis ML (such as amending the criminal code). The paper concludes that further consultation is necessary before taking a decision to regulate the sector for AML/CFT purposes. However, no further action has been taken by competent authorities to follow-up the conclusions of the report and at the time of the on-site visit, no further steps had been taken to include the financial leasing sector in the scope of the Act despite the demonstrated risk of money laundering (as underlined in the paper) attached to this sector.

637. Finance companies have not been subject to any risk assessment and, as a sector, they remain unregulated. There is the perception that since they do not take deposits, they are not in a position to launder money when in fact, sub-prime lending offers many opportunities through taking out loans and then using illegal funds for repayment. It is worth mentioning that three big finance companies have formed a professional association (ACFC, Association of Canadian Financial Corporations) and decided to implement AML/CFT standards on a voluntary basis; they also regularly send voluntary STRs to FINTRAC.

638. According to another undated document entitled "Risk Assessment Issues" (presented more as a policy paper) received post evaluation in response to assessors' requests for additional information on risk assessments, certain areas such as factoring, stored value cards or e-money, Internet payment providers and financial leasing are either under consideration or have been assessed as low risk. However, the document did not fully address assessors' request to see the risk assessment itself.

639. In general, the assessors believe that the justifications underlying decisions to exclude certain categories of financial institutions or activities from the AML/CFT regime are either insufficient or non-existent and that the approach applied by Canada to do so is the opposite of the agreed approach by the FATF in the 40 Recommendations.

640. Canada should rely on a more comprehensive, thorough and formal risk assessment process. This should typically involve meetings and discussions with any relevant AML/CFT stakeholders (Department of Finance, FINTRAC, OSFI, RCMP, Department of Justice, etc.) as it is already the case but also representatives of different sectors of each industry and with their trade associations; a review of money laundering investigations, prosecutions, and convictions in each industry and consideration of law enforcement views; and consideration of international standards (including those of the FATF). Most importantly, the underlying principle should be that the financial activities referred to in the FATF standards should be covered unless there is a proven low risk of ML/TF.

Risk-based approach taken by financial institutions

641. Canada uses a risk-based approach throughout its financial sector AML/CFT regulations. The regulations identify lower risk sectors, products and customers (in close co-operation with the private sector) and determine the related measures that should be in place. The government has defined a common standard for most situations and allows reduced measures in certain specific lower-risk situations.

Use of a Risk-Based Approach in Supervision of Compliance by Competent Authorities

642. The competent authorities use a risk-based approach when supervising reporting entities for compliance with the legislation. FINTRAC and OSFI have taken a risk-based approach in developing and implementing their supervisory programs.

643. Under the PCMLTFA, FINTRAC is responsible for ensuring compliance with the PCMLTFA and its Regulations. The legislation permits FINTRAC to enter into agreements with regulators that supervise reporting entities. While FINTRAC does not devolve its responsibility for ensuring compliance to these regulators, it assesses the risks related to the regulator's supervisory activities and plans accordingly. For instance, FINTRAC may target relatively fewer compliance resources to a particular sector, such as federally regulated financial institutions, where a MOU with OSFI is in place.

644. When assessing the level of risk for reporting entities, FINTRAC looks at a range of factors, including such elements as open source information, reporting volumes, observations gleaned from outreach activities, voluntary information FINTRAC has received on non-compliance, results of compliance questionnaires completed by reporting entities, other database checks, information from regulators, quality and quantity assurance reviews, and the results of compliance examinations.

645. OSFI's supervisory powers are established through the OSFI Act. These set out the framework and limitations within which federally regulated financial institutions can operate in Canada. Within this framework, OSFI uses a risk-based approach to supervision to effectively allocate staff and resources, as well as to allow for private sector development and innovation. Under its supervisory framework, OSFI applies more supervisory resources when a financial institution's risk profile increases – when, for instance, the institution takes on new types of business or faces risks to its solvency.

646. OSFI uses a number of factors to determine the prioritization of AML/CFT assessments. These factors include: the size of the financial institution; the number of branches in Canada and the number of subsidiaries and branches outside Canada; the product mix and client base of each institution; and OSFI's overall view of the institution's compliance and risk management structure.

Scope of the PCMLTFA

647. Article 5 of the PCMLTFA defines the persons and entities to which the Act applies. The Act lists on the one hand, specific categories of entities regulated by federal or provincial acts and, on the other hand, persons or entities engaged in some specific businesses, professions or activities explicitly referred to in the text or further specified in the regulations. The list of persons or entities is as follows:

- Authorised foreign banks within the meaning of section 2 of the Bank Act in respect of their business in Canada, or banks to which that Act applies.
- Cooperative credit societies, savings and credit unions and *caisses populaires* regulated by a provincial Act and associations regulated by the Cooperative Credit Associations Act.
- Life companies or foreign life companies to which the Insurance Companies Act applies or life insurance companies regulated by a provincial Act.
- Companies to which the Trust and Loan Companies Act applies.
- Trust companies regulated by a provincial Act.
- Loan companies regulated by a provincial Act.
- Persons and entities authorised under provincial legislation to engage in the business of dealing in securities or to provide portfolio management or investment counselling services.
- Persons and entities engaged in the business of foreign exchange dealing.
- Life insurance agents and brokers.
- Persons or entities engaged in the business of "remitting or transmitting funds by any means or through any person, entity or electronic funds transfer network or issuing or redeeming money orders, traveller's cheques or other similar negotiable instruments" (namely money services businesses).
- Departments and agents of Her Majesty in right of Canada or of a province when it accepts deposit liabilities or sells or redeems money orders in the course of providing financial services to the public).

3.2 Customer due diligence, including enhanced or reduced measures (R.5-8)

3.2.1 Description and Analysis

Recommendation 5

648. Customer's identification measures in Canada are currently insufficient to meet the FATF standards[65]. The assessors believe that the current practice, in the bigger financial groups at least, may show better results and be *de facto* closer to the international AML/CFT requirements.

Anonymous and numbered accounts

649. There is no direct prohibition on opening anonymous accounts but basic CDD exists where financial institutions have been required since 1993 to obtain information on and ascertain the identity of all new account holders[66]. The assessment team was told that neither OSFI/FINTRAC nor law enforcement authorities in the course of an investigation have ever found an instance of a financial institution operating an anonymous account.

650. Numbered accounts are permissible. This would be the case for instance for corporate acquisitions where the premature circulation of information could jeopardize the transaction. In this case, the ordinary records of this account may only have a number with no name attached. However, even in those circumstances, Canada has informed the assessors that someone in the financial institution has to ascertain the existence of the corporation that is the account holder, and be able to link this account with the actual account holder. The compliance officer has in principle complete access to the customer's information. However, there are no detailed rules or guidance on how such

[65] The substantial compliance with Recommendation 5 should improve as the new regulations that Canada enacted on June, 27 2007 come into force on June, 23 2008.

[66] Under Section 9.2 of the PCMLTFA, financial institutions cannot open an account when the customer's identity has not been obtained. This provision will come in force in June 2008.

accounts should be managed by the financial institutions. The obligation for compliance officers to have access to CDD information is not clearly stated either.

651. In the securities area, certain firms may permit confidential accounts for appropriate reasons, such as a client's prominence or due to concerns for personal safety. The IDA Guidance on Deterring ML sets out that sufficient documentation identifying the underlying owners should be obtained and on file with the firm and available to appropriate compliance staff.

Account opening and CDD

652. *General*. The PCMLTF Regulations establish the circumstances where customer identification is required. Section 53 requires financial institutions to ascertain the identity of any individual in respect of whom they have to keep a large cash transaction record (for cash transactions of CAD 10 000 or more) at the time of the transaction. FINTRAC has developed guidance in relation to client identification for the following financial sectors: financial entities, MSBs, securities dealers, life insurance companies, brokers and agents and foreign exchange dealers. As far as customer identification requirements are concerned, FINTRAC guidelines expand very little on the provisions set out in the PCMLTFA and related regulations.

653. *Financial entities*[67]. Financial entities, as the backbone of the industry, have additional client identification requirements (Section 54 of the PCMLTF Regulations and FINTRAC Guideline 6G "*Record Keeping and Client Identification for Financial Entities*") in certain circumstances, namely:

- Signature cards[68]: the institution must identify any individual who signs a signature card. In cases where a business account which has more than three individuals authorised for it, the institution must identify at least three of the individuals.
- Where the account holder is an entity, the financial institution must, in addition to identifying the persons authorised to act with respect of the account, confirm the existence of the entity[69] and, in the case of a corporation, ascertain the name and address of the corporation and the names of its directors.
- Foreign currency exchange transactions in which an individual conducts a foreign currency exchange transaction of CAD 3 000 or more at the time of the transaction.
- electronic funds transfers[70] of CAD 3 000 or more.

654. *Trust companies*. Trust companies must identify any person who is the settlor of a personal trust (other than a trust created by a will) or who is authorised to act as a co-trustee of any trust (Section 55 of the PCMLTF Regulations). Trust companies must also confirm the existence of any entity (for corporations the name and address must also be ascertained) that is the settlor of an institutional trust. The existence of an entity that is authorised to act as the co-trustee of any trust and, in the case of a corporation, its name and address must be ascertained as well as all persons (up to three) who are authorised to give instructions with respect to the entity's activities as co-trustee.

655. *Life insurance companies, agents or brokers*. Life insurance companies, agents or brokers who receive CAD 10 000 or more for an annuity or life insurance policy over the duration of the product, must keep a client identification record (Section 56 of the PCMLTF Regulations and FINTRAC

---

67 In the PCMLTF Regulations,: "financial entities" are banks, credit unions, *caisses populaires*, trust and loan companies, agents of the Crown that accept deposit liabilities.

68 Signature card in respect of an account means any record that is signed by a person who is authorised to give instructions in respect of the account.

69 Entity" in the PCMLTFA means a body corporate, a trust, a partnership, a fund or an unincorporated association or organisation.

70 "Electronic funds transfer" means the transmission – through any electronic, magnetic, or optical device, telephone instrument or computer – of instructions for the transfer of funds, other than the transfer of funds within Canada. In the case of SWIFT messages, only SWIFT MT 100 and SWIFT MT 103 messages are included".

Guideline 6A "*Record Keeping and Client Identification for Financial Entities*"). When the transaction referred to above is conducted on behalf of an entity, the insurance company, broker and agent must also confirm the existence of every entity, and if such entity is a corporation ascertain its name and address, and the names of the corporation's directors within 6 months of creating this record[71].

656. *Securities dealers*. Securities dealers have to identify any individual who is authorised to give instructions for any account the dealer has to maintain a record for. In the case of a business account, the securities dealer does not have to identify more than three individuals who are authorised to give instructions for an account (Section 57 of the PCMLTF Regulations and FINTRAC Guideline 6E "*Record Keeping and Client Identification for Financial Entities*"). In addition, where the account is opened in the name of an entity, the securities dealer must confirm its existence and, in the case of a corporation, ascertain the name and address of the account holder and the name of its directors.

657. The identification procedures of securities firms start with the basic KYC requirements mandated by the PCMLTF Regulations. IDA Regulations, Policies and By-Laws add further requirements. IDA Policy 2 ("*Minimum Standards for Retail Account Supervision*") sets out precise requirements for opening new accounts. To comply with the "Know-Your-Client" rule each IDA Member must establish procedures to maintain accurate and complete information on each client. The first step towards compliance with this rule is completing proper documentation when opening new accounts. The IDA has elaborated a "*New Client Application Form*" that sets out the type of information that has to be obtained when opening new accounts. This includes, in particular, client's name, address and date of birth, client's social insurance number, client's occupation, client's employer details and insider information.

658. *MSBs*. In addition to remittance or transmission of CAD 3 000 or more by any means through any person, entity or electronic funds transfers network, MSBs are required to keep client information records if they have an on-going business relationship with a client and for the issuance or redemption of money orders, traveller's cheques or other similar negotiable instruments in excess of CAD 3 000 (Section 59 of the PCMLTF Regulations and FINTRAC Guideline 6C "*Record Keeping and Client Identification for MSBs*"). The money services business must confirm the existence of any entity for which it is required to keep client information record (for the purpose of an ongoing relationship). In the case of a corporation, the MSB must also ascertain the corporation's name and address and the names of its directors within this timeframe (see comments under "*timing of verification*").

659. The current requirements are insufficient to meet the FATF standards that identify the circumstances where financial institutions have to perform customer identification (criterion 5.2 of the Methodology). There is no requirement to carry out CDD measures when there is a suspicion of ML or TF or when financial institutions have doubts about the veracity or adequacy of previously obtained CDD data[72]. Financial entities only identify customers when carrying out occasional transactions that are cross-border wire transfers and above CAD 3 000[73]. This threshold is currently too high. With regard to the identification of domestic wire transfers, the assessors were advised that the competent authorities' interpretation of the provision "the remittance or transmission of CAD 3 000 or more by any means through any person, entity or electronic funds transfers network" is that the list of persons, entities and electronic funds transfers networks are part of a non-exhaustive list of illustrations of what can constitute the "any means" by which a transaction can be carried out and that gives rise to identification obligations. In their view, the expression "any means" would therefore include any type of electronic transfer funds system or network, be it domestic or international. The assessors' view is that the language is ambiguous, that electronic funds transfers is definitionally limited to cross-border

[71] PCMLTF Regulations enacted on 27 June 2007 and coming into force in June 2008 reduce this period from 6 months to 30 days (see 64(2)(d), 65(2)(c) and 66(2)(c) of the amended PCMLTF Regulations).

[72] Regulations enacted in June 2007 and coming into force in June 2008 addresses these deficiencies.

[73] Regulations enacted in June 2007 and coming into force in June 2008 addresses these deficiencies.

wire transfers and that therefore this is not sufficient. There is no direct, clear and unambiguous identification requirement for domestic wire transfers.

660. Financial institutions have to ascertain the identity of any individual for large transactions (CAD 10 000 or more). In FINTRAC Guidance ("*Guideline 7A: Submitting Large Cash Transaction Reports to FINTRAC Electronically*"), financial institutions have to make transaction report to FINTRAC in the following situations:

- The financial institution receives an amount of CAD 10 000 or more in cash in the course of a single transaction. Or
- The financial institution receives two or more cash amounts of less than CAD 10 000 each that total CAD 10 000 or more. Entities must make a large cash transaction report if their employee or senior officer knows the transactions were made within 24 consecutive hours of each other by or on behalf of the same individual or entity.

661. The assessment team believes that the 24 consecutive hour rule impedes the application of the FATF requirement (see C.5.2b) of the Methodology) since financial institutions should be able to detect smurfing activities with no limit in time between two or more operations that appear to be linked.

662. With regard to the obligation for financial institutions to ascertain the identity of customers for occasional non-cash transactions, requirements in line with the FATF standards are set in Sections 54(1)(b) and (c), 58(1)(b) and 59(a) of the PCMLTF Regulations.

Required CDD measures

663. Sections 64, 65 and 66 of the PCMLTF Regulations describe the measures that financial institutions are required to take for ascertaining the identity of an individual, corporation and entity other than a corporation, respectively.

664. Natural persons. The PCMLTF Regulations state that the identity of a person shall be ascertained when the person is physically present "by referring to the individual's birth certificate, driver's license, provincial health insurance card, passport or other similar document." "Other similar documents" include a record of landing, permanent resident card, an old age security card, a certificate of Indian status or a card with an individual's signature and photograph on it issued by any of the following (see FINTRAC Guideline 6G):

- Insurance Corporation of British Columbia.
- Alberta Registries.
- Saskatchewan Government Insurance.
- Department of Service Nova Scotia and Municipal Relations.
- Department of Transport and Public Works of Prince Edward Island.
- Service New Brunswick.
- Department of Government Services and Lands of Newfoundland and Labrador.
- Department of Transport of North West Territories;
- Department of Community Government and Transportation of Nunavut.

665. For a document to be acceptable for identification purposes, it must be valid and have a unique identifier number. Also, the document must have been issued by a provincial, territorial or federal government in Canada, or the equivalent in a foreign jurisdiction. When a reporting entity refers to a document to identify an individual, it must be an original and not a copy. Valid foreign identification, if equivalent to an acceptable type of Canadian identification document would also be acceptable (FINTRAC Guidance 6G).

666. The extent to which photographic identification is a requirement is not clear but certain identification documents, such as birth certificates and records of landing, would not contain the

bearer's photograph[74] (which may raise potential risk especially when relying on similar documentation for foreign customers).

667. For individuals not physically present, financial institutions, with the current exception of MSBs must ascertain the identity of the individual by confirming that a cheque drawn by that individual on an account at a financial entity has been cleared (Section 64(1) of the PCMLTF Regulations). This means a cheque that was written by the individual, cashed by the payee and cleared through the individual's account. It does not include pre-authorised payments as these are not cheques written by the individual. Life insurance companies, brokers and agents, securities dealers and departments and agents of Her Majesty in right of Canada or of a province can also ascertain the identity of their client by confirming that the individual holds an account in their name with a financial entity.

668. In the PCMLTF Regulations, the two distinct requirements – identification and verification of customer's identity - are covered by the requirement to "ascertain" customer's identity. In practice, this means that financial institutions must obtain certain data to establish the identity of the customer and verify it by referring to an identification document. It is worth noting that the verification requirement is clearly articulated in the PCMLTFA (Section 6.1) since "*reporting entities shall verify the identity of any person or entity*". Canadian financial institutions are not required to necessarily retain copies of the documentation upon which reliance is placed for verification of the customer's identity on the grounds that such a practice may not respect certain provisions governing privacy and customer protection.

669. In the case of non face-to-face business, the assessors were uncomfortable with the third party cleared cheque confirmation process as it was seen as a potential loophole for illegal use. As a sole means to confirm identity in non face-to-face situations, it is unreliable[75].

670. *Corporations*. When the account is opened, the reporting entity must confirm the existence of the corporation as well as the corporation's name and address and the names of its directors (Section 65 of the PCMLTF Regulations) by referring to the following documents (FINTRAC Guidelines 6G):

- The corporation's certificate of corporate status (including the list of the corporation's directors submitted with the application for incorporation).
- A record that has to be filed annually under provincial securities legislation. Or
- Any other record that confirms the corporation's existence. Examples of these include such other records as the corporation's published annual report signed by an independent audit firm, or a letter or a notice of assessment for the corporation from a municipal, provincial, territorial or federal government.

671. The record that is used to confirm a corporation's existence can be a paper or an electronic version. An electronic version of a record has to be from a public source. If the record is in paper format, the reporting entity has to keep the record or a copy of it. If the record is an electronic version, the reporting entity has to keep a record of the corporation's registration number, the type and source of the record (Section 65(2) of the PCMLTF Regulations).

---

[74] The General Guide to Account Opening and Customer Identification issued by the Basel Committee states that natural persons should be identified using "an official personal identification number or other unique identifier contained in an unexpired official document (*e.g.* passport, identification card, residence permit, social security records, driving licence) that bears a photograph of the customer".

[75] In the case of non face-to-face business, the regulations enacted in June 2007 and coming into force on June 23, 2008 strengthen Canada's non-face-to-face identification methods. In addition to the current third party cleared cheque method various acceptable combinations of identification methods are required for Canadian customers and when the client is a non-resident, face-to-face identification through an agent is required (see 64(1)(b), 64(1.1)(b), 64(1.2), 64(1.3), 64.1 and Schedule 7 of the amended PCMLTF Regulations**)**.

672. There is currently no requirement to identify through personal identification means shareholders of corporations who are beneficial owners (except for IDA supervised entities). Names of directors are obtained from the statutory returns[76].

673. *Entity other than corporation*. The existence of an entity other than a corporation (*e.g.* a partnership, an association or a trust) must be confirmed by referring to a partnership agreement, articles of association or any other similar record (which could include a declaration of trust in the case of a trust) that confirms the entity's existence. Trust companies must identify the settlor (who may be individuals, corporations or entities) and co-trustees of a trust (Section 55 of the PCMLTFA Regulations). In the context of the third party determination, Section 11 of the PCMLTF Regulations sets out the obligation to keep a record of the name, address and principal business and occupation of each of the beneficiaries that are known at the time that the trust company becomes a trustee for the trust. Section 66 of the PCMLTF Regulations sets out very general requirements to ascertain the existence of entities other than corporations and no specific documentation is required to verify the legal status of trusts.

Identification of persons acting on behalf of the customer

674. Financial entities must ascertain the identity of every person who signs a signature card in respect of an account that the financial entity opens, except in the case of a business account of which is signed by more than three persons authorised to act with respect to the account, if the financial entity has ascertained the identity of at least three of those people (Section 54(1)(a) of the PCMLTF Regulations for financial entities). Trust companies (Section 55(d)) and securities dealers (Sections 57(1) and 57(2)(a) must also identify every person – up to three – who is authorised to give instructions in respect of an account. The requirement to identify up to three persons who are allowed to give instructions in respect of an account is too restrictive since any person purporting to act on behalf of the customer should be identified and her/his authorisation to do so should be verified.

Third party determination

675. The PCMLTFA Regulations require financial institutions to determine whether their customers are acting on behalf of another person (see FINTRAC Guidelines 6A, 6C, 6E, 6G). These provisions are generally referred to as "third party determination" (Sections 8 to 11 of the PCMLTF Regulations).

676. Whenever a financial institution is required to keep a large cash transaction record (*i.e.* for cash transactions of CAD 10 000 or more), it must take reasonable measures to determine whether the individual who provides the cash is acting on the instructions of a third party. Whenever a financial institution opens an account, it must take reasonable measures to determine whether the account is to be used by or on behalf of a third party. Such measures also have to be taken by all financial institutions that are required to keep a client information record (MSBs, insurance companies, etc.).

677. Where the person or entity determines that the individual is acting on behalf of a third party, the person or entity shall keep a record that sets out (a) the third party's name and address and the nature of the principal business or occupation of the third party, if the third party is an individual; (b) if the third party is an entity, the third party's name and address and the nature of the principal business of the third party, and, if the entity is a corporation, the entity's incorporation number and its place of issue; and (c) the nature of the relationship between the third party and the individual who gives the cash or between the third party and the account holder. Where the person or entity is not able to determine whether the individual is acting on behalf of a third party but there are reasonable grounds to suspect that the individual is doing so, the person or entity shall keep a record that (a) indicates whether, according to the individual, the transaction is being conducted on behalf of a third party; and

[76] Section 11.1 of the PCMLTF Regulations enacted in June 2007 and coming into force in June 2008, requires financial institutions to take reasonable measures to obtain and keep information on the beneficial owners of corporations, including keeping a record of the name and occupation of all directors and the name, address and occupation of any person who owns or controls 25 per cent or more of the shares of the corporation.

(b) describes the reasonable grounds to suspect that the individual is acting on behalf of a third party. If an account is for or on behalf of future and unknown clients or employees of the individual or entity opening the account, the financial institution must keep a record indicating that the account is to be used by or for third parties who are not known at the time of account opening.

678. If a person is acting on behalf of a corporation, the financial institution must keep a copy of the part of official corporate records that contains any provision relating to the power to bind the corporation in respect of the transactions or in respect of the account, as the case may be (see Sections 14(b), 20, 23(1)(b), 26(b), 30(b) of the PCMLTF Regulations).

Identification of beneficial ownership

679. *General.* Apart from the third party determination requirement, there are significant gaps in the current requirements to establishing beneficial ownership. There is only the requirement to identify the person who is acting on behalf of another person. Financial institutions (except securities dealers) are neither required to understand the ownership and control structure of the customer nor obliged to determine who are the natural persons that ultimately own or control the customer. There is no requirement to identify the beneficiaries of life insurance contracts either. OSFI Guidance B-8 states that "*the FATF recommends that financial institutions "understand the ownership and control structure" of their customers. OSFI suggests that this principle is particularly important when dealing with privately owned companies, trusts and customers that may have more complex legal structures*". OSFI Guidance therefore imposes no requirement in this area. The question was raised during meetings with the Canadian Bankers Association about the methods banks would adopt to identify the beneficial owner in a complex scenario involving corporate shareholdings and whether they would drill down until they identified a personal beneficiary. It seems that in practice there is no identification of the natural person who ultimately owns or controls a customer or exercises ultimate effective control over a legal person or arrangement[77].

680. *Securities dealers*. When opening an initial account for a corporation or similar entity, IDA Members (Regulation 1300 on "Beneficial ownership of non-individual accounts") shall: (i) ascertain the identity of any natural person who is the beneficial owner, directly or indirectly, of more than 10% of the corporation or similar entity, including the name, address, citizenship, occupation and employer of each such beneficial owner, and whether any such beneficial owner is an insider or controlling shareholder of a publicly traded corporation or similar entity; and (ii) as soon as is practicable after opening the account, and in any case no later than six months after the opening of the account, verify the identity of each individual beneficial owner identified in using such methods as enable the Member to form a reasonable belief that it knows the true identity of each individual and that are in compliance with any applicable legislation and regulations of the Government of Canada or any province (Regulation 1300). This does not apply to: (i) a corporation or similar entity that is or is an affiliate of a bank, trust or loan company, credit union, caisse populaire, insurance company, mutual fund, mutual fund management company, pension fund, securities dealer or broker, investment manager or similar financial institution subject to a satisfactory regulatory regime in the country in which it is located (ii) a corporation or similar entity whose securities are publicly traded or an affiliate thereof.

681. When opening an initial account for a trust, an IDA Member shall: (i) ascertain the identity of the settlor of the trust and, as far as is reasonable, of any known beneficiaries of more than 10% of the trust, including the name, address, citizenship, occupation and employer of each such settlor and beneficiary and whether any is an insider or controlling shareholder of a publicly traded corporation or

[77] Under Section 11.1 of the PCMLTF Regulations enacted on 27 June 2007 and entering into force in June 2008, financial institutions are required to confirm the existence of an entity and to take "reasonable measures" to obtain information on the beneficial owners. It is also necessary to keep a record of information on all directors, all partners and owners of 25% or more of the shares of an entity. In so doing, financial entities are required to obtain the name, address, date of birth and occupation of all shareholders with more than 25% holdings.

similar entity. (ii) as soon as is practicable after opening the account, and in any case no later than six months after the opening of the account, verify the identity of each individual identified in using such methods as enable the Member to form a reasonable belief that it knows the true identity of each individual and that are in compliance with any applicable legislation and regulations of the Government of Canada or any province. This does not apply to a testamentary trust or a trust whose units are publicly traded.

682. In its Notice of June 7, 2004, IDA provides further guidance to securities dealers on beneficial ownership identification. The requirement is to identify natural persons owning a greater than 10% interest in a corporation or similar entity, or that are settlors or beneficiaries of trusts. Where interests are held through other corporations or entities, Members are required to determine the identities of those individuals whose net interest in the accountholder exceeds 10%. So for example, where Corporation A holds a 50% interest in a corporate client, the Member is required to identify any natural persons beneficially owning, again directly or indirectly, more than 20% of Corporation A. The requirement is keyed on ownership interest, not on voting control. Where a corporation subject to the requirement has a complicated ownership structure, Members will have to make reasoned judgments to determine who falls within the requirements through discussions with the corporation's representatives. Members should, in compliance with their general know-your-client obligations, obtain a good understanding of the control structure of corporate and other non-individual clients and the nature of their business or other purposes. Members should view with suspicion any indications that a corporation has been structured so as to conceal its true beneficial ownership or avoid any requirement to identify beneficial owners. Any such suspicions should result in additional enquiries before a decision is made to do business with the prospective client.

683. In relation to trusts, the requirement applies for both formal and informal trusts. Some trusts are structured such that the identity of the beneficiaries and/or level of their interest is not known or is subject to alteration under specific conditions; some trusts split different types of beneficial interests, for example between income and underlying assets. A Member is expected to make enquiries sufficient to enable it to understand the nature and details of the trust, but may rely on summary representations made by the settlor or trustee or attorneys for either, without having to examine lengthy and detailed constating documents. The Member should record the essential details including any reasons for the beneficiaries being unknown.

Purpose & intended nature of the business relationship

684. There are currently no requirements to obtain information on the purpose and intended nature of the business relationship[78].

685. Certain information obtained when completing the IDA "*New Client Application Form*" (such as client's occupation, type of business, account objectives) give helpful indications on the intended nature of the business relationship. The IDA Guide on "*Deterring ML Activity*" sets out that a firm's AML program should be designed to permit the firm to make a reasonable risk-based determination as to its customers, its customers' source of income and its expected activity.

Ongoing Due Diligence

686. There are currently no requirements to conduct ongoing due diligence on the business relationship (except for IDA members) although the need to identify customers for large cash transactions and electronic fund transfers provide certain automatic trigger points. OSFI Guideline B-8 (that only sets out recommended actions) states: "*where appropriate (for example, where the volume of transactions is high), FRFIs should consider whether monitoring activity could be strengthened by information technology solutions.*" The OSFI Guideline also stipulates that "*the policies and procedures should include measures to permit FRFIs to identify and report large cash transactions*

[78] Paragraph 14(c.1) of the PCMLTF Regulations, enacted in June 2007 and coming into force in June 2008, requires financial entities to keep a record of the intended use of the account.

(…). The policies and procedures should also include measures to monitor transactions". Many banks appear to have introduced transaction monitoring systems. IDA Policy 4 ("*Minimum Standards for Institutional Account Opening, Operation and Supervision*") states that supervisory procedures and compliance monitoring procedures should be reasonably designed to detect account activity that is or may be a violation of applicable securities legislation, including transactions raising a suspicion of ML or TF activity[79].

687. Financial institutions are not required to ensure that documents, data and information collected under the CDD process are kept up-to-date and relevant[80]. However, IDA Policy 2 requires the maintenance of accurate and current documentation to ensure that all recommendations made for any account are appropriate for the client and in keeping with the client's investment objectives.

Higher risk

688. There is currently no requirement in the PCMLFT Regulations to perform enhanced due diligence for higher risk categories of customer, business relationship or transaction[81].

689. OSFI requires FRFIs to understand the nature of the risks associated with the different parts of their operations. OSFI Guidance makes an inventory of risk categories such as products and services, customers, reliance on others and geographic consideration... Certain transactions have been prescribed as low risk which allow FRFIs some exemption from customer identification requirements. On the contrary, OSFI Guidelines suggest that *"certain customers may merit additional due diligence. Examples could include businesses that handle large amounts of cash, or that deal in luxury or high end consumer goods. Finally customers that hold important public positions (often referred to as "politically exposed persons") may require special attention."*

690. With regard to private banking, the Canadian Bankers Association believes that the form of private banking offered by Canadian banks is a lower risk business model since in their view private banking services are an extension of retail banking and brokerage services offered to primarily Canadian high net worth individuals. However, there is a clear recognition at international level that private banking services are a higher ML/TF risk category of business relationships that require enhanced scrutiny, irrespective of the nationality of the customer[82].

691. IDA Guidance ("*Deterring ML activity, a Guide for Investment Dealers*") identifies higher risk customers (such as offshore customers) and provides indicators in assessing the risk posed by particular customers or transactions (whether the customer is an individual, an intermediary, public, private, domestic or foreign corporation, a financial or non-financial institution, or a regulated person

---

79 Regulations enacted in June 2007 and coming into force in June 2008 require all reporting entities to conduct ongoing monitoring for the purpose of detecting suspicious transactions and keep client information up-to-date when a situation or client represents higher risks) (see Section 71.1 of the amended PCMLTF Regulations**).**

80 This has been addressed through December 2006 changes to the legislation and the regulations coming into force in June 2008 (see Section 71.1 of the amended PCMLTF Regulations, which must be read in conjunction with new section 9.6 of the PCMLTFA).

81 New provisions enacted in June 2007 and coming into force in June 2008 require reporting entities to have written policies and procedures to be used in assessing the risk of ML or TF and take, in the case of higher risk situations, reasonable measures to conduct ongoing monitoring, keep information up-to-date and take any other necessary measures to mitigate the risks. The new regulations include enhanced non-face-to-face methods that take into account the higher risk inherent to a non-face-to-face environment, especially when the customer is a non-resident (see Section 71, Section 71.1 and Sections 64(1)(b), 64(1.1)(b), 64(1.2), 64(1.3), 64.1 and Schedule 7 of the amended PCMLTF Regulations).

82 PCMLTF Regulations enacted on 27 June 2007 (Section 71) and coming into force in June 2008 require written policies and procedures to be used in assessing the risk of ML or TF offence under the compliance program to include, taking into consideration the type of client and the nature of the relationship between the person or entity and the client, the type of product, and the delivery channels for the product and the geographic location and any other relevant factor.

or entity; whether the customer has been an existing customer for a significant period of time; how the client became a customer of the firm; whether the business of the customer, or the particular type of account, is a type more likely to be involved in illicit activity (*e.g.* cash intensive businesses); etc.). For higher risk customers, investment dealers may carry out extra due diligence that may include credit checks, checking of outside databases through the Internet, verification of personal details and references or other more extensive background checks using external resources.

Lower risk

692. The PCMLTF Regulations provide for certain exemptions from the client identification and record-keeping requirements in certain specific circumstances of lower risk of money laundering or terrorist financing. These exemptions mean that, rather than reduced or simplified CDD measures, no CDD measures apply whatsoever for these cases, which is not in line with the FATF requirements that only permit reduced or simplified CDD in certain circumstances.

693. Sections 62 and 63 of the PCMLTF Regulations prescribe the exceptions to ascertaining identity of individuals and existence of entities. Section 9 prescribes the exceptions to third party determination. The assessment team was told that these exemptions were developed following extensive discussions between the Department of Finance, FINTRAC, the RCMP and the reporting entities. No more information was provided at the time of the on-site visit.

694. *General exemptions from CDD requirements*. The general exceptions (Section 63) are as follows:

- Once a reporting entity has ascertained the identity of an individual, it does not have to confirm their identity again if it recognizes the individual at the time of a future event that would otherwise trigger the identification requirement.
- Once a reporting entity has confirmed the existence of a corporation and confirmed its name, address and the names of its directors, it is not required to confirm that same information in the future;
- Once a reporting entity has confirmed the existence of an entity other than a corporation, it is not required to confirm that same information in the future.
- When the corporation is a securities dealer, the reporting entity is not required to ascertain the name of the directors.

695. *Specific exemption from CDD requirements*. In the insurance sector, more specific exceptions are proposed under the PCMLTF Regulations (Sections 62 & 63), again to address low risk situations, namely:

- The purchase of an immediate or deferred annuity that is paid for entirely with funds that are directly transferred from a registered pension plan or from a pension plan that is required to be registered under the Pension Benefits Standards Act, 1985, or similar provincial legislation.
- The purchase of a registered annuity policy in respect of an annuity referred to in subsection (5) or a registered retirement income fund.
- The purchase of an immediate or deferred annuity that is paid for entirely with the proceeds of a group life insurance policy.
- A transaction that is part of a reverse mortgage or of a structured settlement.
- The opening of a registered plan account, including a locked-in retirement plan account, a registered retirement savings plan account and a group registered retirement savings plan account.
- The opening of an employees profit sharing plan account or a deferred profit sharing plan account, unless the account is funded in whole or in part by contributions by a person or entity other than the employer. Or

- The opening of a dividend reinvestment plan account sponsored by a corporation for its investors, unless the account is funded in whole or in part by a source other than the corporation.

696. Financial entities, securities dealers and the insurance sector are not required to ascertain identity if:

- The person already has an account with the financial entity or the securities dealer, as the case may be. Or
- There are reasonable grounds to believe that the account holder is a public body or a corporation that has minimum net assets of CAD 75 million on its last audited balance sheet and whose shares are traded on a Canadian stock exchange or a stock exchange that is prescribed by section 3201 of the *Income Tax Regulations* and operates in a country that is a member of the Financial Action Task Force on Money Laundering (Section 62(2)(b)).

697. The second exemption raises concerns since the exemption is broad in scope (and "the reasonable grounds to believe" element introduces a weak and indefinite threshold). The assessors were told that a thorough risk assessment was conducted before deciding on this exemption. The decision was based on the fact that corporations with a minimum of CAD 75 million in net assets are already under considerable public scrutiny and regulation. There are numerous documents publicly available outlining their financial situation, ownership, structure and management. These corporations are also subject to provincial securities legislation as public issuers and are subject to sanctions if they provide false or misleading information. From the assessment team's point of view, the exemption in the securities industry to identify corporations that, among other criteria, operate in FATF countries is not satisfactory since it is only based on the principle of presumption of conformity. The assessors were told that the decision to exempt entities from FATF member countries is based on the fact that AML/CFT requirements and CDD measures in particular, can reasonably be expected to be stronger and more effective in these countries.

698. Finally, the identity requirement does not apply if the account holder or settlor is a pension fund that is regulated under an Act of Parliament or of the legislature of a province. The assessors were told that pension funds are subject to strict information disclosure requirements and to fines or imprisonment if these rules are violated. Financial entities are not required to ascertain identity in respect of (a) employees profit sharing plan accounts and deferred profit sharing plan accounts, unless the accounts are funded in whole or in part by contributions from a person or entity other than the employer; or (b) dividend reinvestment plan accounts sponsored by a corporation for its investors, unless the accounts are funded in whole or in part from a source other than the corporation. These plans are considered to be lower risk because they do not provide the opportunity for the members to place additional funds in the plan beyond small payroll deductions prescribed under the plan[83].

699. *Exemptions from third party determination*. The third party determination provision does not apply in respect of an account where the account holder is a financial entity or a securities dealer engaged in the business of dealing in securities in Canada. Also, in cases where the account holder is a person or entity engaged in the business of dealing in securities outside Canada only, securities dealers do not have to make a third party determination if any of the following conditions are met:

- The account is in a country that is a member of the FATF.
- The account is in a country that is not a member of the FATF, but, when opening the account, the security dealer gets written assurance from that account holder that the country where the account is located has implemented the FATF Recommendations concerning customer identification. Or

[83] Under regulations that have been enacted in June 2007 and come into force in June 2008, clients that want to make lump-sum payments to these plans will have to be identified in addition to the administrator of the plan (see Subsection 62(3) of the amended PCMLTF Regulations).

- The account is in a country that is not a member of the FATF and that country has not implemented the FATF recommendations concerning customer identification, but the securities dealer has ascertained the identity of all third parties relating to the account.

700. In addition, financial institutions do not have to make a third party determination for an account if the following conditions are met: (1) the account is opened by a legal counsel, an accountant or a real estate broker or sales representative; and (2) the reporting entity has reasonable grounds to believe that the account is to be used only for their clients.

701. The assessors were told that Canada has taken a risk-based approach in deciding to provide certain exemptions to third party determination. As such, all the exemptions are with respect to professionals in Canada that are subject to strict rules and codes of conduct and that are supervised by an SRO that can impose severe sanctions or, where the professional is not in Canada, is located in a FATF country or has identified its clients. The assessment team believes that despite these safeguards the exemptions to carry out third party determination bring in very far reaching exceptions that introduce potential gaps in the customer identification process and create some potential risky situations as far as ML and FT are concerned.

702. FATF Recommendations allow financial institutions to apply simplified or reduced CDD measures to customers resident in another country provided that the original country is satisfied that the other country is in compliance with and has effectively implemented the FATF Recommendations. Section 62(2)(b) and Section 9(5) as described earlier give financial institutions, in certain circumstances, the permission to exempt from CDD requirements or third party determination obligations certain customers resident in another country. However, Canada has not carried out a systematic country risk analysis to ensure that third countries in which customers of Canadian financial institutions are resident are in compliance with and have effectively implemented the FATF Recommendations.

703. CDD or third party determination exemptions are applicable where there is a suspicion of ML or FT or specific higher risk scenarios apply. This should be corrected.

Guidelines on the risk-based approach

704. Where financial institutions are permitted to determine the extent of the CDD measures on a risk sensitive basis, this should normally be consistent with guidelines issued by the competent authorities. At present, there are no detailed specific guidance measures that permit financial institutions to determine the extent of CDD measures on a risk sensitive basis.

705. OSFI Guideline B-8 refers institutions to the Basel Committee paper on Customer Due Diligence, issued in 2001, and encourages them to familiarise themselves with the standards outlined in the BCBS paper.

706. FINTRAC has issued a range of guidance, including "Implementation of a Compliance Regime" but this focuses primarily on the need to appoint a compliance officer, develop policies and procedures, conduct periodic reviews of policies and procedures and implement a training program. It does not specifically advise reporting entities on how to conduct a risk assessment, the risk-based approach to determination of vulnerabilities and the appropriate and proportional risk-based approaches to high-risk areas.

Timing of Verification

707. In line with the FATF requirements, financial institutions should be required to verify the identity of the customer and beneficial owner before or during the course of establishing a business relationship or conducting transactions for occasional customers. Subsections 64(2), 65(2) and 66(2) of the PCMLTF regulations set out the requirements for ascertaining the identity of individuals, corporations and other entities as follows:

Type of transactions or reporting party in charge of verification	Timelines to carry out verification
Verification of natural person identity	
Signature of a signature card on an account managed by a financial entity	Before any transaction other than an initial deposit is carried out on an account[84]
▪ Large cash transactions of CAD 10 000 or more ▪ Electronic fund transfers of CAD 3 000 or more ▪ Foreign currency exchange transactions of CAD 3 000 or more ▪ Issuance or redemption of money orders, traveller's cheques or other similar negotiable instruments	At the time of the transaction
Trust company	Within 15 days after the trust company becomes the trustee
Life insurance company or life insurance broker or agent	Within six months after the client information record is created[85]
Securities dealers	Within six months after the account is opened[86]
Verification of corporation identity (including directors) or entity other than corporation	
Financial entities	Before any transaction other than an initial deposit is carried out on an account[87]
Trust company	Within 15 days after the trust company becomes the trustee
Life insurance company or life insurance broker or agent	Within six months after the client information record is created[88]
Foreign exchange dealing	Within six months after client information record is created
Money Services Businesses	Within six months after the client information record is created[89]
Securities dealers	Within six months after the account is opened[90]

708. The regulations establish generally acceptable timelines for ascertaining customer identity in some scenarios and especially when such verification is carried out by financial entities (for verification of identity of natural persons, corporations and entities other than corporations). However, certain serious weaknesses exist for the verification of identity carried out by some financial sectors (such as securities and insurance sectors) and/or vis-à-vis certain types of customers (such as corporations or entities other than corporations). The Canadian authorities recognise the risks involved here and the PCMLFT Regulations shorten these timelines in certain circumstances. The assessors believe that the proposed 30 day timeline for corporations' verification in the MSBs, insurance and securities sectors is too long, especially in normal business circumstances.

709. IDA Policy 2 requires IDA members to have procedures in place to ensure supporting documents are received within a reasonable period of time of opening the account. Incomplete New Client Application Form and documentation not received must be noted, filed in a pending documentation file and be reviewed on a periodic basis. Failure to obtain required documentation

[84] In June 2008 credit card issuers will have to identify clients before the card is activated (see Sections 64(2)(b.2) of the amended PCMLTF Regulations).

[85] In June 2008 this timeline will be within 30 days (see Sections 64(2)(d) of the amended PCMLTF Regulations).

[86] In June 2008, before any transaction other than an initial deposit is carried out on an account (see Section 64(2)(a) of the amended PCMLTF Regulations).

[87] In June 2008, credit card issuers must identify the account holder before any card is issued on the account (see Sections 65(2)(a.1) and 66(2)(a.1) of the amended PCMLTF Regulations).

[88] In June 2008 this timeline will be within 30 days (see Sections 65(2)(c) and 66(2)(c) of the amended PCMLTF Regulations) .

[89] In June 2008 this timeline will be within 30 days (see Sections 65(2)(c) and 66(2)(c) of the amended PCMLTF Regulations).

[90] In June 2008 this timeline will be within 30 days (see Sections 65(2)(d) and 66(2)(d) of the amended PCMLTF Regulations).

within 25 clearing days must result in positive actions being taken. The nature of the positive action must be specified in the Member's written procedures.

710. For IDA Members, verification of the identity of the beneficial owners must be completed "as soon as practicable" after account opening, and in any case no longer than six months after the account is opened. Verification procedures must begin at the time of account opening. Delaying efforts to verify the identity of beneficial owners with a view only to the six-month deadline will be viewed by the Association as non-compliance with the regulation. IDA Sales Compliance reviews will examine Members' practices to ensure that verification efforts are begun on a timely basis and are diligently pursued. In keeping with their obligations under anti-money laundering regulations, Members should consider imposing higher standards for accounts posing a higher risk of use for money laundering or other improper activity, for example requiring prior verification of the identity of beneficial owners or maintaining closer supervision of account activity until beneficial ownership has been verified.

711. OSFI has advised FRFIs that with respect to loans, including mortgage loans, there is only one "transaction", which is the disbursement of the proceeds of the loan. OSFI expects institutions to verify the identity of individuals, corporations, and entities other than corporations that open accounts for the borrowing of funds prior to the disbursement of such funds, and to refrain from disbursing such funds until such identify is satisfactorily verified.

Failure to complete CDD

712. In situations where the financial institution has already commenced a business relationship but is unable to perform adequate CDD and establish beneficial ownership, FATF Recommendations require the business relationship to be terminated and consideration given to making a suspicious transaction report. However, the current regulations, in case of failure to satisfactorily complete CDD, are not in line with the FATF standards[91] as there is no explicit requirement to close an account when a financial institution fails to properly identify a customer. However, OSFI Guideline B-8 makes reference to closing accounts, namely *"FRFIs should consider terminating relationships with introducers that cannot, or fail to, provide the FRFI with the requisite customer identification and verification data that the FRFI is required to obtain under the PCMLTFA and Regulations"*. However, as mentioned before, financial entities are generally required to identify their customers at the outset and institutions that continue to operate the business relationship without ascertaining the customer's identity are liable to criminal penalties. FINTRAC has also identified the refusal of a customer to provide information or identification as one of the suspicious transaction indicators that would merit a suspicious transaction report.

713. In IDA Regulation 1300, if securities dealers are unable to obtain the information on the beneficial owner of non-individual accounts, they shall not open the account. If an IDA Member is unable to verify the identities of individuals within six months of opening the account, the Member shall restrict the account to liquidating trades and transfers, payments or deliveries out of funds or securities only until such time as the verification is completed. Similarly, any delays in verification that appear to result from lack of client cooperation should result in a careful assessment of the circumstances. Appropriate responses could include heightened supervision of account activity, filing of suspicious transaction reports with FINTRAC and/or closing of the account.

Existing Customers

714. Financial institutions are not required to apply CDD requirements to existing customers on the basis of materiality and risk and to conduct due diligence on such existing relationships at appropriate times[92].Subsection 63(1) of the PCMLTF Regulations only states that "where a person has ascertained

[91] Section 9.2 of the PCMLTFA that will enter into force in June 2008 prohibits financial institutions from opening an account when the customer's identity was not obtained.

[92] New requirements to come into force in June 2008 will apply the CDD requirements to existing customers on the basis of materiality and risk (see Section 71.1 of the amended PCMLTF Regulations**)**.

the identity of another person in accordance with section 64, the person is not required to subsequently ascertain that same identity again if they recognize that other person". The interpretation that Canada gives to that provision is that if the identity of a person was not ascertained in accordance with Section 64 (*e.g.* because they opened an account 20 years ago before CDD requirements were in place) and this person wants to open another account., this person, even though they are an existing customer, will have to be identified. The assessment team believes that this insufficiently addresses the requirement under Recommendation 5 (criterion 5.13).

Recommendation 6

715. *Legislative and regulatory requirements.* No specific legislative or other enforceable requirements in relation to PEPs are currently in force[93].

716. OSFI Guidance. The OSFI Guideline B-8 advises institutions that "certain customers may merit additional due diligence. Examples could include businesses that handle large amounts of cash, or that deal in luxury or high-end consumer goods. Finally, customers that hold important public positions (often referred to as "politically exposed persons") may require special attention". However, the guidance goes no deeper than this and banks, to a large extent, are left to decide how best to tackle the situation. The assessment team was told that OSFI has communicated its expectations to FRFIs in relation to PEPs and the need to have measures in place commensurate with the risks attached to PEPs although no binding requirement is currently in place.

717. In the insurance sector, although federally regulated life insurance companies are bound by OSFI Guidance B-8 (since the Guidance applies to all FRFIs), the CLHIA, the life insurance association, believes that Guideline B-8 is primarily intended to apply to the banking sector. As a consequence, the assessment team was advised that there is a perception that the guideline does not contain requirements that the insurance sector has to implement, for example no obligation to identify PEPs. The representatives of the association confirmed that no screening for PEPs actually takes place in the industry.

718. Discussions with the banking industry indicate that at least the larger banks have undertaken their own measures to help identify customers who may be PEPs, normally by investing in proprietary software solutions. However, this is not standard across the industry and indeed smaller banks indicated that they were not addressing the issue, largely as a result of cost factors. A similar position appears to exist for other types of financial institutions.

Recommendation 7

719. *Definition.* A correspondent banking relationship is defined in the PCMLTFA as a relationship created by an agreement or arrangement under which banks to which the Bank Act applies, cooperative credit societies, savings and credit unions and *caisses popularies*, companies to which the Trust and Loan Companies Act applies, and trust companies regulated by a provincial act or certain prescribed entities undertake to provide to a prescribed foreign entity services such as international electronic funds transfers, cash management, cheque clearing and any prescribed services.

720. *Legislative and regulatory requirements*. Canada enacted new requirements in June 2007 (that entered into force on June 30, 2007) that deal with correspondent banking related issues, and address many of the requirements of Recommendation 7. Section 9.4 (1) of the PCMLTFA came into force in June 2007 and requires every financial entity to take the following measures before entering into a correspondent banking relationship with a prescribed foreign entity: (1) obtain prescribed information about the foreign entity and its activities; (2) ensure that the foreign entity is not a shell bank as defined in the regulations; (3) obtain the approval of senior management; (4) set out in writing their

[93] New requirements in relation to PEPs that were introduced under amendments to the PCMLTFA (Section 9.3) and the PCMLTF Regulations will come into force on 23 June 2008.

obligations and those of the foreign entity in respect of the correspondent banking services; and (5) any prescribed measures.

721. New provisions in the PCMLTF Regulations in relation to correspondent banking have also been in force since June 30, 2007. These provisions require that every financial entity that enters into a correspondent banking relationship shall (Section 55 of the PCMLTF Regulations):

- Ascertain the name and address of the foreign financial institution by examining a copy of the foreign financial institution's banking licence, banking charter, authorisation or certification to operate from the relevant regulatory agency or certificate of corporate status or a copy of another similar document.
- Take reasonable measures to ascertain, based on publicly available information, whether there are any civil or criminal penalties that have been imposed on the foreign financial institution in respect of anti-money laundering or anti-terrorist financing requirements and, if so, to conduct, for the purpose of detecting any transactions that are required to be reported under the Act, ongoing monitoring of all transactions in the context of the correspondent banking relationship.

722. The same regulations state that every financial entity shall, when it enters into a correspondent banking relationship, keep a record in respect of the foreign financial institution containing the following information and documents (Section 15.1(2) of the PCMLTF Regulations):

- The name and address of the foreign financial institution.
- The names of the directors of the foreign financial institution.
- The primary business line of the foreign financial institution.
- A copy of the most recent annual report or audited financial statement of the foreign financial institution.
- A copy of the foreign financial institution's banking licence, banking charter, authorisation or certification to operate from the relevant regulatory agency or certificate of corporate status or a copy of another similar document.
- A copy of the correspondent banking agreement or arrangement, or product agreements, defining the respective responsibilities of each entity.
- The anticipated correspondent banking account activity of the foreign financial institution, including the products or services to be used.
- A statement from the foreign financial institution that it does not have, directly or indirectly, correspondent banking relationships with shell banks.
- A statement from the foreign financial institution that it is in compliance with anti-money laundering and anti-terrorist financing legislation in its own jurisdiction.

723. Finally, the Regulations require these types of financial institutions to take reasonable measures to ascertain whether the foreign financial institution has in place anti-money laundering and anti-terrorist financing policies and procedures, including procedures for approval for the opening of new accounts and, if not, for the purpose of detecting any transactions that are required to be reported to FINTRAC, take reasonable measures to conduct ongoing monitoring of all transactions conducted in the context of the correspondent banking relationship. All of these measures apply to all foreign financial institutions, regardless of country of origin. However, there is no requirement to assess the respondent institution's AML/CFT controls, and ascertain that they are adequate and effective. Nor are there requirements for the financial institutions to determine the reputation of the foreign financial entity (other than take reasonable measures to ascertain, based on publicly available information, whether there are any civil or criminal penalties that have been imposed on the foreign financial institution in respect of anti-money laundering or anti-terrorist financing requirements) or the quality of supervision of that entity.

724. *Payable through accounts*. The PCMLTF Regulations require that in situations where the customer of the respondent entity has direct access to the services provided under the correspondent banking relationship, the entity shall take reasonable measures to ascertain that:

- The respondent entity has performed the customer due diligence obligations, in accordance with the measures for ascertaining customer identity set out in the Regulations, in respect of those of its customers that have direct access to the accounts of the correspondent entity.
- The respondent entity has agreed to provide relevant customer identification data upon request to the correspondent entity.

725. The respondent entity must carry out customer identification based on the CDD requirements set out in the PCMLTF Regulations (as applicable from time to time). However the full set of CDD measures in the Regulations will not be in force until June 2008, and the current requirements are not in line with the FATF standards (see conclusions of the report in relation to Recommendation 5). Financial institutions are therefore not currently required to be satisfied that the respondent financial institutions have performed all the normal CDD obligations set out in Recommendation 5 on those of their customers that have direct access to the accounts of the correspondent financial institutions.

726. *OSFI Guidance*. Guidance to all banks and federally regulated trust & loan companies since 2002 has taken the form of a letter from OSFI, dated February 22, 2002 entitled "*Enhanced Due Diligence for Correspondent Accounts*". This letter advises recipients of the introduction of the USA PATRIOT Act and the prohibition on dealing with shell banks. The letter goes on to draw recipients' attention to the Basel Committee Paper *"Customer Due Diligence for Banks"* issued October 2001 and states, *"In light of these two initiatives, we believe that Canadian deposit taking institutions should be aware of the enhanced BIS standard for dealing with correspondent banking accounts and encourage them to adopt measures which will ensure that they do not enter into correspondent accounts with shell banks"*. There is also passing reference in OSFI Guideline B-8 about the risks involved in entering into correspondent relations with shell banks, namely; *"We draw the attention of FRFIs to the risks involved in dealing with "shell" banks…and in the light of applicable international standards, OSFI encourages all FRFIs to adopt measures which will ensure that they do not enter into correspondent relationships with shell banks"*.

727. Canada has indicated that Canadian financial institutions with correspondent banking relationships have branches or subsidiaries in the U.S. These financial institutions have applied to their Canadian operations the requirements of the 2002 US PATRIOT Act on correspondent banking relationships.

Recommendation 8

728. *Legislative and regulatory requirements.* At the time of the on-site visit, there were no specific legislative or other enforceable obligations addressing the risks posed by the application of new technological developments to the provision of financial services other than the fundamental identification requirements of each person or entity under the PCMLTFA, regardless of delivery channel.

729. Financial institutions are currently not required to have policies and procedures in place to address any specific risk associated with non face-to-face business relationships or transactions[94].

730. *OSFI Guidance*. OSFI Guideline B-8 currently encourages Canadian FRFIs to implement the customer due diligence standards set out in the Customer Due Diligence for Banks paper released by the Basel's Committee in 2001 in a manner that is appropriate with the size, the complexity and the

[94] New regulations that will enter into force in June 2008 include enhanced identification measures to ascertain the identity of a client who is not physically present (see Sections 64(1)(b), 64(1.1)(b), 64(1.2) 64(1.3), 64.1 and Schedule 7 of the amended PCMLTF Regulations).

nature of the entity's activities. This paper highlights the necessity for banks to have adequate measures to mitigate higher risks, including non-face-to-face transactions or relationships. The guidelines further require these institutions to have in place a non-face-to-face identification process that is as effective as when the client is physically present. The assessors were told that in the course of its examinations of correspondent banking operations, it has never seen any direct or indirect relationship with a shell bank.

731. The assessors were advised of an emerging technology known as "white label" automated teller machines, the development of which is being monitored by the Department of Finance, together with the use of stored value cards and Internet payment providers. "White label" automated teller machines, are operated by non-financial institutions and represent approximately 60% of the total number of cash dispensers in Canada. They are generally located in non-traditional places, including supermarkets and bars. The main concern is that they can be loaded by the owner and may create opportunities to 'place' illicit cash.

732. Interac has developed limited mechanisms to prevent the misuse of these machines, such as enhancing the process for accepting new members and strengthening the regulation of owners, but concerns reflected by the RCMP suggested that bar owners or other entertainment complexes that provide heavily cash-based services could in effect recycle their own money each night, supplementing it with other illegal funds. Discussions seem to take place with Interac to enhance existing mechanisms in respect of customer due diligence and record keeping. A number of gaps in Interac's existing CDD rules have been identified (*e.g.* the acquirer, or the Interac member that ultimately provides connection for an ATM to the Interac network, has to conduct CDD on their direct business partners only (the payments processor), but are not required to perform CDD on the ATM owner if he is not a direct partner). Discussions are ongoing to determine additional measures.

733. The Department of Finance has also conducted a preliminary analysis of the AML/CFT risks of the stored value card market and intends to examine in more detail the shortfalls in the client identification practices of these vendors. The RCMP acknowledge that such gift cards represent a serious money laundering option, especially in the absence of any money laundering control at retail locations. In addition, the Department of Finance has engaged a number of Internet payment providers to discuss the AML/CFT risks and the structure of that sector. These are positive moves at the Government level but there remains nothing in force at the financial institution level that requires them to implement policies and procedures addressing new technologies when face to face identification is not possible.

734. The current CDD measures in relation to non face-to-face business are rather weak (see comments in relation to Recommendation 5 – *Required CDD measures*) since the only measure for the reporting entities is to ascertain the identity of the individual by confirming that a cheque drawn by that individual on an account at a financial entity has been cleared[95].

735. Some large financial institutions met during the on-site visit seem to apply higher internal standards in this area. However, the assessment team met with a limited sample of financial institutions and was also told that in other institutions such higher standards were not in place yet.

3.2.2 Recommendations and Comments

736. *Scope issues*. Financial leasing, factoring, finance companies (entities specialized in consumer lending, credit cards, equipment financing and small business loans); providers of e-money; Internet payment providers; cheques cashiers when only cashing cheques issued to denominated persons are not currently included in the scope of the PCMLTFA, and are thus not covered by the CDD

[95] The PCMLTF Regulations (Section 64) introduce new non-face-to-face identification methods that are applicable to any person or entity covered by the PCMLTFA and are applicable to any non-face-to-face circumstances.

requirements. This is an important omission and Canada should take steps to bring them within the CDD requirements unless it can prove, based on a formalised and thorough risk assessment analysis that these categories of institutions are of lower ML/TF risks.

737. So far, financial institutions (except the securities dealers monitored by the IDA) have received very little guidance spelling out the measures to take to implement proper AML/CFT measures. FINTRAC guidance focuses primarily on meeting record keeping and reporting requirements and is not very detailed. OSFI Guidance is also very limited since it covers a limited range of requirements. It is important for financial institutions to have detailed and comprehensive guidance at their disposal as a tool to properly and uniformly implement the AML/CFT requirements.

738. *Recommendation 5*. With regard to numbered or confidential accounts, Canada should consider adopting detailed rules or guidance on the use of such accounts by financial institutions. Such rules should clearly set out the obligation for compliance officers to have access to CDD information.

739. New provisions will come into force in 2008 with regard to the circumstances where financial institutions have to perform customer identification. Canada should ensure that the new provisions are fully in line with the FATF requirements.

740. With regard to the identification measures for natural persons, Canada should ensure that only reliable CDD documentation is acceptable, especially in non face-to-face situations. Canada should consider introducing additional requirements for identifying foreign customers.

741. New provisions will come into force in June 2008 with regard to identification of beneficial owners. Canada should ensure that the new provisions are fully in line with the FATF requirements and are properly implemented by all financial institutions.

742. The requirement to identify up to three persons who are authorised to give instructions in respect of an account should be extended to any person purporting to act on behalf of the customer.

743. The PCMLTF Regulations, enacted in June 2007 and coming into force in June 2008 require financial entities to keep a record of the intended use of the account. Canada should ensure that such requirement is implemented by all financial institutions in line with the FATF standards. Based on the provisions adopted in June 2007 and coming into force in 2008, Canada should ensure that financial institutions fully implement the obligation to conduct ongoing due diligence on the business relationship and ensure all documents, data and information collected under the CDD process in line with the FATF standards (as it is already the case for securities dealers) are kept up-to-date and relevant.

744. In relation to ML/FT risks, Canada should ensure that financial institutions perform enhanced due diligence for higher risk categories of customer, business relationship or transaction once the new regulations enter into force in June 2008. This should be done in line with the FATF standards. Current scenarios of full exemptions from CDD and third party determination should be subject to simplified or reduced CDD. Where financial institutions are permitted to apply simplified or reduced CDD measures to customers resident in another country, this should be limited to countries that Canada is satisfied are in compliance with and have effectively implemented the FATF recommendations (*i.e.* Canada should not rely on presumption of conformity of FATF countries for instance). Canada should adopt explicit provisions that set out that such exemptions are not acceptable where there is a suspicion of ML or FT or specific higher risk scenarios apply. Canada should consider developing guidelines for financial institutions that are permitted to determine the extent of the CDD measures on a risk sensitive basis.

745. With regard to the timing of customer's identity verification, new regulations that will enter into force in June 2008 should be implemented in line with the FATF standards and Canada should

consider adopting shorten timelines in the insurance, foreign exchange, MSBs and securities sectors for corporations' or entities' identification, especially in normal business circumstances.

746. *Recommendation 6.* Canada should ensure that the new provisions enacted in June 2007 are fully in line with the FATF requirements and ensure that reporting entities implement measures that meet the FATF standards.

747. *Recommendation 7.* Canada should require financial entities to assess the respondent institution's AML/CFT controls and to ascertain that these controls are adequate and effective. Institutions should also be required to further determine the reputation of the foreign financial entity and the quality of supervision of that entity.

748. In the context of payable through accounts, financial institutions should be required to be satisfied that the respondent financial institutions have performed all the normal CDD obligations set out in Recommendation 5 on those of their customers that have direct access to the accounts of the correspondent financial institutions. Canada should ensure that reporting entities implement measures that meet the FATF standards.

749. *Recommendation 8.* Canada should ensure that the new provisions enacted in June 2007 are fully in line with the FATF requirements and ensure that reporting entities implement measures that meet the FATF standards.

3.2.3 Compliance with Recommendations 5 to 8

Rec.	Rating	Summary of factors underlying ratings
Rec.5	NC	*Scope issue* • The requirement to conduct CDD does not extend to all financial institutions as defined by the FATF (notably financial leasing, factoring and finance companies). *Numbered accounts* • *Although numbered accounts are permissible and used, there is no direct requirement to maintain them in such a way that full compliance can be achieved with the FATF Recommendations.* *When CDD is required* • There is no requirement to carry out CDD measures when there is a suspicion of ML or TF and when financial institutions have doubts about the veracity or adequacy of previously obtained CDD data. • Customer identification for occasional transactions that are cross-border wire transfers takes place for transactions above CAD 3 000. This threshold is currently too high and no equivalent requirement is in place for domestic wire transfers. *Required CDD measures* • The current customer identification measures for natural persons are insufficient, especially in relation to non face-to-face business relationships. *Identification of persons acting on behalf of the customer* • The requirement to identify up to three persons who are allowed to give instructions in respect of an account is too limitative. *Third party determination and identification of beneficial owners* • Except for IDA supervised entities, financial institutions are neither required to understand the ownership and control structure of the customer nor obliged to determine who are the natural persons that ultimately own or control the customer. *Purpose & intended nature of the business relationship* • There are currently no requirements (except for securities dealers) to obtain information on the purpose and intended nature of the business relationship.

Rec.	Rating	Summary of factors underlying ratings
		Ongoing Due Diligence • Except for securities dealers, there are currently no requirements to conduct ongoing due diligence on the business relationship although the need to identify customers for large cash transactions and electronic fund transfers provide certain automatic trigger points. • Except for securities dealers financial institutions are not required to ensure that documents, data and information collected under the CDD process is kept up-to-date and relevant. *ML/FT risks – enhanced due diligence* • There is no requirement to perform enhanced due diligence for higher risk categories of customer, business relationship or transaction. *ML/FT risks – reduced or simplified due diligence* • The current exemptions mean that, rather than reduced or simplified CDD measures, no CDD apply, which is not in line with the FATF standards. • Exemptions from CDD and third party determination bring in very far reaching exceptions that introduce potential gaps in the customer identification process (especially the exemptions apply to financial entities that operate in FATF countries based on presumption of conformity only). • There is no explicit provisions that set out that CDD or third party determination exemptions are not acceptable where there is a suspicion of ML or FT or specific higher risk scenarios apply. • Financial institutions, in certain circumstances, are given the permission to exempt from CDD requirements or third party determination obligations certain customers resident in another country. However, Canada has not carried out a systematic country risk analysis to ensure that third countries in which customers of Canadian financial institutions are resident are in compliance with and have effectively implemented the FATF Recommendations. *Timing of verification* • PCMLTF Regulations sets out unreasonable verification timelines to be carried out by certain financial sectors and/or in relation to certain customers. *Failure to satisfactorily complete CDD* • Financial institutions (except securities dealers in some circumstances) are not prevented from opening an account or commencing business relationship or performing a transaction and they are not required to make a suspicious transaction report. • In situations where the financial institution has already commenced a business relationship but is unable to perform adequate CDD and establish beneficial ownership, there is no requirement to terminate the business relationship and to consider making a suspicious transaction report.
Rec. 6	NC	• There were no mandatory legislative or other enforceable requirements in relation to PEPs at the time of the on-site visit.
Rec. 7	PC	• Financial entities are not required to assess the respondent institution's AML/CFT controls and to ascertain that these controls are adequate and effective. • Financial institutions are not required to determine the reputation of the foreign financial entity (other than take reasonable measures to ascertain whether there are any civil or criminal penalties that have been imposed on the foreign financial institution in respect of AML/CFT requirements) and the quality of supervision of that entity. • In the context of payable through accounts, the respondent entity is not required to perform all the normal CDD obligations set out in Recommendation 5 on its customers that have direct access to the accounts of the correspondent institution in line with the FATF standards. • The effectiveness of the measures in place cannot yet be assessed.
Rec. 8	NC	• There are no specific legislative or other enforceable obligations. addressing the risks posed by the application of new technological developments. • Financial institutions are not required to have policies and procedures in

Rec.	Rating	Summary of factors underlying ratings
		place to address any specific risk associated with non face-to-face business relationships or transactions. • No effective CDD procedures for non face-to-face customers are in place.

3.3 Third parties and introduced business (R.9)

3.3.1 Description and Analysis

750. *General*. The two scenarios of introduced business (where CDD is completed by someone who is neither an employee, nor a person in a contractual agency relationship) and outsourcing or agency relationships agreements (where the agent is to be regarded as synonymous with the financial institution *i.e.* the processes and documentation are those of the financial institution itself) exit in Canada. Under the Regulations, only two scenarios of introduced business are contemplated (Sections 56(2) and 57(5)). Outside these two situations, the assessment team was told that financial institutions are expected to either carry out the CDD process themselves or enter into an agency agreement with the entity authorised to act on their behalf[96].

751. *Regulatory provisions on agency relationships*. Section 6(2) of the PCMLTF Regulations addresses the issue of agency relationships. Where a person, other than a life insurance broker or agent, is an agent of or is authorised to act on behalf of another person or entity (banks, trust companies, etc.), it is that other person or entity rather than the agent or the authorised entity or person who is responsible for meeting the requirements under the PCMLTF Regulations. Based on that provision, FINTRAC and OSFI have developed further guidance, including with respect to persons or entities who may be appointed as agent but who are not subject to the regulations.

752. *Regulatory provisions on introduced business*. In the PCMLTF Regulations, only two provisions are applicable to the introduced business scenario (although in a very indirect way). Section 56(2) states that a life insurance company or life insurance broker or agent is not required to ascertain the identity of a person where there are reasonable grounds to believe that the person's identity has been ascertained by another life insurance company or life insurance broker or agent in respect of the same transaction or of a transaction that is part of a series of transactions that includes the original transaction. Section 57(5) states that a securities dealer is not required to ascertain the identity of a person who is authorised to give instructions in respect of an account that is opened for the sale of mutual funds where there are reasonable grounds to believe that the person's identity has been ascertained by another securities dealer in respect of (a) the sale of the mutual funds for which the account has been opened; or (b) a transaction that is part of a series of transactions that includes that sale. These are the only exceptions where reliance on a third party or introduced business is allowed without an agreement or arrangement (and where the outsourcing scenario applies). When these scenarios apply, there is no explicit requirement in the Regulations for financial institutions to obtain from the third party the necessary information concerning certain elements of the CDD process and satisfy themselves that copies of identification data are made available from the third party upon request without delay. The Regulations do not set out that the ultimate responsibility for customer identification and verification should remain with the financial institution relying on the third party.

753. *Existing guidance*. In FINTRAC guidance on record keeping and client identification, where reporting entities choose to rely on a third party (called "agent") to identify their customers, they should enter into a written agreement with the agent outlining what they expect the agent to do for them. The guidelines clearly states that even if reporting entities use an agent, they remain responsible for making sure the identification requirements are met. FINTRAC Interpretation Notice n°3 of January 17, 2006 sets out that all persons and entities subject to the PCMLTFA can rely on the use of the agent scenario to ascertain customer's identity; however the ultimate responsibility of ascertaining identity and making any third party determination remains with the person or entity and not their

[96] An amendment enacted in June 2007 and coming into force in June 2008 clarifies the requirements in respect of agency agreements.

agent. FINTRAC Interpretation Notices provide technical interpretation and positions regarding certain provisions contained in the PCMLTFA and related regulations.

754. OSFI Guideline B-10 ("*Outsourcing of Business Activities, Functions and Processes*") deals with outsourcing arrangements that are outside the scope of Recommendation 9. OSFI Guideline B-8 clearly refers to outsourcing record keeping or other functions (including customer identification) that form part of their obligations, or that utilize introducers to gather new business.. In this Guideline, FRFIs that outsource record keeping or other functions that form part of their PCMLTFA compliance regime, or that utilize introducers to gather new business (such as deposit brokers, mortgage brokers, correspondents, law firms, accounting firms, etc., including those outside Canada) are reminded that they retain full accountability for having customer identification and verification processes, and for obtaining customer records with respect to accounts opened through such sources. With respect to introduced business, FRFIs must obtain the necessary customer information for their records prior to, at, or at a reasonable time after, the time that the business is accepted. OSFI recommends that relationships with introducers be subject to written agreements to ensure that the responsibility for collecting and verifying customer identification information is clearly understood. FRFIs should consider terminating relationships with introducers that cannot, or fail to, provide the FRFI with the requisite customer identification and verification data that the FRFI is required to obtain under the PCMLTFA and the Regulations.

755. *Business practice*. As confirmed by the financial sector representatives during the on-site visit, introduced business mechanisms are broadly used by the industry in Canada. For instance, in practice, where banks are not able to verify the identity of a customer directly, verification is typically provided through a Canadian embassy, lawyers, and in the case of businesses, lawyers external to the business, accounting firms, referrals from another financial institution, or other types of agents for particular products or services that a financial institution provides. here is typically no formal contract between the bank and these other parties (there is no outsourcing arrangement). The banking sector believes that in some circumstances, a requirement to enter into contractual arrangements is operationally impractical, as banks would need to enter into multiple contracts with agents in every country in which clients reside or operate or in which signing officers reside or work. In this case, the introduced business scenario takes place (since financial institutions do not enter into formal outsourcing arrangements) although no measures in line with Recommendation 9 are in force.

756. In the securities sector, there are many situations in which businesses make use of agents to act on their behalf. The relationship between a dealer and individuals acting on its behalf may be a principal-agent relationship. IDA By-law 39 covers such relationships. In such cases the agent may be largely indistinguishable from an employee. By contrast, the term "introducer" has a variety of meanings in different contexts. In general, it suggests a pre-existing relationship between the introducer and the customer or prospective customer. It refers to a specific type of services relationship between dealers. IDA Members make use of accounting and law firms to conduct money laundering verification on their behalf using letters of instruction rather than contracts. For IDA, it is always essential that the terms of the relationship be clear. The principal is always responsible for the acts of its agent done within those terms and for keeping proper records of things done by the agent on its behalf.

757. Insurance companies invariably use introduced business too. In the life insurance field, independent brokers and agents are a separate reporting entity under the PCMLTFA and are permitted to identify customers under the PCMLTF regulations. The MSB sector relies largely on its own agents to promote and expand the business network and companies enter into agreements with agents as a general practice.

758. Trust companies utilise introducers to varying degrees to gather new deposit and loan business but remain well aware of their ultimate responsibility and accountability for having full customer identification and verification. Introducers fall under two categories, namely SRO and Non-SRO. Under the former category, they source new business through the IDA or the MFDA members who are

subject to the PCMLTFA. Non-SRO introducers include mortgage brokers and "Guaranteed Investment Certificate" (GIC) Agents/Brokers such as the FCIDB. Business introduced by this category is considered to have a somewhat higher risk profile relative to compliance because they are not directly subject to the PCMLTFA and therefore do not represent the same assurance of compliance. Risks are mitigated by requiring agent/broker certifications as required in signed agreements. In order for business to be accepted by trust companies, each introducer must have a signed agreement in place which specifies the customer information requirements and provides rights of audit to ensure the introducer has appropriate processes in place to meet trust company requirements.

759. *Conclusion*. Outside the very specific situations covered under Sections 56(2) and 57(5), no other introduced business scenarios are contemplated or controlled by the PCMLTF Regulations although the financial sector uses introduced business mechanisms (in addition to outsourcing or agency arrangements) as a business practice. However, no specific requirements as set out in Recommendation 9 apply to these scenarios (since Section 6(2) of the PCMLTF Regulations exclusively covers agency relationships type of arrangements that are outside the scope of Recommendation 9).

3.3.2 Recommendations and Comments

760. Since introduced business arrangements exist in Canada in other circumstances than those captured by Sections 56(2) and 57(5) of the PCMLTF Regulations, Canada should adopt provisions that address all aspects of Recommendation 9 and ensure that financial institutions implement them.

3.3.3 Compliance with Recommendation 9

Rec.	Rating	Summary of factors underlying ratings
Rec.9	NC	• In the only two scenarios where reliance on a third party or introduced business is legally allowed without an agreement or arrangement, the measures in place are insufficient to meet the FATF requirements. • In addition to the two reliance on third parties/introduced business scenarios contemplated by the Regulations, the financial sector uses introduced business mechanisms as a business practice. However, no specific requirements as set out in Recommendation 9 apply to these scenarios.

3.4 Financial institution secrecy or confidentiality (R.4)

3.4.1 Description and Analysis

761. *Access to information for competent authorities*. Section 8 of the Canadian Charter of Rights and Freedoms (the Charter) establishes a fundamental principle that everybody has the right to be secure against unreasonable search and seizure. This Charter protection has a direct impact on law enforcement's ability to seize information and evidence and generally, prior judicial authorisation is required before intrusions can be made upon individual privacy.

762. Section 5 of PIPEDA (which is Canada's data protection law) requires organizations to comply with specific obligations concerning the collection, use and dissemination of customers' personal information but Subsection 7(2) of PIPEDA provides that an organisation can elect to disclose personal information that it has reasonable grounds to believe could be useful in the investigation of a contravention of the laws of Canada, a province or a foreign jurisdiction that has been, is being or is about to be committed and the information is used for the purpose of investigating that contravention. Further subsections of PIPEDA allow an organisation to voluntarily disclose personal information without disclosing the fact to their customer and to comply with subpoenas, warrants and court orders to compel the production of court orders. Section 7(3)(c.1) allows organizations to disclose personal information to government institutions without the knowledge or consent of the individual and without judicial authorisation in certain specified circumstances related to law enforcement and national

security (especially the government institution must identified its lawful authority to obtain the information)[97].

763. The assessment team was told that law enforcement efforts are actually being thwarted by stringent interpretations of PIPEDA with respect to obtaining non-sensitive personal information on a voluntary basis from companies. This finding is also reflected in the Fourth Report of the Standing Committee on Access to Information, Privacy and Ethics that published a review of PIPEDA in May 2007[98]. The report mentions that in some occasions (for instance, a police officer may be in the early stages of an investigation, in which he or she is trying to determine if in fact a crime has occurred. He or she may have to solicit the assistance of a financial institution because he or she needs to know if that person used a credit card for instance and for this information he or she relies on paragraph 7(3)(c.1), which permits disclosure upon lawful authority), companies insist on seeing a court order from a law enforcement or investigative agency before disclosing any personal information pursuant to Section 7(3)(c.1). Some companies interpret "*lawful authority*" to mean that a warrant or court order is required before they comply. This interpretation may not be consistent with the intent of the drafting of the Act and seems overly restrictive. The Standing Committee agrees that there is a valid concern around what constitutes lawful authority for the purposes of disclosure under section 7(3)(c.1). The Committee agrees that clearly something other than judicial authorisation is required for the purposes of this section given that section 7(3)(c) provides for disclosure without knowledge or consent in compliance with a warrant or subpoena[99]. The RCMP indicated to the assessment team that this issue is not a concern as far as AML/CFT investigations are concerned and the RCMP has access to the information it needs to carry out such investigations. Nevertheless, the assessment team believes that further clarification should be brought to the Act to ensure that competent authorities have the ability to access information they require to properly perform their functions.

764. *Sharing of information between competent authorities.* The Canadian Privacy Act requires all federal departments, agencies and most Crown corporations to have lawful, authorised purposes for collection of the personal information of individuals. It also requires these departments, agencies and corporations to notify individuals of those purposes; restricts the purposes for which information collected can later be used or disclosed; and provides individuals a right of access to the personal information about them held by government institutions. The implementation of the Privacy Act does not seem to have caused problems as far as AML/CFT issues are concerned. More issues seem to arise from the PCMLTFA and the interpretation of FINTRAC of "designated information"[100] (see Section 2.5 of the report for further comments).

---

97 Section 7(3)(c.1) says: "*For the purpose of clause 4.3 of Schedule 1, and despite the note that accompanies that clause, an organization may disclose personal information without the knowledge or consent of the individual only if the disclosure is made to a government institution or part of a government institution that has made a request for the information, identified its lawful authority to obtain the information and indicated that (i) it suspects that the information relates to national security, the defense of Canada or the conduct of international affairs, (ii) the disclosure is requested for the purpose of enforcing any law of Canada, a province or a foreign jurisdiction, carrying out an investigation relating to the enforcement of any such law or gathering intelligence for the purpose of enforcing any such law, or (iii) the disclosure is requested for the purpose of administering any law of Canada or a province*".

98 Pursuant to its mandate under Standing Order 108(2), the Committee publishes Statutory Reviews of the Personal Information Protection and Electronic Documents Act (PIPEDA).
See http://cmte.parl.gc.ca/Content/HOC/committee/391/ethi/reports/rp2891060/ethirp04/05-rep-e.htm

99 The Committee believes that it is important, for both organizations and law enforcement agencies, that what is meant by "lawful authority" be clarified in section 7(3)(c.1). Moreover, the Committee feels that consideration should be given to changing the word "may" in the opening part of section 7(3) in order to make the provision mandatory as opposed to permissive.

100 FINTRAC obligation to disseminate financial information to domestic authorities for further action when it has reasonable ground to suspect that the information would be relevant to the investigation or prosecution of a money laundering or terrorist activity offence seems to be too strictly implemented using a higher threshold that the one required by law. The assessors have concerns about the interpretation that is made by FINTRAC of the "threshold to disclose" level that might be reached to disclose.

765. *Sharing of information between financial institutions.* The Bank Act contains provisions regulating the use and disclosure of personal financial information by banks. Most provinces have legislation dealing with consumer credit reporting. These acts typically impose an obligation on credit reporting agencies to ensure the accuracy of the information, place limits on the disclosure of the information and give consumers the right to have access to, and challenge the accuracy of, the information. Provincial laws governing credit unions typically have provisions dealing with the confidentiality of information relating to members' transactions. There are a large number of provincial acts that contain confidentiality provisions concerning personal information collected by professionals. Such provisions do not seem to inhibit the implementation of the FATF Recommendations.

766. Generally the banks are of the view that the PIPEDA has served Canadians well in protecting information collected, used and disclosed about them by private sector organizations and has provided the necessary structure to allow private sector organizations to effectively implement its requirements into their business operations. The assessment team was told that FRFIs can share information with foreign financial institutions where this information is required by Recommendations 7, 9 or Special Recommendation VII. The exchange of information in the context of SRVII has raised concern in the past in relation to Principle 4.1.3 of Schedule 1 of the PIPEDA[101]. In 2006, the Office of the Privacy Commissioner of Canada received a complaint against six Canadian financial institutions as a result of the disclosures by the Society for Worldwide Interbank Financial Telecommunication (SWIFT) of personal information to US authorities. The complainant was of the view the banks were responsible for the personal information that was transferred to SWIFT for processing of money orders and maintained that the disclosures were for an inappropriate purpose since they circumvented established approved processes for transferring data as set out in the PIPEDA. The Privacy Commissioner of Canada analysed the issue (see "Responsibility of Canadian financial institutions in SWIFT's disclosure of personal information to US authorities", PIPEDA case summary 365) and considered the contractual documentation that exists between SWIFT and the banks. She concluded that they are meeting their obligations under the Act, specifically, Principle 4.1.3, to ensure a comparable level of protection when processing wire transfers.

767. A comparable case was also discussed by the Privacy Commissioner of Canada in a context of outsourcing of financial services by a Canadian bank to the United States. While the PIPEDA does not prohibit the use of foreign-based third-party service providers, it does oblige Canadian-based organizations to have provisions in place, when using third-party service providers, to ensure a comparable level of protection. The Privacy Commissioner of Canada concluded that the Canadian Bank had in place a contract with its third-party service provider that provided guarantees of confidentiality and security of personal information and that an organization with a presence in Canada that outsources the processing of personal information to a U.S. firm cannot prevent its customers' personal information from being lawfully accessed by U.S. authorities. the Commissioner finally recommended that a company in Canada that outsources information processing to a third country should notify its customers that the information may be available to the U.S. government or its agencies under a lawful order made in that country.

768. Sharing information within corporate groups is another issue raised by the banking sector. Many corporations that have multiple separate subsidiary companies, as required by federal/provincial regulatory requirements nevertheless operate as one unit under a single management team. With AML requirements, the parent bank's compliance officers must look at the activities of each client across their dealings with the entire banking group, not just each entity separately. In the securities field too, related parties assessments must include information from all parts of the financial group, not each entity separately. The AML requirements require that information about individuals be available to

[101] Principle 4.1.3 sets out that "an organization is responsible for personal information in its possession or custody, including information that has been transferred to a third party for processing. The organization shall use contractual or other means to provide a comparable level of protection while the information is being processed by a third party".

compliance officers, which may result in the sharing of information. In this situation, the institutions must fully apply the PIPEDA provisions and insure that their customers are aware of and consent to that practice so as to satisfy PIPEDA's requirements not to share information with different parts of the corporate group. The banking sector has called for amendments to PIPEDA that would acknowledge these other legislative requirements and facilitate regulatory reporting[102].

3.4.2 Recommendations and Comments

769. Canada should verify that the implementation of the data protection law (PIPEDA) is not subject to excessively strict interpretations that might prevent law enforcement authorities accessing information in the course of investigations.

3.4.3 Compliance with Recommendation 4

Rec.	Rating	Summary of factors underlying ratings
Rec.4	C	• The Recommendation is fully met.

3.5 Record keeping and wire transfer rules (R.10 & SR.VII)

3.5.1 Description and Analysis

Recommendation 10

770. Section 6 of the PCMLTFA states that every reporting entity shall keep and retain prescribed records in accordance with the regulations.

771. The requirement to retain records for a period of at least five years applies across the board to all reporting entities, although it seems a general practice to have a record retention policy and procedures in place to maintain records for at least seven years, largely for tax purposes. Section 69 of the PCMLTF Regulations states that all records that relate to signature cards, account operating agreements, client credit files and account application forms must be kept for at least five years after the date the account is closed. Client information records (i.e. client's name and address and the nature of the client's principal business or occupation), records of certificates of corporation status, records that ascertain the existence of a corporation or entity must be kept for at least five years after the last business transaction is conducted. In respect of all other records, the records must be maintained from the day on which they have been created.

772. Financial entities have to keep the following records:

- Large cash transaction records.
- Account opening records.
- Certain records created in the normal course of business.
- Certain records about the operation of an account (such as account statements).
- Foreign currency exchange transaction tickets.
- Certain records about transactions with non-account holders.
- The name and address of the client initiating a wire transfer for CAD 3 000 or more when the financial entity is acting as an MSB.
- Trust related records (trust companies)[103].

[102] See in particular the Canadian Bankers Association response to the Office of the Privacy Commissioner of Canada on PIPEDA, 7 September 2006.

[103] Receipt of funds records will have to be kept from June 2008 (see Sections 1(2), 36(1), 39(1) (these provisions were finalized on June 27, 2007) and 33.2 and 33.4 (these provisions were pre-published on June 30, 2007) of the amended PCMLTF Regulations).

773. *Large cash transaction record*. For any large cash transaction, the information to be kept in a large cash transaction record includes the following:

- The amount and currency of the cash received.
- The name of the individual from whom the financial entity received the cash and that individual's address and principal business or occupation[104].
- The date of the transaction.
- The purpose, details and type of transaction (for example, the cash was deposited, or the cash was used to buy traveller's cheques, etc.) including whether any other individuals or entities were involved in the transaction.
- How the cash was received (for example, in person, by mail, by armoured car, or any other way).
- If an account was affected by the transaction, include the following:
    - The number and type of any such account.
    - The full name of the client that holds the account.
    - The currency in which the account's transactions are conducted.

774. If the financial entity has to identify the individual, the large cash transaction record also has to contain the following information:

- The individual's date of birth.
- The type of document used to confirm the individual's identity, the document's reference number and its place of issue.

775. In the case of a deposit, the large cash transaction record also has to include the following:
776.

- The name of the client in whose account the amount is deposited. If the amount was deposited to more than one client's account, the record has to include the names of each client.
- The time of the deposit, if it was made during normal business hours, or an indication of "night deposit" for any such deposit made outside your normal business hours.

777. *Account opening records*. These records include those required when the financial entity opens an account, such as signature cards, copies of official corporate records (binding provisions) and other information[105].

778. *Certain Records Created in the Normal Course of Business.* Financial entities have to keep the following records:

- Account operating agreement.
- Debit or credit memos.
- Client credit files[106].

779. *Certain Records About the Operation of an Account.* Financial entities have to keep the following records relating to the operation of an account:

- A copy of every account statement.
- A deposit slip[107] for every deposit made to an account.

---

104 The regulations enacted in June 2007 and coming into force in June 2008 require that the person's date of birth also be recorded (see Subsection 1(2), of the amended PCMLTF Regulations).

105 Information in relation to the intended use of the account will have to be recorded from June 2008 (see Sections 14(c.1) and 23(1)(a.1) of the amended PCMLTF Regulations).

106 "Client credit file" means a record that relates to a credit arrangement with a client and includes the name, address and financial capacity of the client, the terms of the credit arrangement, the nature of the principal business or occupation of the client, the name of the business, if any, and the address of the client's business or place of work.

- Every cleared cheque drawn on or deposited to an account.

780. *Foreign Currency Exchange Transaction Tickets.* For every foreign currency exchange transaction financial entities conduct, regardless of the amount, they have to keep a transaction ticket. A transaction ticket means a record that sets out the following information:

- The date, amount and currency of the purchase or sale.
- The method, amount and currency of the payment made or received.

781. *Transactions of CAD 3 000 or More with Non-Account Holders.* Financial entities have to keep a record for every one of the following transactions that they conduct with a person or entity that is not an account holder:

- If they receive CAD 3 000 or more for the issuance of traveller's cheques, money orders or other similar negotiable instruments. In this case, they shall keep a record of the date, the amount received and the name and address of the individual who carried out the transaction. This record also must indicate whether the amount was received in cash, cheques, traveller's cheques, money orders or other similar negotiable instruments.
- If they cash CAD 3 000 or more in money orders. In this case, they must keep a record of the name and address of the individual cashing the money order. This record also must indicate the name of the issuer of the money order. Or
- If they remit or transmit CAD 3 000 or more by any means or through any individual, entity or electronic funds transfer network. In this case, keep a record of the name and address of the client who initiated the transaction[108].

782. *Trust-Related Records.* Every trust company shall also keep the following records in respect of a trust for which it is trustee: (a) a copy of the trust deed; (b) a record of the settlor's information record; and (c) where the trust is an institutional trust and the settlor is a corporation, a copy of the part of official corporate records that contains any provision relating to the power to bind the settlor in respect of the trust (Section 15(1)).

783. *Third Party Records.* In case of third party determination, financial entities have to keep a record of the following information:

- The third party's name, address and principal business or occupation.
- The incorporation number and place of incorporation if the third party is a corporation.
- In the case of a large cash transaction, the nature of the relationship between the third party and the individual who gives the cash. Or
- In the case of an account, the nature of the relationship between the third party and the account holder.

784. If financial entities are not able to determine that there is in fact a third party, but they have reasonable grounds to suspect that there are instructions of a third party involved, they have to keep a record to indicate the following:

- In the case of a large cash transaction, whether, according to the individual giving the cash, the transaction is being conducted on behalf of a third party. Or
- In the case of an account, whether, according to the individual authorised to act for the account, the account will be used by or on behalf of a third party.

---

[107] A "deposit slip" means a record that sets out the date of a deposit, the holder of the account in whose name the deposit is made, the number of the account, the amount of the deposit and any part of the deposit that is made in cash.

[108] For all these transactions, the date of birth will have to be recorded from June 2008 (see Sections 14(k), (l), (m), 30(c), (d) and(e) of the amended PCMLTF Regulations).

785. This record must also indicate details of why financial entities suspect the individual is acting on a third party's instructions.

786. Life insurers offering certain annuities or life insurance with a savings component or a cash surrender value must retain client information records, including the date of birth (Section 19).

787. Every securities dealer shall keep the following records:

- In respect of every account that the securities dealer opens, a signature card, an account operating agreement or an account application that (i) bears the signature of the person who is authorised to give instructions in respect of the account, and (ii) sets out the account number, where that person's identity was ascertained.
- Where the securities dealer opens an account in respect of a corporation, a copy of the part of official corporate records that contains any provision relating to the power to bind the corporation in respect of that account.
- Where the securities dealer opens an account in the name of a person or of an entity other than a corporation, a record of the name and address and the nature of the principal business or occupation of the person or entity, as the case may be.
- Every new account application, confirmation of purchase or sale, guarantee, trade authorisation, power of attorney and joint account agreement, and all correspondence that pertains to the operation of accounts, that the securities dealer creates in the normal course of business.
- A copy of every statement that the securities dealer sends to a client, if the information in the statement is not readily obtainable from other records that the securities dealer keeps and retains under the Regulations (Section 23).

788. Every money services business shall keep the following records:

- Every client information record that is created for the purpose of an ongoing business relationship between the money services business and a client.
- Where a client information record is in respect of a client that is a corporation, a copy of the part of official corporate records that contains any provision relating to the power to bind the corporation in respect of transactions with the money services business, if the copy of that part is obtained in the normal course of business.
- Where CAD 3 000 or more is received in consideration of the issuance of traveller's cheques, money orders or other similar negotiable instruments, a record of the date, the amount received, the name and address of the person who in fact gives the amount and whether the amount received was in cash, cheques, traveller's cheques, money orders or other similar negotiable instruments.
- Where money orders of CAD 3 000 or more are cashed, a record of the name and address of the person cashing the money orders and the name of the issuer of the money orders.
- Where CAD 3 000 or more is remitted or transmitted by any means or through any person, entity or electronic funds transfer network, a record of the name and address of the client who initiated the transaction (Section 30 of the PCMLTF Regulations).

789. The PCMLTF Regulations set out detailed rules to maintain records of account files and business correspondence. Canadian financial institutions are not required to necessarily retain copies of the documentation upon which reliance is placed for verification of the customer's identity. Reporting entities are expected to note down the type and reference number and place of issue of the identity document but the actual market practice in this area seems to vary. At a provincial level, financial entities are prevented in some cases from taking copies of personal health cards while other banks advised that they would routinely take and retain copies of photo identification, a practice that is supported if not actively encouraged by OSFI. Other banks advised that this practice was not feasible on the basis of practical storage issues.

790. In the PCMLTF Regulations, the obligation to retain records of transactions is limited to certain operations that are listed by type of financial institutions. This may create potential gaps (for instance, there is no obligation in the Regulations to keep a record of all types of business correspondence but only of a limited list of such correspondence).

791. Section 68 of the PCMLTF Regulations states that where any record is required to be kept, a copy of it may be kept (1) in a machine-readable form, if a paper copy can be readily produced from it or (2) in an electronic form, if a paper copy can be readily produced from it and an electronic signature of the person who must sign the record in accordance with the Regulations is retained.

792. Financial institutions must ensure that all records required to be kept under the PCMLTFA can be provided within 30 days (Section 70). Although this may describe an extreme scenario and despite that financial entities advised that they can normally comply in a much shorter timescale, the current rule does not meet the requirement to make CDD records available on a *timely* basis to competent authorities, especially in normal business circumstances.

793. IDA Regulation 200 sets out detailed record keeping requirements of business transactions. The Regulation does not require the various books and records to be kept in any prescribed form. It is expected, however, that the means of recording the information will be complemented by appropriate internal controls to guard against the risk of falsification and will make available clear and accurate information to the Financial Compliance within a reasonable length of time.

Special Recommendation VII

794. At present, Canada has no provisions that address the requirements in relation to SRVII[109].The only existing obligations in relation to electronic funds transfers in the PCMLTF Regulation are as follows:

- Financial entities shall ascertain the identity of every person who requests an electronic funds transfers of CAD 3 000 or more (Section 54(1)(b)) of the PCMLTF Regulations)[110]. The identity of such person shall be ascertained by referring to the person's birth certificate, driver's licence, provincial health insurance card, passport or any similar record (Section 64(1)(a)). The current threshold of CAD 3 000 (that only applies to cross-border transfers) is not in line with SR VII;
- Financial entities (Section 12(1)(b) & (c) and money services businesses (Section 28(1)(b) & (c)) are required to report incoming and outgoing international electronic funds transfers of CAD 10 000 or more to FINTRAC. Information to be reported includes the name, address and account number of the client ordering the electronic funds transfer.

795. There are currently no requirements for ordering financial institutions either to obtain or maintain full originator information or to include such information in cross border wire transfers. The assessors were told that, at present, only originating customer name and address are included in such transfers as the account number is considered to be private personal information.

796. While the assessors were told that financial entities and money services businesses are taking measures in identifying and handling wire transfers that are not accompanied by complete originator information, there is currently no regulatory or legal requirements to adopt risk-based procedures or conduct enhanced due diligence.

---

[109] New provisions will come into force on 23 June 2008 (see Section 66.1 of the amended PCMLTF Regulations that must be read in conjunction with Section 9.5 of the amended PCMLTFA).

[110] "Electronic funds transfer" means the transmission – through any electronic, magnetic or optical device, telephone instrument or computer- of instructions for the transfers of funds, other than the transfers of funds within Canada. In the case of SWIFT messages, only SWIFT MT 103 messages are included" (PCMLTF Regulations).

797. FINTRAC has a responsibility to ensure compliance with the legislative requirements under the PCMLTFA, including the customer due diligence and originator information inclusion requirements for wire transfers. Until the legislative changes take effect and formalise the requirement for full originator information, enforcement measures can only be on a best efforts basis without any formal powers of sanction or penalty.

798. The assessment team was advised that casinos process electronic funds transfers using their own internal corporate system, *i.e.* outside the banking sector. The team is not aware of any controls that exist, and no more details were provided despite the team's request (in this situation, casinos are considered as financial institutions since they conduct a business that is covered under the FATF definition of financial institutions).

3.5.2 Recommendations and Comments

799. *Recommendation 10*. Canada should ensure that all types of transactions (including business correspondence) carried out by financial institutions (except for IDA members) are subject to proper record keeping requirements that permit their reconstruction so as to provide, if necessary, evidence for prosecution of criminal activity. Canada should ensure that all customer and transactions records and information are available on a timely basis to domestic competent authorities.

800. *SR.VII*. Canada should ensure that the new provisions enacted in December 2006 and coming into force in June 2008 are fully in line with the FATF requirements and ensure that reporting entities implement measures that meet the FATF standards. Canada should ensure that the wire transfers operated by casinos outside the banking network are subject to equivalent requirements.

3.5.3 Compliance with Recommendation 10 and Special Recommendation VII

Rec.	Rating	Summary of factors underlying ratings
Rec.10	LC	*Scope issue* • The record keeping requirement does not extend to all financial institutions as defined by the FATF (notably financial leasing, factoring and finance companies); • Financial institutions must ensure that all records required to be kept under the PCMLTFA can be provided within 30 days which does not meet the requirement to make CDD records available on a *timely* basis to competent authorities, especially in normal business circumstances.
SRVII	NC	• Canada has not implemented SRVII.

3.6 Monitoring of transactions and relationships (R.11 & 21)

3.6.1 Description and Analysis

801. Under the PCMLTFA, there is currently no explicit provision requiring that financial institutions must pay special attention to all complex, unusual large transactions[111]. As noted earlier, there is no explicit obligation to conduct on-going monitoring of accounts or transactions under the current legislation.

802. Thus, such a requirement may only be indirectly deduced from the requirement to report to FINTRAC suspicious transactions that may be related to money laundering or terrorist financing, as well as the obligation to report large international electronic funds transfer reports involving CAD 10 000 or more (EFTRs) and large cash transaction reports of CAD 10 000 or more (LCTRs).

803. In its Guidelines, which are provided as general information only, FINTRAC provides indicators, both common and industry-specific, to financial institutions on how suspicious transactions

[111] The PCMLTFA as amended in June 2007 sets out new requirements in this area that will enter into force in June 2008.

can be detected. These indicators include, among others, patterns of unusually large or complex transactions with no economic purpose, such as :

- Transaction that seems to be inconsistent with the client's apparent financial standing or usual pattern of activities.
- Transaction that appears to be out of the ordinary course for industry practice or does not appear to be economically viable for the client.
- Transaction that is unnecessarily complex for its stated purpose.
- Activity that is inconsistent with what would be expected from declared business.
- Client who starts conducting frequent cash transactions in large amounts when this has not been a normal activity for the client in the past.
- Client who asks reporting entity to hold or transmit large sums of money or other assets when this type of activity is unusual for the client.

804. It is worth noting that some regulators or regulatory organizations have introduced additional recommendations or rules relating to the monitoring of unusual transactions:

- Concerning federally regulated financial institutions, OSFI states in very general terms in its Guidelines, that *"the policies and procedures should […] include measures to monitor transactions. These measures will help FRFIs to identify potentially suspicious transactions by using criteria that will enable them to detect unusual or abnormal activity"*. OSFI also encourages FRFIs to implement the Basel *Customer Due Diligence for Banks* paper *"in a manner appropriate to the size, complexity and nature of the institution's business activities"*.
- Concerning securities dealers firms, the IDA has issued regulations and policies related to the supervision of accounts (see Regulation 1300 and Policy n° 2) which contain precise rules relating to the performance by members of reviews aiming at detecting *"items for further investigation or an examination of unusual trading activity or both"*. The IDA Guide on "Deterring money laundering activity – A Guide for Investment Dealers" sets out that "a firm should adopt procedures setting forth appropriate parameters and methods of monitoring account activity so that unusual or suspicious transactions can be detected".

805. The assessors were not provided with any specific AML requirements (excluding FINTRAC non-binding guidelines) that included obligations relating to unusual transactions issued by primary supervisors to other sectors such as credit unions. However, the AMF, in Quebec, indicated that it was in the process of developing AML/CFT standards.

806. The assessors met with a number of large financial institutions, and in practice it seems that such institutions have adopted procedures and systems to detect and further examine complex, unusual large transactions in order to comply with their reporting obligations. Such transactions are usually identified by financial institutions in two different ways: 1) at the front line in executing the transaction for the client; and 2) through the use of software based on rules or profiles to monitor and identify unusual transactions. Unusual transactions are forwarded to corporate security and/or the AML compliance group for further analysis. Where the unusual transaction meets the test of reasonable grounds to suspect ML or TF, a suspicious transaction report is prepared and sent to FINTRAC.

807. Nevertheless, there is insufficient information available to determine whether this practice is universal and the current legislative and regulatory framework remains too general and implicit with respect to the monitoring of complex, unusual large transactions to meet the FATF requirements. In particular, there is no specific requirement that financial institutions examine the background and purpose of such transactions and, especially, set forth their findings in writing. Under the current

legislation, financial institutions are not required to keep a record of the STRs that they file with FINTRAC[112].

808. As a business practice, a number of financial institutions that detect such unusual transactions indicated that they would usually conduct further research on the customer's transactions in order to determine whether, based on the knowledge in hand, the threshold for determining suspicion has been met and hence an STR must be filed with FINTRAC. The section of the report describing the suspicious activity is very important as it explains what led the financial institution to believe there is something suspicious about the transaction. Financial institutions are expected to clearly and completely describe all of the factors or unusual circumstances which led them to a suspicion of money laundering or terrorist financing, and provide as many relevant details as possible to support this determination. Financial institutions are also required to describe what action, if any, was taken by them, as a result of the suspicious transaction, in addition to reporting to FINTRAC. Such action could include, for example, sending a report to law enforcement in addition to FINTRAC. Nevertheless, there are no provisions under the PCMLTFA and PCMLTFR requiring that such actions and their results be documented and kept available for competent authorities, especially if no STR is finally filed with FINTRAC[113].

809. Large financial institutions met by the assessment team such as banks generally appear to comply with this requirement on a voluntary basis. Moreover, concerning securities dealers, the IDA Rulebook requires in Policy n° 2 that *"evidence of supervisory reviews must be maintained. Evidence of the review, such as inquiries made, replies received, actions taken, date of completion etc. must be maintained for seven years and on-site for 1 year"*. But there is no evidence that this practice is generalized among the other types of financial institutions.

Recommendation 21

Special attention to business relationships and transactions with persons from or in countries which do not or insufficiently apply the FATF recommendations

810. Requirement to give special attention to business relationships and transactions with persons from or in countries which do not or insufficiently apply the FATF Recommendations. On every occasion that the FATF has invoked Recommendation 21 in the context of the NCCT (Non-cooperative Country and Territory) process, FINTRAC and OSFI have issued advisories asking financial institutions and reporting entities to pay special attention with respect to any business or affairs being transacted with persons or entities from identified countries or territories. Financial institutions are requested to take this into account directly or through any subsidiary or branch operations. In addition, competent authorities in Canada (including FINTRAC, OSFI and IDA) communicated on a regular basis with the reporting entities to provide regular updates and required financial institutions to pay "special attention by exercising appropriate due diligence and caution in conducting any transactions with such persons or entities"[114].

---

[112] The PCMLTF Suspicious Transaction Reporting Regulations enacted in June 2007 that will come into force in June 2008 require reporting entities to keep a copy of every STR they file with FINTRAC for five years (Section 12.1).

[113] As mentioned above and under Section 12.1 of the PCMLTF Suspicious Transaction Reporting Regulations financial institutions will be required from June 2008 to keep a record of every STR that they file with FINTRAC for five years. A Suspicious Transaction Report, and the related record includes detailed information about the person or entities involved, the nature and type of transaction and a description of the suspicious activity. The Regulations require details of suspicious attempted transaction reports to also be kept on file for five years. Under the new regime, financial institutions have to ensure that such records can be provided to a FINTRAC compliance officer within 30 days. Law enforcement representatives can access these records if they obtain a search warrant or production order from a court.

[114] In October 2007 and consistent with the FATF action, OSFI and FINTRAC issued statements to indicate that Canadian financial institutions and reporting entities should give heightened attention to transactions to Iran.

811. Advisories describe how OSFI administers and interprets provisions of existing legislation, regulations or guidelines, or provide OSFI's position regarding certain policy issues. OSFI clearly states that advisories are not law and that readers should refer to the relevant provisions of the legislation, regulation or guideline, including any amendments that came into effect subsequent to the Advisory's publication, when considering the relevancy of the Advisory. The assessment team was told that failure to implement OSFI advisories could result in regulatory action by OSFI.

812. In FINTRAC and OSFI advisories, reporting entities are generally asked to exercise an enhanced level of scrutiny when dealing with transactions from or in NCCTs involving exercising appropriate due diligence and caution in conducting transactions.

813. Based on these advisories, FINTRAC has included the monitoring of transactions and enhanced due diligence with respect to NCCTs within its compliance verification structure although the advisories are not enforceable and failure to implement them cannot be subject to sanction. There is a section related to NCCTs in FINTRAC's Compliance Questionnaires. As well, it is standard practice in FINTRAC examinations of financial institutions to review the policies and procedures of an entity, with respect to enhanced due diligence with any jurisdictions that the FATF has identified as being of particular concern.

814. FINTRAC Guideline 2 on suspicious transaction reporting provides indicators for identifying suspicious transactions involving other countries, including "transactions involving countries deemed by the FATF as requiring enhanced surveillance". OSFI Guideline B-8 also addresses the need for federally regulated financial institutions to develop higher levels of due diligence when processing transactions connected to NCCTs.

815. When the FATF no longer has concerns regarding a particular jurisdiction, e.g. when NCCTs were de-listed or their status was otherwise changed, both FINTRAC and OSFI have issued further advisories to reporting entities to inform them on the change and request them to continue monitoring transactions from such a jurisdiction as long as it remains of concern.

816. For securities dealers, the IDA requires its members to heighten scrutiny of accounts and transactions from NCCT countries: it requires that its members give special attention to business relations and transactions with persons, including companies and financial institutions, from the NCCT list. The IDA requires that its members ensure strict adherence to the client identification and verification requirements of the Regulations under the PCMLTFA and that relevant sales and operational personnel are made aware of the countries and territories which have been identified as NCCTs.

817. *Measures to ensure that financial institutions are advised of concerns about weaknesses in the AML/CFT systems of other countries.* As regards countries (other than NCCT countries) which do not or insufficiently apply the FATF Recommendations, FINTRAC and OSFI Guidelines call for special vigilance when doing business with a range of entities, including those in countries with inadequate AML/CFT controls; located in offshore jurisdictions; located in countries with highly secretive banking and corporate law; or in countries known or suspected of facilitating money laundering activities. FINTRAC Guideline points out the International Narcotics Control Strategy Report, released by the U.S. Department of State, to assist reporting entities in undertaking a risk analysis of foreign dealings. OSFI also advises banks with correspondent banking operations to implement additional safeguards when dealing with banks operating in jurisdictions they consider to be of higher risk. The IDA advises its members to ensure proper application of the provisions under the PCMLTFA to clients in countries without adequate anti-money laundering regimes such as in the case of the FATF NCCTs list. With the exception of the general advice described above, financial institutions have not been advised of concerns about specific countries that do not or insufficiently apply the FATF Recommendations, or which have specific weaknesses in their AML/CFT systems(even if their system overall could be considered adequate). For example, such advice could result from a mutual evaluation within the FATF or within an FATF Style Regional Body).

818. *Requirement to examine the background and purpose of transactions and keep written records*. There is no explicit requirement for financial institutions to examine the background and purpose of those transactions that have no apparent economic or visible lawful purpose. Financial institutions are not required to document in writing the findings in relation to these transactions and to keep the later available for competent authorities and auditors.

Countermeasures

819. When counter-measures have been considered by FATF against some NCCTs, FINTRAC and OSFI have advised reporting entities to apply enhanced due diligence to financial transactions emanating from, or destined to the specified jurisdiction and viewed them as potentially suspicious. Reporting entities were urged to exercise an enhanced level of scrutiny when dealing with transactions involving the identified jurisdiction and undertake heightened customer identification due diligence measures to ensure that the principals or beneficial owners are identified. In FINTRAC non-binding advisories, financial institutions were advised that financial transactions emanating from, or destined to countries subject to FATF countermeasures had to be viewed by reporting entities as potentially suspicious.

820. The Minister of Finance, under the *Bank Act*, has the authority to approve the establishment of subsidiaries and branches of foreign financial institutions. In addition to requiring criminal checks and broad fit and proper tests, the Minister considers the "National Security" and "Canada's international relations and obligations" tests during the application process. The assessment team was told that this includes consideration of whether a country was found to be severely deficient in its implementation of AML/CFT standards by the FATF. However, there is no evidence that this mechanism has not been used in the context of countermeasures.

821. Canada also notes that it takes counter-measures against countries that pose specific economic and security risks to Canada through the *Special Economic Measures Act (SEMA)*. This legislation provides for a wide range of economic and financial measures against a foreign state, including: seizing or freezing assets of a foreign state, or of persons from that state, restricting or prohibiting Canadians from dealing in property of that state, from exporting, selling, importing, acquiring goods from that state or from providing or acquiring any financial or other services to or from that state. These mechanisms have not been used in a context of a country that continues not to apply or insufficiently applies the FATF recommendations[115].

3.6.2 Recommendations and Comments

822. *Recommendation 11*. In order to comply with Recommendation 11, Canada should ensure that the new provisions enacted in June 2007 are fully in line with the FATF requirements and ensure that reporting entities implement measures that meet the FATF standards.

823. *Recommendation 21*. The requirement to give special attention to business relationships or transactions with persons from or in countries which do not or insufficiently apply the FATF Recommendations should be included in an enforceable legal instrument applicable to all financial institutions. Effective measures should be put in place whereby financial institutions are advised of other countries that have specific weaknesses in their AML/CFT systems. This should be completed by a provision requiring that the background and purpose of such transactions having no apparent economic or visible lawful purpose be examined and the findings documented.

[115] For example, Canada used SEMA in December 2007 against Myanmar - on December 13, 2007, the *Special Economic Measures (Burma) Regulations* came into force in order to respond to the "abhorrent human rights and humanitarian situation in Burma".

3.6.3 Compliance with Recommendations 11 and 21

Rec.	Rating	Summary of factors underlying ratings
Rec.11	PC	• There is no explicit nor enforceable requirement for financial institutions to examine all complex, unusual large transactions under the current legislation (except for IDA members). Except for IDA members, the monitoring obligation is implied and indirect (it flows from reporting suspicious transactions, large international electronic funds transfer and large cash transactions) and it does not cover the full range of monitoring situations as stipulated in Recommendation 11; • There is no explicit requirement to examine the background and purpose of these unusual transactions (except for IDA members) • There is no requirement to keep record of financial institutions' findings in relation to complex, unusual large or unusual patterns of transactions.
Rec.21	PC	• There is no general enforceable requirement for financial institutions to give special attention to transactions or business relationships connected with persons from or in countries which do not or insufficiently apply the FATF Recommendations. • There are no effective measures in place whereby financial institutions are advised of other countries that have specific weaknesses in their AML/CFT systems • There is no requirement to examine the background and purpose of these transactions and to document the related findings.

3.7 Suspicious transaction and other reporting (R.13-14, 19, 25, 32 & SR.IV)

3.7.1 Description and Analysis

Recommendation 13 & Special Recommendation IV

824. *Suspicious transactions reporting obligation*. All financial institutions subject to the PCMLTFA are required to report to FINTRAC transactions of any amount for which there are reasonable grounds to suspect that the transaction is related to the commission of a money laundering offence or a terrorist financing offence (Section 7 of the PCMLTFA). The requirement applies to all persons and entities subject to Part I of the PCMLTFA, including the following financial institutions:

825.

- Financial entities: banks, credit unions, *caisses populaires*, trust and loan companies and agents of the Crown that accept deposit liabilities.
- Life insurance companies, brokers and agents.
- Securities dealers including portfolio managers and investment counsellors.
- Money services businesses including the business of foreign exchange dealing and alternative remittance systems, such as *hawala, hundi* and *chitti*.
- Canada Post for money orders.

826. However, as stated above in Section 3.1 of the report, several categories of financial institution, such as financial leasing, factoring, electronic money institutions, finance companies of customer credit, credit and debit cards companies are not subject to the PCMLTFA and, consequently, to any mandatory reporting requirement to FINTRAC.

827. In the PCMLTFA, the terms "money laundering offence" and "terrorist financing offence" refer directly to their definition in the Criminal Code which indicates that suspicious transaction reports must be made in relation to all the predicate offences to money laundering and terrorist financing. These offences include virtually all indictable offences under the Criminal Code or any other federal Act. The few exceptions are for offences such as those related to tax evasion or breach of copyright and some others that involve administrative and monetary penalty structure.

828. The PCMLTF Suspicious Transaction Reporting Regulations establish the form and manner for reporting, including the list of information to report and prescribe the reporting time limits. A Suspicious Transaction Report must be filed with FINTRAC within 30 days from the date the

suspicion was formed about the transaction. Failure to report a suspicious transaction could lead to up to five years imprisonment, a fine of CAD 2 million, or both.

829. FINTRAC's Suspicious Transactions Reporting guideline further elaborates on the requirement and explains that financial institutions should look at what is reasonable under the circumstances, including normal business practices and systems within the industry, to reach the "reasonable grounds to suspect" threshold. The guideline also provides an extensive list of general and sector specific indicators to help financial institutions assess the behaviour of the customer and their transactions.

830. A Suspicious Transaction Report must include detailed information about the person or entities involved, the nature and type of transaction and a description of the suspicious activity. Certain fields in the report must be filled on a mandatory basis, while others on reasonable efforts, which means that the financial institution must make every effort to obtain the information required in the report. If the information is available or can be obtained from the financial institution's records, it must be included in the report. The suspicious transaction report explains what led the financial institution to identify the transaction as suspicious (part G of the suspicious transaction report). Financial institutions are expected to describe clearly and completely all of the factors or unusual circumstances which led them to a suspicion of money laundering or terrorist financing, and provide as many relevant details as possible to support this determination. Financial institutions are also required to describe what action, if any, has been taken by them as a result of the suspicious transaction, in addition to reporting to FINTRAC. Such action could include, for example, sending a report to law enforcement in addition to FINTRAC, monitoring or closing the account.

831. *Attempted transactions and threshold.* There is no monetary threshold associated to the requirement to report STRs to FINTRAC, all suspicious transactions must be reported regardless of the amount of the transaction.

832. Under the current legislation, reporting entities are only required to report completed transactions to FINTRAC. FINTRAC Guideline 2 indicates that "*the requirement (…) to report a suspicious transaction applies only when the financial transaction has occurred. (…) If you decide or the client decides not to complete the transaction, there is no obligation to report it as a suspicious transaction to FINTRAC*".

833. Financial institutions can choose to report an uncompleted transaction and a suspicion about it directly to law enforcement and can also decide to report it to FINTRAC on a voluntary basis. As a matter of fact, IDA, in a notice of October 2001 about the "Implementation of Suspicious Transaction Reporting Regulations" strongly recommends that its members voluntarily report to either to FINTRAC or the police, of any approach that raises a suspicion of being related to criminal activity or money laundering. Nevertheless, the assessment team was told that by the banking sector that sending such reports is not a current practice in this sector.

834. The PCMLTF Regulations broaden the reporting requirement to the reporting of any suspicious attempted transactions related to money laundering or terrorist financing, but as the implementation of the measure requires IT developments both at FINTRAC and in financial institutions, it will not be in force until June 2008.

835. *Tax matters*. The PCMLTFA requires the reporting of all completed transactions, where there are reasonable grounds to suspect that they relate to the commission of a money laundering or a terrorist financing offence, regardless of the involvement in tax matters. Furthermore, the PCMLTFA allows FINTRAC to disclose information to the Canada Revenue Agency when it meets the dual test of firstly having reasonable grounds to suspect that the information contained in the disclosure would be relevant to money laundering or terrorist financing investigation and secondly, if FINTRAC also determines that the information is relevant to an offence of evading or attempting to evade paying taxes or fraudulently attempting to obtain a tax rebate, refund or credit.

836. *Additional elements*. The predicate offences for money laundering include the commission in Canada of a designated offence or an act or omission anywhere that, had it occurred in Canada would have constituted a designated offence.

837. *Statistics*. The number of STRs reported to FINTRAC is as follows:

	2001/2002	2002/2003	2003/2004	2004/2005	2005/2006	2006/2007	**Total**
STR	3 772	17 358	14 794	19 113	29 367	18 431	**102 835**

838. The following table indicates the number of STRs per fiscal year and by financial sector:

	2001/2002	2002/2003	2003/2004	2004/2005	2005/2006	2006/2007	**Total**
Banks	576	3 623	4 077	5 665	12 084	5 174	**31 199**
Caisses Populaires	1 045	3 357	1 946	3 151	4 918	5 185	**19 602**
Cooperative Credit Society	20	29	-	1	6	0	**56**
Life insurance brokers or agents	1	1	11	2	4	0	**19**
Life insurance companies	10	30	52	29	32	78	**231**
MSBs	1 207	6 962	5 165	6 176	8 090	5 826	**33 426**
Provincial Savings Office	5	61	17	202	336	114	**735**
Credit Unions	639	2 415	2 767	3 905	2 837	1 377	**12 940**
Securities dealers	42	169	80	74	83	48	**496**
Trust and loan companies	31	37	64	214	438	388	**1 172**
Total	3 576	16 684	14 179	19 419	23 910	18 190	**95 958**

839. The total number of STRs sent by the financial sector appears globally satisfactory (an average of 20 000 every year since 2004). Since FINTRAC first became operational, in fiscal year 2001-2002, it has received about one hundred thousand STRs from financial institutions (95 958), representing 97 % of the total of STRs received. The annual total number of STRs has been steadily increasing since 2001/2002.

840. The different categories of financial institutions have however contributed unequally to the total number of STRs received by FINTRAC, with the majority of STRs received from MSBs, followed by banks, *caisses populaires* and credit unions. On the other hand, securities dealers, life insurance companies and, even more noticeably life insurance brokers and dealers have sent limited numbers of STRs.

841. Based on further statistics made available to the assessment team (on Canada request, such statistics cannot be published), it appears that only a limited number of MSBs report STRs to FINTRAC considering the wide range of MSBs active in Canada. Most of the STRs filed are sent by the larger players of the sector.

842. The quality of the reports is improving, following the numerous information and training sessions delivered by FINTRAC to reporting entities. The electronic format of the STRs, although quite constraining (see comments in Section 2.5 of the Report), and the electronic feedback of missing

information on every report filed electronically, help financial institutions to meet their obligations in that respect. An extensive use of the section of the STR intended to receive comments describing the suspicious activity generally helps however to overcome the rather rigid format of the STRs.

843. Indicators of terrorist financing (*e.g.* terrorist listings, particular products and countries involved) have been used by reporting entities in the narrative section of a number of reports submitted to FINTRAC. However, FINTRAC was not able to provide to the assessors the approximate number of STRs reported which have involved suspected terrorist financing.

Recommendation 14

844. *Protection from criminal liability of reporting entities*. Section 10 of the PCMLTFA prescribes the immunity provisions for reporting entities. No criminal or civil proceeding lie against persons and entities for making a suspicious transaction report, a terrorist property report, a large cash transaction report or an electronic funds transfer report in good faith or for providing FINTRAC with information about suspicions of money laundering or of the financing of terrorist activities. In addition, Section 462.47 and 487.014 of the Criminal Code establishes a safe harbour defence for persons or entities disclosing a suspicion of money laundering to the police or the Attorney General.

845. *Tipping off*. Section 8 of the PCMLTFA specifies that no person or entity can disclose that they have made a suspicious transaction report, or disclose the contents of a report, with the intent to prejudice a criminal investigation, whether or not a criminal investigation has begun. Failure to comply with these requirements could result in up to two years imprisonment.

846. *Additional elements*. Subsection 58(2) of the PCMLTFA prohibits FINTRAC from disclosing any information that would directly or indirectly identify an individual who provided a report or information to FINTRAC, or a person or an entity about whom a report or information was provided. FINTRAC employees and contractors are subject to criminal penalties of up to five years in jail or a fine of CAD 500 000 or both, for unauthorised disclosure or use of information.

847. FINTRAC is subject to the Privacy Act that strictly regulates how federal institutions can use and disclose personal information collected about individuals. In addition, the PCMLTFA stipulates that one of FINTRAC's objectives is to ensure that the personal information under its control is protected from unauthorised disclosure. High standards of information privacy and security are important for FINTRAC and FINTRAC continually monitors its systems and recently made improvements to its security monitoring capabilities.

848. Based on the discussions that took place during the on-site visit, the assessment team came to the conclusion that no major issues arise in relation to the implementation of the requirement sunder Recommendation 14.

Recommendation 25 (only feedback and guidance related to STRs)

Guidance related to STRs

849. FINTRAC gives very detailed guidance related to STRs to assist financial institutions in implementing and complying with STR requirements. FINTRAC has developed standard reporting form for all types of existing reporting. Such guidelines are posted on the FINTRAC website.

850. In relation to STR requirements, FINTRAC has adopted two guidelines that deal specifically with STRs: Guideline 2: Suspicious Transactions provides information on identifying suspicious transactions, including common an sector-specific indicators related to money laundering and indicators related to terrorist financing. Guideline 3: Submitting Suspicious Transaction Reports to FINTRAC; delivers very detailed information on, among other things: timelines and format (electronic vs. paper) of the report, instructions for completing reporting forms including the type of information to deliver under each field of the reporting form, etc.

851. The industry bodies spoken to by the evaluation team expressed satisfaction at the guidance provided in relation to the reporting requirement.

Feedback

852. The ways FINTRAC may provide feedback includes the following general and specific elements:

- The Annual Report provides general feedback such as:
  - statistics on reports received
  - disclosures made
  - contribution of each type of report to these disclosures
  - a sanitized ML case
  - typologies and indicators of ML and TF
- Electronic feedback on every report filed electronically.
- Feedback session, at least once a year, to the Canadian Bankers Association (CBA) and the CBA Anti-Money Laundering Working Group.
- Annual presentation to ten of the largest providers of reports.
- Presentations to each reporting sector at least once a year.
- Meeting on a one-on-one basis with individual reporting entities to discuss any issues an entity may have.
- FINTRAC staff also make presentations at, and participate in, industry conferences attended by representatives of reporting entities.
- Macro analysis of patterns, typologies and trends (international, national, regional and sectoral) that characterize money laundering and terrorist activity financing.

853. FINTRAC provides financial institutions and DNFPBs with general and specific feedback.

General Feedback

854. FINTRAC provides feedback presentations to each reporting entity sector (*e.g.* at industry association conferences or other meetings) at least once a year. These feedback sessions include discussions of general reporting trends for the sector and how STRs and other reports from that sector contributed to FINTRAC's disclosures to law enforcement. Other issues, including quality of reporting, are also discussed.

855. Presentations are tailored specifically to either a reporting entity, or an association covering a group of reporting entities, by illustrating the percentage of reports they submitted versus other reporting entities and pinpointing the percentage of their reports that factored into ML and/or TF disclosures.

856. For example, FINTRAC meets at least once a year with the Canadian Bankers Association (CBA) and the CBA Anti-Money Laundering Working Group. CBA members provide approximately 65% of all reports received by FINTRAC. These feedback sessions are a minimum of half a day in duration and address everything from their membership's contribution to reporting (by report type), systematic quality or timing issues, and the way in which their member's reports contributed to ML and/or TF disclosures. FINTRAC tactical analysts participate to these sessions and present various sanitized ML and/or TF cases.

857. FINTRAC also provides similar presentations to about ten of the largest providers of reports. In 2005-06, FINTRAC staff prepared 17 presentations to be delivered to individual reporting entities and industry associations representing different types of reporting entities and in 2004-05, there were 20 such meetings.

858. FINTRAC provides reporting entities with information about internationally recognized trends and typologies. With time, the volume of STRs (and other reports) and the number of disclosures continue to increase considerably, allowing FINTRAC to identify patterns, typologies and trends based on its own work (international, national, regional and sectoral) that characterize domestic money laundering and/or terrorist activity financing.

859. FINTRAC's annual report is another way to provide feedback to reporting entities. For instance, the 2006 annual report presents a very complex sanitized ML case to demonstrate how it uses reports received from reporting entities and what FINTRAC includes in a disclosure to law enforcement. FINTRAC's annual reports also provide statistics on various types of reports received from reporting entities and on disclosures made to law enforcement and the contribution of each type of report to these disclosures. Annual reports also present indicators of ML and TF. Every year, FINTRAC's Annual Report is tabled before the Canadian Parliament in the fall, and is provided in hardcopy format to reporting entities, as well as posted on the FINTRAC's website.

860. There is a need for FINTRAC to publish more concrete and targeted information on ML and TF. The information published by FINTRAC is in general very descriptive and does not provide very in depth analysis. FINTRAC should be able to provide more comprehensive data on techniques and trends in specific sectors. The Annual Report 2006 for instance publishes one sanitised case; the assessors are of the view that more ML/TF cases should be made public in sanitized form in order to increase awareness and improve compliance and reporting. FINTRAC is in quite a unique position to develop and disseminate strategic intelligence but has not taken advantage so far to develop more substantive information.

Specific Feedback

861. FINTRAC automatically provides electronic feedback on every report filed electronically (over 99% of reports submitted to FINTRAC are filled electronically). This feedback highlights to reporting entities any data quality issues that are present or any potential data quality issues they may want to review on a report-by-report basis. FINTRAC also immediately advises a reporting entity if its report was accepted or rejected due to significant data quality issues. FINTRAC can also request that reporting entities re-submit reports received if certain data elements are missing.

862. Given the time sensitivity of STRs, FINTRAC will also provide direct verbal follow-up on the quality of the reports. However, the PCMLTFA prohibits FINTRAC from providing feedback on the outcome of the individual reports made to FINTRAC.

863. FINTRAC has developed comprehensive guidance and quite good general feedback for reporting entities. FINTRAC has initiated a series of feedback presentations for a number of large reporting entity sectors and entities. These presentations offered initial insights on reporting levels, the use of reports in our case disclosures, as well as some examples of sanitized cases. However, the general feedback concentrates more on large financial institutions.

Recommendation 19

864. The PCMLTFA requires reporting entities to submit reports to FINTRAC on large cash transactions and electronic funds transfers.

865. Section 9 of the PCMLTFA establishes a requirement for all persons and entities subject to Part 1 of the PCMLTFA to report to FINTRAC any transaction prescribed in regulations. Two types of reportable transactions are prescribed under the PCMLTF Regulations: large cash transactions and international electronic funds transfers.

866. Financial institutions (as well as accountants, casinos and real estate brokers and sales representatives) are required to report to FINTRAC the receipt of an amount in cash of CAD 10 000 or more in Canadian currency or its equivalent in foreign currency. Reportable cash transactions include

single transactions and two or more transactions by or on behalf of the same individual or entity that are conducted in a 24-hour period and that total CAD 10 000 or more, as described under section 3 of the PCMLTF Regulations. A Large Cash Transaction Report (LCTR) must be submitted to FINTRAC within 15 days of the transaction.

867. With respect to the large cash transaction reporting regime, an exception scheme – called the Alternative to Large Cash Transaction Reports to FINTRAC – is provided for in the PCMLTF Regulations. In order to assist reporting entities, FINTRAC has developed a guideline on the Alternative to LCTRs, Guideline 9, which is posted on the FINTRAC website.

868. Alternative to sending large cash transaction reports applies only to certain clients of financial entities (banks, credit unions, *caisses populaires*, trust and loan companies and an agent of the crown that accepts deposit liabilities) that are corporations. Criteria have to be met before financial entities can choose for the alternative to large cash transaction reports:

- The client of the financial entity is a corporation that carries on business within a list of business excluding business with high risk of ML or TF.
- The client of the financial entity must have an account with the financial entity or another financial entity for at least 24 months.
- The client deposited CAD 10 000 or more in cash at least twice a week, on average, for the preceding 12 months.
- The cash deposits are consistent with the usual practices of the business;
- Reasonable measures have been taken to determine the source of the cash for the deposits.

869. Where these conditions are met, financial entities are not obliged to submit large cash transaction reports to FINTRAC but have to:

- Send a report to FINTRAC about the business client for whom they are making this choice.
- Report certain changes about the business client to FINTRAC.
- Verify annually that conditions are met for each client and report this to FINTRAC.
- Maintain a list with the name and address of each client for whom they have chosen not to report large cash transactions.

870. Reportable information in a LCTR is listed in Schedule 1 to the PCMLTF Regulations. The record includes identifying and banking information on the person or entities involved, including persons on behalf of who the transaction is conducted and the purpose and details of the transaction.

871. Similar reporting requirements apply to deposit taking institutions and money services businesses (including foreign exchange dealers) in respect of outgoing and incoming international electronic funds transfers of CAD 10 000 or more (including single transactions and two or more transactions by or on behalf of the same individual or entity that are conducted in a 24-hour period and that total CAD 10 000 or more). These include both transfers made using the SWIFT system, as well as those using proprietary systems (non-SWIFT). An Electronic Funds Transfer Report (EFTR) must be filed within five working days of the transfer.

872. Since FINTRAC first became operational, in fiscal year 2001-2002, it has received about 16 million LCTRs and 29 million EFTRs.

873. The criminal penalty for failure to report a LCTR or EFTR could lead to a fine of up to CAD 500 000 for a first time offence and CAD1 000 000 for a subsequent offence.

874. FINTRAC devotes resources to improving the data quality, refining analytical tools and upgrading systems.

875. High standards of information privacy and security are important for FINTRAC, as already explained in section 2.5. FINTRAC continually monitors its systems and recently made improvements to its security monitoring capabilities.

Statistics

876. Statistics available at FINTRAC are generally very comprehensive (especially on STRs, LCTRs and EFTRs). However, this report delivers a limited range of them on Canada request and for confidentiality purposes.

3.7.2 Recommendations and Comments

877. All financial institutions covered by the definition of the FATF should be subject to the suspicious transactions reporting requirement unless a proven low risk of ML and FT is established in the sectors that are currently exempted. The different categories of financial institutions contribute unequally to the total number of STRs received by FINTRAC, this is an issue that FINTRAC should address further.

878. FINTRAC should develop more general feedback for smaller reporting entities. While legislation prevents FINTRAC from giving feedback on how it has used specific reports, FINTRAC should consider implementing more specific feedback mechanisms.

879. FINTRAC could consider disseminating more figures and data that do not breach applicable confidentially rules. This would certainly help increasing awareness and improving general compliance and reporting. FINTRAC should collect more data on the number of reports that it receives in relation to suspected terrorist financing.

3.7.3 Compliance with Recommendations 13, 14, 19, 25 and Special Recommendation IV

Rec.	Rating	Summary of factors underlying ratings
Rec.13	LC	▪ Some financial institutions as defined by the FATF (especially financial leasing, finance companies, providers of e-money) are not covered by the obligation to report; ▪ There is no requirement to report attempted transactions; ▪ The low numbers of STRs sent by certain financial sectors raise concerns in relation to the effectiveness of the reporting system.
Rec.14	C	▪ The Recommendation is fully met.
Rec.19	C	▪ The Recommendation is fully met.
Rec.25	LC	▪ There is not enough general feedback given outside the large financial institutions sector.
SR.IV	LC	▪ Some financial institutions as defined by the FATF (especially financial leasing, finance companies, providers of e-money) are not covered by the obligation to report; ▪ There is no requirement to report attempted transactions.

Internal controls and other measures

3.8 Internal controls, compliance, audit and foreign branches (R.15 & 22)

3.8.1 Description and Analysis

Recommendation 15

880. Currently, the PCMLTFA itself contains no specific requirement for the development and maintenance of an AML/CFT compliance regime by the reporting entities[116]. Such a requirement is

[116] Article 9.6 (1) of the PCMLTFA provides for a general compliance program requirement in force in June 2008. The compliance regime requirements will be expanded to include, among other things, a written

prescribed in Section 71 of the PCMLTF Regulations that requires every person or entity subject to the PCMLTFA to establish a compliance regime for complying with the PCMLTFA. The compliance regime must include, "as far as practicable", the following four core elements:

a. The appointment of a person who is responsible for the implementation of the compliance regime.
b. The development and application of compliance policies and procedures.
c. A review of those policies and procedures that is conducted as often as necessary to test their effectiveness by an internal or external auditor of the person or entity or, if it does not have such an auditor, by the person or entity itself (the proposed regulations require minimum review once every 2 years).
d. Where the person or entity has employees or agents or persons authorised to act on behalf of the person or entity, an ongoing compliance training program for those employees, agents or persons.

881. The "as far as practicable" illustrates the need to adopt more or less sophisticated or formal policies and procedures depending on the size of the business.

882. FINTRAC's Guideline 4 provides more specific direction on what is expected to be in place for each component of the compliance program based on the type and the size of the business of the reporting entity. Other financial sector regulators impose similar requirements on their respective supervised entities.

Internal Policies, Procedures and Controls

883. The current PCMLTF Regulations require reporting entities to develop and apply policies and procedures to comply with the anti-money laundering and anti-terrorist financing requirements imposed under Part I of the PCMLTFA. FINTRAC's Guideline 4 provides further details on what these policies and procedure should encompass, including policies and procedures that must show the business's commitment to prevent, detect and address non-compliance. In addition, such policies and procedures must incorporate, at a minimum, the reporting, record-keeping and client identification requirements applicable to the business and it is suggested that they specify situations where an enhanced level of caution is required. Nevertheless, it is not specifically required that rules regarding detection of unusual and suspicious transactions be included. However, when performing its compliance assessments, FINTRAC does inform reporting entities that they should have policies and procedures to identify and report suspicious transactions.

884. OSFI Guideline B-8 goes beyond the basic requirements laid down by the PCLMLTF Regulations and the FINTRAC Guidelines by specifying that "*the policies and procedures should include measures to permit the FRFIs to identify and report Large Cash Transactions. The policies and procedures should also include measures to monitor transactions*". The IDA rules specify that "*firms should have procedures in place that are designed to assist personnel in detecting unusual or suspicious activities*". The IDA has generally advised that AML/CFT policies and procedures should be integrated into a dealer's general compliance regime, for example in the guide "Deterring Money Laundering Activity", the IDA notes: *"a firm's existing policies and procedures for its various business functions should form the basis for its overall money laundering prevention program. This will assure that anti-money laundering compliance reaches all aspects of a firm's business. As an initial matter, a firm could consider reviewing and evaluating those procedures and, where appropriate, enhance them to address anti-money laundering issues"*.

885. The degree of detail and formality of the procedures and policies depends on the business's type of activities and on risk of exposure to money laundering and terrorist financing. Currently, it is not

assessment of the money laundering and terrorist financing risks through regulations enacted in June 2007 and in force in June 2008.

specified in the PCMLTF Regulations that such procedures and policies should be written and kept up to date[117], even if this requirement is considered by FINTRAC as being implicit. OSFI specifies in its Guideline B-8 that "*policies and procedures should be formally documented*". IDA requires "*written anti-money laundering procedures*" in its non-binding "*Deterring money laundering activity*" Guide.

886. According to FINTRAC Guidelines, the business's policies and procedures must be communicated, understood and adhered to by any employee who deals with clients and their assets or who could be affected by the requirements under Part1 of the PCMLTFA and its Regulations. They need enough information to process and complete a transaction properly as well as to identify clients and keep records as required. They also need to know when an enhanced level of caution is required in dealing with transactions, such as those involving countries or territories that have not yet established adequate anti-money laundering regimes consistent with international standards. Information about this, including updates to the list of NCCTs issued by the FATF is available on FINTRAC's website[118] and all of the advisories that FINTRAC has issued throughout the years can be found in the 'FINTRAC Advisories' section of the website[119]. Although directors and senior officers may not be involved in day-to-day compliance, they need to understand the statutory duties placed upon them, their staff and the entity itself.

Appointment of a Compliance Officer

887. Section 71 of the PCMLTF Regulations requires reporting entities to appoint a compliance officer who is responsible for the implementation of the compliance regime.

888. According to FINTRAC Guidelines, the compliance officer should have the authority and the resources necessary to discharge his or her responsibilities effectively. Depending on the type of business, the compliance officer should report, on a regular basis, to the board of directors or senior management, or to the owner or chief operator.

889. If the reporting entity is a small business, the appointed officer could be a senior manager or the owner or operator of the business. If the reporting entity is comprised of an individual, this person can appoint themselves as compliance officer or they may choose to appoint another individual to help them implement a compliance regime. In the case of a large business, the compliance officer should be from a senior level and have direct access to senior management and the board of directors. Further, as a good governance practice, the appointed compliance officer in a large business should not be directly involved in the receipt, transfer or payment of funds.

890. For consistency and ongoing administration of the compliance regime, the appointed compliance officer may choose to delegate certain duties to other employees, for example, the officer may delegate an individual in a local office or branch to ensure that compliance procedures are properly implemented and enforced at that location.

891. OSFI's Guideline B-8 states that the compliance officer should ensure that every division potentially exposed to money laundering or terrorist financing activities appoints an officer to ensure that these divisions implement their policies and procedures. These officers should report regularly on compliance issues and weaknesses in policies and procedures. The financial institution should also designate employees to be accountable for ensuring that policies and procedures intended for these branches are applied. The identification of the AML/CFT compliance officer (CAMLO) must be communicated to OSFI as part of the annual "OSFI-57: Return of Corporate Information" report (for domestic entities) and "OSFI-57A Return of Corporate Information (for foreign entities. In addition, an amended return must be filed disclosing the name of a new CAMLO should a new person be

---

117 The PCMLFT Regulations enacted on 27 June 2007 fill this gap. They require that compliance policies and procedures are written, approved by a senior officer and kept up to date (see Section 71 of the amended PCMLTF Regulations).

118 http://www.fintrac-canafe.gc.ca/intro-eng.asp.

119 http://www.fintrac-canafe.gc.ca/publications/avs/1-eng.asp.

appointed to the position during the year. OSFI Guideline B-8 advises that the CAMLO's mandate be enterprise-wide.

892. Other regulators of financial institutions in Canada have had similar requirements in place, that in some cases have preceded the PCMLTFA requirements. For example, every IDA member is required to designate its Chief Executive Officer, its President, its Chief Operating Officer or its Chief Financial Officer (or such other officer designated with the equivalent supervisory and decision-making responsibility) to act as an "Ultimate Designated Person", responsible for the conduct of the firm and employees. An "Alternate Designated Person" must also be approved to act as Chief Compliance Officer (see IDA By-Law No.38). Firms may be required to designate more than one Chief Compliance Officer depending on the scope and complexity of its business. Alternatively, the Ultimate Designated Person can also act as the Chief Compliance Officer. The responsibilities of the Ultimate Designated Person and Chief Compliance Officer include ensuring firm compliance with IDA and provincial Securities Act regulations, along with federal regulations, such as, the PCMLTFA.

893. Apart from the very generic wording in the FINTRAC Guidelines, there is no explicit requirement to ensure that the AML/CFT compliance officer has timely access to customer identification data and other CDD information, transactions records and other relevant information. The assessors were told that OSFI, in conducting its AML/CFT assessments, has never identified a situation where the CAMLO has not had timely access to all the information needed.

Review of the Compliance Policies and Procedures

894. Another component of a comprehensive compliance regime is a review of the reporting entity's compliance policies and procedures, as often as is necessary, to test their effectiveness.

895. Section 71 of the PCMLTF Regulations requires reporting entities to review their anti-money laundering and anti-terrorist financing policies and procedures "as often as necessary" to test their effectiveness by an internal or external auditor, or if there is no auditor, by the person or entity itself. FINTRAC's Guideline 4 provides a list of triggers that might suggest when a review is needed, such as changes in the legislation, the issuance of new products or services and non-compliance issues[120].

896. It is specified in FINTRAC Guideline 4 that the review is to be completed by an external or internal auditor, if the entity has one. It is indicated that the review could include interviews, tests and sampling. The scope and results of the review should be documented and deficiencies should be identified and reported to senior management or the board of directors. A request for a response indicating corrective actions and a timeline for the implementation of such actions must be sent with the report to senior management and both the request and the response should be documented.

897. FINTRAC's Guideline 4 also indicates that reporting entities must conduct a self-review when it is impossible to have an auditor. The person conducting the review has to be independent, "if feasible", of the reporting, record-keeping and compliance monitoring functions. The review has the same objectives as those conducted by an auditor and should be documented. It should address whether policies and procedures are in place and are being adhered to, and whether procedures and practices comply with legislative and regulatory requirements. It should include corrective measures and follow-up actions.

898. The scope and details of a review will depend, according the FINTRAC's Guideline 4, on the nature, size and complexity of the operations of the reporting entity.

899. Thus, there is no actual requirement for an independent audit function to test AML/CFT regime compliance for small financial institutions (including small MSBs)for which a simple self-assessment is admitted. Moreover, the review of the AML/CFT compliance has to be performed only "as often as

[120] Amendments to section 71 will require, as of June 2008 that this review be conducted every two years.

necessary" and the methods to be used to perform the review (including sample testing) are only quoted in the FINTRAC Guideline as an indication.

900. OSFI's Supervisory Framework considers internal audit to be a key risk management function and assesses it accordingly during the review cycle. Moreover, pursuant to OSFI's Guideline E-13 - Legislative Compliance Management (LCM), FRFIs are obligated to implement a compliance management control on an enterprise-wide basis to ensure that they have the ability to meet all regulatory requirements.

901. OSFI Guideline B-8 states that the independent audit of the AML/CFT Compliance Program should be conducted annually. The Guideline indicates that the review of the business's AML/CFT program should encompass three processes. First, FRFIs have to establish an internal compliance reporting process, which should demonstrate at a minimum conformity with all AML and CFT requirements. It should also review regularly compliance issues and identify and document any weaknesses. These weaknesses shall be reviewed with OSFI.

902. The second process is an annual self-assessment, which must evaluate on a group-wide basis the effectiveness of the AML/CFT procedures to identify the areas and types of risks and suggest corrective measures to address weaknesses and gaps in the risk management system. The results must be reported to senior management and the board of directors. The document should contain the scope of the review, the main elements of policies and procedures, as well as the extent to which policies and procedures comply with the PCMLTFA and its Regulations and OSFI's Guidelines.

903. The last process consists of independent procedures testing to be conducted by the internal audit department, compliance department, or by an outside party such as an external auditor. The testing must cover the entire operation of the entity and must be performed at least annually. The results should be documented and reported to senior management and the board of directors. The report should not only include steps to be taken to address weaknesses and gaps, but could also address areas such as the employees' knowledge of policies and procedures, systems for client identification, large cash transaction and suspicious transactions identification and reporting, and record keeping.

904. Together, the annual self-assessment and independent procedures testing, coupled with LCM requirement, create a control environment which, if implemented effectively, will identify weaknesses or compliance deficiencies in a timely fashion and permit corrective measures to be taken by the financial institutions' senior management and boards of directors. To reinforce the importance of a strong control framework, evidenced through measures such as policies, procedures and other controls, OSFI held information sessions for the industry on November 9, 2005 and October 17, 2006.

905. Other regulators of financial institutions in Canada require similar policies and procedures. In the securities industry for example, IDA By-law 29.27 requires member firms to establish and maintain internal procedures, policies and controls, including compliance procedures for monitoring and reporting adherence to all laws, rules, regulations, requirements, policies and procedures governing their business. The broad scope of the requirement covers AML/CFT laws and regulations. IDA members must establish a compliance monitoring system to prevent and detect violations, that includes a procedure for reporting results of its monitoring efforts to management and, where appropriate, the Board of Directors or its equivalent. Under IDA By-law 38 IDA the Chief Compliance Officer must, at a minimum, report annually to the Board of Directors or its equivalent on the state of compliance at the dealer. The Board of Directors is subsequently required to review the report and determine necessary actions to address any compliance deficiencies noted in the report. Another example can be found in Quebec where the designation of a Compliance Officer (CO) is required by Québec securities regulation and the compliance officer must have access to all necessary information to carry out his function.

906. Furthermore IDA "*Deterring money laundering activity*" Guide specifies that "except for very small firms", the audit should be at least annual and that firms should keep records of measures taken to correct any weaknesses identified in the audit.

Ongoing Compliance Training

907. Section 71 of the PCMLTF Regulations requires every reporting entity to provide ongoing training to their employees, agents or any other person authorised to act on behalf of the business.

908. As further explained in FINTRAC's Guideline 4, reporting entities must not only develop compliance policies and procedures, but ensure that these policies and procedures are understood by all employees within the organization and agents who have contact with customers, who see customer transaction activity, or who handle cash in any way understand the reporting, client identification and record-keeping requirements. This includes those at the front line as well as senior management. In addition, others who have responsibilities under the compliance regime, such as information technology and other staff responsible for designing and implementing electronic or manual internal controls should receive training. This could also include the appointed compliance officer and internal auditors.

909. Reporting entities must address standards for the frequency and method of training, such as formal, on-the-job or external. New people should be trained before they begin to deal with customers. All should be periodically informed of any changes in anti-money-laundering or anti-terrorism legislation, policies and procedures, as well as current developments and changes in money laundering or terrorist activity financing schemes particular to their jobs. Those who change jobs within the organization should be given training as necessary to be up-to-date with the policies, procedures and risks of exposure to money laundering or terrorist financing that are associated with their new job.

910. The method of training may vary greatly depending on the size of the business and the complexity of the subject matter. The training program for a small business may be less sophisticated and not necessarily formalized in writing. In line with FINTRAC guidelines and when assessing training needs, a reporting entity should consider the following elements:

- *Requirements and related liabilities:* the training should give those who need it an understanding of the reporting, client identification and record-keeping requirements as well as penalties for not meeting those requirements.
- *Policies and procedures:* the training should make the entity's employees, agents, or others who act on its behalf aware of the internal policies and procedures for deterring and detecting money laundering and terrorist financing that are associated with their jobs. It should also give each one a clear understanding of his or her responsibilities under these policies and procedures and of how their institution, organization or profession is vulnerable to abuse by criminals laundering the proceeds of crime or by terrorists financing their activities. Training should include examples of how the entity's particular type of organization could be used to launder illicit funds or fund terrorist activity.
- *Background information on money laundering and terrorist financing*: any training program should include some background information on money laundering so everyone who needs to understand what money laundering is, why criminals choose to launder money and how the process usually works. They also need to understand what terrorist financing is and how that process usually works. FINTRAC makes material available on its website that can provide help with training.

911. OSFI's Guideline B-8 further stipulates that employees of FRFIs should receive sufficient training. This training must encompass the policies and procedures of the entity, the techniques used by money launderers in financial institutions and current AML/CFT legislation and regulation. Special attention must be given to front-line staff.

912. When OSFI undertakes AML/CFT assessments it reviews the material produced by each financial institution to train its staff. The assessors were told that employee knowledge is ascertained through interviews, during on-site reviews and assessing the account opening process. It is expected that all new employees receive adequate training before dealing with customers and that continuing employees receive training appropriate to their responsibilities at least on an annual basis. In this regard, a number of recommendations and requirements have been given to improve the AML/CFT training given by financial institutions to assist employees in understanding money laundering and terrorist financing and its consequent reporting processes.

913. AML/CFT requirements have been included in the IDA's mandatory courses for those dealing with the public or holding supervisory positions. Those courses touch on conduct and practices handbook for securities industry professionals, partners, directors and senior officers' examination, branch managers' course and chief compliance officers course (under development).

914. In addition to mandatory courses, the IDA has a mandatory continuing education program and sets guidelines for acceptable continuing education course content, length and rigor (see IDA Policy 6). The guidelines recommend a process to aid firms in identifying appropriate suppliers and courses. The IDA requires that certain persons successfully complete a compliance course within a three-year cycle. These courses must review critical regulations and application, regulatory changes, rules relating to new products and ethics. Anti-money laundering laws and regulations and their implementation at the member is highlighted in the IDA Policy 6. As part of the audit process, the IDA will review member-developed compliance courses to ensure they satisfy the guidelines. IDA member firm AML/CFT training is reviewed during the IDA's sales compliance audits.

Screening procedures when hiring employees

915. There is currently no general enforceable requirement for Canada's financial institutions to screen candidates for employment.

916. Under OSFI's Supervisory framework, the FRFI's senior management and/or the board of directors are responsible for planning, directing and controlling the strategic direction and general operations. One of their key responsibilities includes developing sound business practices, culture and high ethical standards within the financial institution that help protect its reputation. This is primarily achieved by the developing of sound human resource policies associated with staff selection, hiring, retention, conflict of interest and code of conduct. As such, it is in the best interest of senior management and the board at the financial institutions to adopt appropriate and relevant screening procedures when hiring employees to ensure that potential employees have high ethical standards so as to minimize exposure by the financial institution or its clients to potential abuses or reputational risks issues. Consequently, as part of its supervisory role and in assessing the board and senior management control functions, OSFI would expect them to have adopted appropriate screening procedures at the financial institution to ensure high standards when hiring potential new employee. In this respect, OSFI has issued a draft Guideline (E-17) outlining principles to assist FRFIs in establishing policies and procedures regarding the conduct of assessments of their Responsible Persons (*i.e.* directors, senior officers, principal officers, chief agent or any person playing a significant role in the management of the financial institution) upon their initial appointment and at regular intervals. This Guideline will nevertheless remain limited to responsible persons and will not concern all employees.

917. As a practice, Canada's largest banks screen all new potential employees to determine if they have criminal records. Such screening is made possible by a Memorandum of Understanding between the Canadian Bankers Association and the RCMP. In addition, participating banks can screen the names of potential employees against a list of previous bank employees who may have been dismissed by another participating bank for undertaking unethical activities against the bank or its client.

918. The IDA also oversees the professional standards and educational programs that ensure the competence of securities industry employees. The IDA screens all investment advisors employed by

member firms to ensure that those entering the industry are of good character and have successfully completed all the required educational courses and programs. The IDA requires that member firm employees who deal with the public interest must be licensed. The IDA does this more as part of its mandate to protect the public interest and the integrity of the capital markets rather than as a service to members. The IDA has good access to information that its members may not have, such as reports from previous employers and occasionally other confidential information.

Recommendation 22

919. Section 15(4) of the Bank Act states that "subject to this Act, a bank has the capacity to carry on its business, conduct its affairs and exercise its powers in any jurisdiction outside Canada to the extent and in the manner that the laws of that jurisdiction permit." A similar provision is set out in the Insurance Companies Act (Section 15.4). However, Canadian financial institutions and any branches or subsidiaries are generally subject to the laws of the jurisdiction in which they are incorporated. The assessment team believes that the provisions as set out in the Bank Act and in the Insurance Companies Act are insufficient to address the specific requirements in the context of Recommendation 22.

920. Currently, the PCMLTFA and PCMLTF Regulations contain no specific enforceable provision requiring financial institutions to ensure that their foreign branches and subsidiaries observe AML/CFT measures consistent with home country requirements[121]. There is no legal obligation in the PCMLTFA and PCMLTF Regulations that, where the minimum AML/CFT requirements of the home and host countries differ, branches and subsidiaries in host countries are required to apply the higher standard, to the extent that local (*i.e.* host country) laws and regulations permit. Equally, there is no requirement that financial institutions be required to inform their home country supervisor when a foreign branch or subsidiary is unable to observe appropriate AML/CFT measures because this is prohibited by local (*i.e.* host country) laws, regulations or other measures.

921. As the home regulator, OSFI already expects FRFIs with international operations to implement enterprise-wide policies consistent with the Core Principles. One such policy would relate to the implementation of an enterprise-wide AML/CFT Programme, as outlined in its Guideline B-8. As such, OSFI expects the international operations of financial institutions to implement policies and procedures consistent with the domestic financial institutions enterprise-wide standards - regardless of whether the country is an FATF member or not.

922. The one exception to this would be where the AML/CFT standard in a particular jurisdiction is higher than or in addition to the enterprise-wide standard. Under those circumstances OSFI would expect the international operation in the particular jurisdiction, whether the operation is a branch of a domestic financial institution or a separate legal subsidiary, to implement AML/CFT standards that go beyond the enterprise-wide or group standards.

923. Moreover, Guideline B-8 states that FRFIs should ensure that subsidiaries having potential exposure to money laundering or terrorist financing activities follow the guideline.

924. OSFI examinations in financial institutions are performed on all parts of the FRFIs' enterprise-wide operations, including branches and subsidiaries located outside Canada. Deficiencies in any subsidiary or branch of the financial institution have been subject of deficiency letters by OSFI, or can trigger the issuance of a direction of compliance if the deficiency amounts to the commission of an unsafe or unsound practice in conducting the business of the institution. With respect to subsidiaries, OSFI's usual practice is to share any identified material weaknesses with host regulators. Furthermore, OSFI shares the results of its AML/CTF examinations with FINTRAC (except for information

[121] Some provisions in relation to Recommendation 22 have been adopted in the PCMLTFA in December 2006. They will enter into force in June 2008.

pertaining to non-Canadian subsidiaries) who, in turn, has the ability to impose legal sanctions with respect to compliance deficiencies.

925. To date OSFI has undertaken 6 separate reviews of the international operations of Canadian domestic banks to verify that AML/CFT policies and procedures are being implemented on an enterprise-wide basis.

3.8.2 Recommendations and Comments

926. *Recommendation 15.* The current requirements should be expanded, made more explicit and enforceable, in particular:

- Written policies and procedures should be explicitly required, and should be kept up to date, and their minimum mandatory content should include the detection of unusual and suspicious transactions.
- There should be an explicit requirement to ensure that the AML/CFT compliance officer has a timely access to customer identification data and other CDD information, transactions records and other relevant information.
- The requirement for an independent audit function (internal or external) to test on a regular basis the compliance of the AML regime should be strengthened for MSBs and small financial institutions, and made more explicit generally.
- Canada should impose screening procedures when hiring employees for financial institutions.

927. *Recommendation 22*. Canada should ensure that the provisions in relation to Recommendation 22 that will enter into force in June 2008 are in line with the FATF requirements and are properly implemented by all financial institutions.

3.8.3 Compliance with Recommendations 15 & 22

Rec.	Rating	Summary of factors underlying ratings
Rec.15	LC	• The requirement for internal controls does not extend to all financial institutions as defined by the FATF (notably financial leasing, factoring and finance companies). • There is no mandatory explicit requirement to maintain up to date internal procedures, policies and controls and such policies do not include the detection of unusual and suspicious transactions. • There is no explicit requirement to ensure that the AML/CFT compliance officer has a timely access to customer identification data and other CDD information, transactions records and other relevant information. • There is no mandatory requirement for an independent audit function to test AML/CFT regime compliance for small financial institutions (including some MSBs) for which a simple self-assessment is admitted. • There is no general requirement concerning screening procedures when hiring employees.

Rec.	Rating	Summary of factors underlying ratings
Rec.22	NC	• Currently, the PCMLTFA and PCMLTF Regulations contain no explicit provision requiring financial institutions to ensure that their foreign branches and subsidiaries observe AML/CFT measures consistent with home country requirements although foreign branches of Canadian financial institutions are Canadian entities under the Bank Act and the Insurance Companies Act that are subject to Canadian laws. • There is no requirement that particular attention be paid to branches and subsidiaries in countries which do not or insufficiently apply the FATF Recommendations. • There is no legal obligation in the PCMLTFA and PCMLTF Regulations that, where the minimum AML/CFT requirements of the home and host countries differ, branches and subsidiaries in host countries are required to apply the higher standard, to the extent that local (*i.e.* host country) laws and regulations permit. • There is no requirement that financial institutions be required to inform their home country supervisor when a foreign branch or subsidiary is unable to observe appropriate AML/CFT measures because this is prohibited by local (*i.e.* host country) laws, regulations or other measures.

3.9 Shell banks (R.18)

3.9.1 Description and Analysis

Establishment or continued operations of shell banks

928. The Bank Act does not permit the incorporation of a shell bank since all banks operating in Canada must have a physical presence. All banks incorporated in Canada must be listed in Schedule I or Schedule II of the Bank Act and such a listing must always include a reference to the place in Canada where the head office is situated. Section 237 of the Bank Act also provides that a bank incorporated in Canada must have, at all times, a head office within Canada that is specified in either the Bank's incorporating instrument or its by-laws.

Correspondent banking relationships with shell banks

929. Legislative amendments enacted in December 2006 and regulatory amendments that were brought into force on 30 June 2007 specifically address the issue of shell banks in Canada's AML/CFT legislative and regulatory texts. Section 9.4(2) of the PCMLTFA specifically prohibits Canadian financial entities from entering into a business relationship with shell banks. There is no prohibition to continue business relationships with shell banks.

930. Prior to these legislative changes, financial regulators had issued guidance and regulations in this area. OSFI, for example, has been providing guidance to all banks and federally regulated trust and loan companies in the area of correspondent banking since 2002. OSFI Guideline B-8 ''encourages FRFIs to pay special attention to business relationships with shell banks and to adopt measures that will ensure that they do not enter into correspondent banking relationships with shell banks''. The practice was first communicated in guidance sent to banks and trust and loan companies on February 22, 2002 encouraging them to adopt measures to ensure that they do not enter into correspondent banking relationships with shell banks and added to Guideline B-8 when it was subsequently revised. In the securities sector, the IDA has had a regulation in place since 2004 that prohibits member securities dealers from dealing with shell banks, with an exception for affiliates of banks subject to a suitable regulatory regime in their home jurisdiction.

931. It should be noted that as part of its assessment of a bank's correspondent banking business, OSFI verifies that the bank has adopted in writing such controls against dealing with shell banks and that it does not have any correspondent banking relationships with shell banks.

Possible use of respondent financial institutions accounts by shell banks

932. Under the December 2006 PCMLTFA provisions that entered into force on June 30, 2007, there is a compulsory requirement for financial institutions to satisfy themselves that respondent financial institutions in a foreign country do not permit their accounts to be used by shell banks. Section 15 of the PCMLTF Regulations adopted on June 27, 2007 and in force since June 30, 2007 requires every financial entity that enters into a correspondent banking relationship to obtain a statement from the foreign financial institution that it does not have, directly or indirectly, correspondent banking relationships with shell banks.

933. The assessors were advised that when OSFI reviews the files of the correspondent accounts, it expects to see evidence that the bank has conducted enhanced due diligence in managing the money laundering and terrorist financing risks associated with correspondent banking activities. OSFI looks for evidence that the bank has requested information and documentation from the respondent bank that verifies, among other things, that the respondent is a regulated bank, is not a shell bank and does not deal directly or indirectly with shell banks. The assessment team was told that OSFI has never encountered instances where one of its regulated institutions had correspondent relationships with a shell bank.

3.9.2 Recommendations and Comments

934. Canada should adopt a requirement for financial entities to terminate business relationships with shell banks as well as with any foreign financial institution that has, directly or indirectly, correspondent banking relationships with shell banks. Canada should ensure that the measures adopted in relation to shell banks are fully implemented by financial institutions.

3.9.3 Compliance with Recommendation 18

Rec.	Rating	Summary of factors underlying ratings
Rec.18	LC	• Financial entities are not required to terminate business relationships with shell banks, nor with any foreign financial institution that has, directly or indirectly, correspondent banking relationships with shell banks. • The effectiveness of the measures in place cannot yet be assessed.

Regulation, supervision, guidance, monitoring and sanctions

3.10 Supervision and oversight (R. 23, 30, 29, 17, 32, & 25)

3.10.1 Description and Analysis

Authorities/SROs roles and duties & Structure and resources - R.23, 30

General

935. The overall Canadian supervisory regime is complex due to the federal and provincial structure of government. However, AML/CFT compliance is in principle straightforward as FINTRAC is solely responsible. In order to assist it, FINTRAC has signed MOUs with certain regulators or supervisors to share information. In addition to this, some regulators have provisions under their own legislation or codes of conduct that impose similar requirements to, or which complement the key provisions in the PCMLTFA through separate enforcement powers (for example, OSFI advises FRFIs to have proper due diligence procedures; IDA requires securities dealers to properly identify beneficial owners). FINTRAC supervision provides the minimum standard; however, having regard to all the elements, it is not easy to get a complete overview of the supervision of AML/CFT compliance that is being applied in practice to each category of financial institution.

936. It is worth mentioning that the financial sectors which are currently not covered by the PCMLTFA (see Section 3.1 of the report) are generally subject neither to specific regulation nor to prudential supervision concerning AML/CFT issues. For example, for financial leasing, the industry is

represented by the Canadian Leasing and Finance Association (CLFA) which provides information on the industry and input into the policy-making process, but does not provide any regulatory oversight. Membership in the CLFA is voluntary. As stated above, it is only on a voluntary basis that some finance companies have decided to comply with minimum AML/CFT standards and they are not subject to any supervision in that area.

937. The following table generally summarizes the list of existing regulators per reporting entities:

Reporting Entities	Number of reporting Entities	Sector Particularities	Primary Regulator	AML/CFT Regulator
Banks	71	Biggest six hold 90% of assets	OSFI	FINTRAC
Credit unions and *caisses populaires*	1 250	Majority located in Quebec	Provincial authorities (*e.g.* AMF in Quebec)	FINTRAC
Life insurance companies	105 - federal 33 - provincial	Five largest are federally regulated and handle 64% of net premiums	OSFI - 90% of firms Provincial authorities - 10% of firms	FINTRAC
Life insurance brokers and agents	73 000	A significant number work for insurance companies	Provincial authorities (*e.g.* AMF, FSCO)	FINTRAC
Trust and Loan companies	81	Largest are banks' subsidiaries	OSFI and some provinces[1]	FINTRAC
Investment dealers firms[2]	208	Biggest 11 firms hold 71% of revenues. 6 of these are owned by the largest banks	IDA	FINTRAC
Mutual Fund dealers firms[2]	197	Only deal in mutual funds. Many of the largest are owned by the large banks.	MFDA AMF in Quebec	FINTRAC
Investment Counsel and Portfolio Management firms[2]	397	Activities limited to providing investment advice and counselling	Provincial authorities (*e.g.* AMF and OSC)	FINTRAC
Other securities firms[2]	309	Limited trading in securities	Provincial authorities (*e.g.* AMF and OSC)	FINTRAC
Money service businesses	700	A few large firms cover the large majority of the market	None	FINTRAC

Notes:

[1] Ontario only permits the operation of federally regulated trust companies.

[2] Some 90 000 securities participants are licensed/registered to sell securities in these firms and are subject to AML/CFT requirements.

OSFI: Office of the Superintendent of Financial Institutions.

AMF: L'Autorité des marchés financiers du Québec.

OSC: Ontario Securities Commission.

FSCO: Financial Services Commission of Ontario.

IDA: Investment Dealers Association of Canada.

MFDA: Mutual Fund Dealers Association of Canada

938. The basis on which the regulators (excluding FINTRAC) perform AML/CFT compliance supervision varies from one organization to another, as they are not specifically mandated by law to ensure compliance with PCMLTFA/PCMLTF Regulations:

- OSFI, for instance, as the prudential regulator of federal financial institutions is primarily concerned with ensuring safety and soundness which are key elements in its supervisory interventions in the AML/CFT area. If OSFI determines that a FRFI has failed to implement AML/CFT requirements in a manner that amounts to the commission of an unsafe or unsound practice it can apply a full range of supervisory enforcement actions including a "Direction of Compliance". It has adopted AML/CFT guidance (Guideline B-8) to help FRFIs to comply

with the various legal requirements. Failure to comply with B-8 gives rise to recommendations aimed at strengthening risk management controls.

- Under various provincial Acts governing financial institutions, compliance with federal law and regulation is a condition for obtaining and keeping a license. Thus regulators, even if they do not have direct jurisdiction to administer the PCMLTFA, are entitled to verify that the entities they supervise comply with it as they have, in a number of cases, the mandate to ensure compliance with any federal or provincial legislation. But some actually do not look specifically at those aspects in their compliance regime or look at it in a very cursory and limited way: for instance, average time spent by DICO, which is in charge of the supervision of credit unions in Ontario, to the review of AML/CFT compliance (*i.e.* the review of the financial institution report to FINTRAC) is two hours per inspection. Alberta Securities Commission compliance officers look only at the existence of procedures and policies but would not make sample testing to assess their effectiveness. For its part, FSCO, the Ontario provincial regulator for life insurance companies (4 provincially regulated) and agents[122], which has a memorandum of understanding with OSFI for the supervision of the four Ontario life insurance companies does not perform any on-site review for AML/CFT purposes in the other entities it supervises. Another example of limited on-site reviews performed by the provincial regulator is the control exercised by the AMF, the provincial regulator of Quebec of the *caisses populaires* of the Desjardin group, as it relies mainly on the controls performed by the Federation itself on its member entities.

- Other regulators, such as the IDA for investment dealers, have issued code of conducts or mandatory regulations establishing standards comparable to or higher than PCMLTFA and control the compliance of reporting entities with these standards.

939. Thus the role of the different regulators and SROs regarding the control of AML/CFT compliance may differ considerably, and, depending on their different levels (and in some cases absence) of involvement in that area, the different financial sectors are subject to disparate degrees of supervision for AML/CFT purposes.

940. The MSBs sector which comprises 700 identified reporting entities and possibly more than 20 000 branches or agents is only supervised by FINTRAC. FINTRAC has given priority to inspections in this sector after commencing its compliance reviews and has covered about 300 entities during the last four last fiscal years.

941. FINTRAC has entered in agreements with 12 regulators and SROs in the financial sector to exchange AML/CFT supervisory information, the most recent having been signed in February 2007. Information provided by these regulators to FINTRAC feeds into FINTRAC's risk assessment.

942. In general, under the MOUs, the regulators provide FINTRAC with the following information regarding their activities related to the compliance of the entities they regulate with the PCMLTFA: lists of entities that they plan to examine; a copy of their compliance review program; results of compliance reviews undertaken; copies of correspondence regarding deficiencies; descriptions of actions the regulator has required to be taken to correct deficiencies; and descriptions of corrective actions taken by entities.

943. The following table describes FINTRAC's MOU partners in the financial sector, the entities supervised by the regulator, and the process undertaken by the given regulator to carry out AML/CFT inspections.

[122] The definition of agents in the Insurance Act of Ontario is intended to capture all conduct for someone placing business with a life insurance company, whether the person is appointed by an insurance company or he/she is acting on behalf of the consumer.

Region	Regulator	Number of FIs Supervised by the Regulator	Regulator AML/CFT Inspections Methodology
Canada	Office of the Superintendent of Financial Institutions	71 Banks 46 Trust Companies 22 Loan Companies 96 Life Ins. Companies	Detailed exams in all sectors Risk based Examine one-quarter of regulated entities annually
Canada	Investment Dealers Association of Canada	208 securities firms	Risk based. One-third annual coverage.
British Columbia	Financial Institutions Commission of British Columbia (FICOM)	53 Credit Unions 2 Life Ins. Companies, 5 500 agents 7 Trust Companies	Risk & random. No set examination program with exams primarily selected by weaknesses identified in risk management system
Manitoba	Credit Union Deposit Insurance Corporation	58 Credit Unions	Risk based. 25% annual exam coverage
New Brunswick	New Brunswick Office de stabilisation de la Fédération des caisses populaires acadiennes	33 *Caisse Populaires*	Risk & random. All entities examined within 18-month exam cycle
New Brunswick	New Brunswick Department of Justice, Insurance Branch	2 Life Ins. Companies	Random, 3-year exam cycle
Newfoundland	Credit Union Deposit Guarantee Corporation of Newfoundland and Labrador	13 Credit Unions	All entities examined within a 2-year cycle
New Brunswick	New Brunswick Credit Union Federation Stabilization Board	23 Credit Unions	Risk & random. All entities examined within 18-month exam cycle
Nova Scotia	Nova Scotia Credit Union Deposit Insurance Corporation	34 Credit Unions	Risk & random, with each entity examined in 18-month cycle
Ontario	Deposit Insurance Corporation of Ontario	221 Credit Unions & *Caisses populaires*	Risk based, currently being refined. Conduct apprx. 70 exams annually, with 15-20 targeted
Québec	L'Autorité des marchés financiers du Québec	300 securities firms 600 *Caisses populaires* 28 Life Ins. Companies	Risk based
Saskatchewan	Saskatchewan Credit Union Deposit Guarantee Corporation	88 Credit Unions	Risk based, annual exams of each entity

944. FINTRAC provides these regulators with information related to the risk assessment undertaken by FINTRAC, results of FINTRAC's compliance actions and copies of correspondence between FINTRAC and the supervised entities.

945. It is to be noted that FINTRAC does not delegate its supervisory role through MOUs to other regulators. Information obtained by other regulators through their own supervisory activities, including examinations, is provided to FINTRAC under the MOU and is taken into consideration by FINTRAC during its risk assessment process. In addition to the audits and examinations performed by the regulators under their own supervisory framework, the results of which, with respect to AML/CFT relevant issues are provided to FINTRAC, FINTRAC conducts examinations in each sector, whether or not it is covered by an MOU. In fact, FINTRAC has conducted examinations in every sector covered by the PCMLTFA with the exception of financial institutions supervised by OSFI since FINTRAC fully relies on OSFI to conduct AML/CFT compliance initiatives.

946. Sanctions available under the PCMLTFA can only be administered by FINTRAC (see below-Recommendations 17 and 29).

947. In conclusion, beyond the centralized role of FINTRAC, it has been difficult for the assessment team to have a completely reliable overview of the efficiency of the supervision of AML/CFT compliance, except at the federally regulated level.

948. These preliminary remarks and observations will be illustrated and further developed in the following parts of this section, describing some of the main features and participants in the AML/CFT regime. The assessment team has opted for a sample approach whereby the AML/CFT supervision carried out by FINTRAC, OSFI and IDA, being the principal players, will be developed in more depth and detail when compared with the supervisory regimes implemented by SROs or provincial regulators where detailed and comprehensive information is not so readily available.

Overview of the main regulators acting in the AML/CFT area (with the exception of FINTRAC)

OSFI

949. OSFI is the prudential regulator for all banks, federally regulated trust and loan companies, federally regulated insurance companies, cooperative retail associations and cooperative credit associations and is given its responsibilities and authority by the OSFI Act and federal financial institution legislation.

950. FRFIs supervised by OSFI are subject to prudential regulation through legislated authorities and powers provided in the Bank Act, the Trust and Loan Companies Act, the Insurance Companies Act, and the Cooperative Credit Associations Act. The Office of the Superintendent of Financial Institutions Act provides the Superintendent with authority to assess controls designed to ensure that each FRFI is operated in a safe and sound manner and complies with its governing statute.

Securities regulators

951. *General*. The regulation of the securities industry is under provincial and territorial jurisdiction and is carried out through provincial/territorial securities regulatory authorities (SRAs). Self-regulatory organizations (SROs) and market infrastructure entities, such as exchanges and clearing agencies, supplement direct regulation by the SRAs in Canada's ten provinces and three territories. All SROs and market infrastructure entities set and enforce requirements that restrict access to the securities markets; however, some are for-profit organizations, others are not, and some have competitors while others are monopolies. The Canadian securities regulatory regime relies on these organizations and entities to help protect investors and promote fair, efficient and competitive capital markets. They develop standards of practice and business conduct, monitor their members' or participants' compliance with these standards and take appropriate enforcement actions against those who violate these requirements.

952. The current regulatory regime provides for parallel regulation of members and participants of these organizations and entities. For instance, SRAs make general rules for dealers, while SROs make rules that are consistent but may be more restrictive on the same subject matter; therefore, both SRAs and SROs may take enforcement actions against members. Some provinces and territories have delegated certain powers under their securities legislation to the SROs, such as registration and compliance[123].

953. Since there are different types of SROs and market infrastructure entities with varying functions and purposes, the nature and degree of the reliance of securities regulators on them may vary. For example, they rely heavily on certain SROs, such as the Bourse de Montréal Inc. (Bourse)[124], the

[123] The Alberta Securities Commission, the British Columbia Securities Commission and the Ontario Securities Commission have delegated certain registration functions to the Investment Dealers Association of Canada. The Autorité des marchés financiers (Québec) delegated registration and inspection functions and powers to the Investment Dealers Association of Canada.

[124] The Bourse is an exchange and also a recognized SRO in Quebec.

Investment Dealers Association of Canada (IDA), the Mutual Fund Dealers Association of Canada (MFDA) and Market Regulation Services Inc. (RS) to perform front-line regulatory functions.

954. The principle of reliance on SROs is well entrenched in Canadian securities legislation, for example, through explicit authorisation for the SRAs to recognize SROs[125]. In order to ensure the on-going reliance is appropriate, SRAs conduct regular oversight of SROs to evaluate their effectiveness, to confirm that they are acting in the public interest and to ensure that any conflicts of interest between the public and their members/users and any conflicts among members/users are properly managed. Legislation in many jurisdictions outlines this responsibility when regulators rely on SROs[126].

955. *IDA.* The IDA is a provincially recognized SRO in all provinces[127]. Recognition is done through an order of the SRA in the Province, generally subject to conditions set forth in or with the order. The IDA is the front-line regulator of investment dealers and a number of provisions in provincial securities regulations recognize IDA rules as an alternative to provincial regulations, generally by explicitly granting or allowing the granting of exemptions from the provincial rules to members who abide by IDA rules.

956. *MFDA.* The MFDA, established in June 1998, is the national SRO for the distribution side of the Canadian mutual fund industry. The MFDA regulates the operations, standards of practice and business conduct of its members and their representatives with a mandate to enhance investor protection and strengthen public confidence in the Canadian mutual fund industry. In general, the MFDA has a similar regulatory regime as the IDA, which includes rules and detailed requirements MFDA members must comply with, including particulars respecting business structures, capital requirements, insurance, books and records, client reporting, and business conduct. Subject to limited exceptions (for example, for firms for whom the mutual fund business is incidental to their primary business of advising), in British Columbia, Alberta, Saskatchewan, Manitoba, Ontario, New Brunswick and Nova Scotia, a mutual fund dealer must be a member of the MFDA[128].

957. *OSC.* The following provides examples where SRAs regulate registrants directly. These examples pertain specifically to the case of securities regulation in the largest province, Ontario, by the Ontario Securities Commission (OSC).

958. Investment Counsel/Portfolio Managers (IC/PMs). This is the largest category of registrants reviewed directly by the OSC. IC/PMs have discretionary investment authority over client funds. The OSC considers them to be low risk for AML/CFT purposes since most advisers do not have access to client funds, trades are executed through an IDA member and assets are held by a custodian. As a result, the OSC only reviews policies and procedures relating to compliance with money laundering legislation and does only limited substantive testing such as the client identification procedures as part of its know-your-client testing procedures. To the extent that the policies and procedures are deficient,

---

125 For example, section 2.1 of the *Securities Act* (Ontario) states, in part, that "In pursuing the purposes of this Act, the Commission shall have regard to the following fundamental principles: ... 4. The Commission should, subject to an appropriate system of supervision, use the enforcement capability and regulatory expertise of recognized self-regulatory organizations". Section 21.1 of the Securities Act (Ontario) sets out the statutory authority to recognize SROs.

126 For example, section 2.1 of the Securities Act (Ontario) sets out the principle of "an appropriate system of supervision." Subsection 21.1(4) provides that "the Commission may, if it is satisfied that to do so would be in the public interest, make any decision with respect to any by-law, rule, regulation, policy, procedure, interpretation or practice of a recognized self-regulatory organization." Subsection 21.7(1) allows the Ontario Securities Commission to hear appeals from "a direction, decision, ruling or order" made by a recognized SRO.

127 With the exception of Prince Edward Island which has no authority in its Securities Act to recognize a SRO and there is a pending recognition application with New Brunswick.

128 While the MFDA is not formally recognized as an SRO by the *Autorité des marchés financiers* (AMF), it has entered into a co-operative agreement with the AMF and actively participates in the regulation of mutual fund dealers in Québec.

the OSC issues a deficiency notice as part of its field review deficiency report and provides a copy of the deficiency notice to FINTRAC periodically.

959. Scholarship Plan Dealers (SPDs). SPDs are relatively low risk for AML/CFT purposes because they deal with relatively small amounts of money from a large numbers of investors. Given the nature of the scholarship plans, the risk of money laundering was considered low. Money is locked in for a number of years. Although the money can eventually be withdrawn, only the amount net of enrolment fees would be returned.

960. Limited Market Dealers (LMDs). In Ontario, there are approximately 550 LMDs engaged in the business of selling "exempt" securities to accredited investors. The majority of LMDs do not receive money from clients. Client cheques are payable directly to the issuer of a security. In January 2006, 78 of those LMDs were registered both as mutual fund dealers and LMDs and therefore were subject to on-site compliance reviews by MFDA. LMDs are subject to on-site compliance reviews of OSC.

Credit Unions regulators

961. All credit unions and *caisses populaires* are provincially incorporated and almost exclusively regulated at the provincial level. The legislative and regulatory framework for credit unions and *caisses populaires* generally run parallel to that of federal financial institutions, such as banks. In addition, the provinces provide deposit insurance for members of credit unions or *caisses populaires*.

962. *Regulation in Ontario.* The Financial Services Commission of Ontario (FSCO), an arm's-length agency of the Department of Finance, regulates registration of credit unions and *caisses populaires* under the Credit Unions and *Caisses Populaires* Act, 1994. The Deposit Insurance Corporation of Ontario (DICO) has signed a Letter of Understanding (LOU) with the FSCO. DICO is responsible for conducting onsite verifications and reviews and copies of all on-site examinations reports are shared with FSCO.

963. *Regulation in Quebec*. The Autorité des marchés financiers (AMF), the integrated supervisor in Quebec, regulates *caisses populaires*, securities firms and insurance companies and agents, regulates *caisses populaires* under an Act respecting financial services cooperatives. Under this Act, the Desjardins federation, the joint supervisor of the *caisses populaires* with the AMF, must inspect the internal affairs of each *caisse populaire*, including that AML/CFT requirements are being followed, at least once every 18 months and must transmit to the AMF its findings.

Insurance regulators

964. Canadian insurance companies can be either federally or provincially incorporated. Branches of foreign insurance companies are regulated at the federal level only. Federally incorporated regulated life insurance companies dominate Canada's life and health sector. At the end of 2005 there were about 107 active life insurance companies operating in Canada and out of these, some 80 (which includes 30 foreign branches) were federally regulated, generating almost 92% of total life and health premium income. In addition the 3 largest federally regulated insurance companies and their life insurance subsidiaries account for 81% of the life and health sector's assets.

965. OSFI also prudentially supervises provincially chartered life companies regulated by three provinces; Manitoba, Ontario and New Brunswick under MOUs with those provinces. In 2005 these MOU's together cover 6 provincial companies. The remaining active provincial life insurers were incorporated in Quebec (17), British Columbia (2) and Alberta (1).

966. *Provincial Regulation*. In Ontario, FSCO licenses and regulates insurers that sell life and health insurance in the province of Ontario to ensure they comply with the provincial market conduct legislation. Life and health insurance products are sold to consumers directly by companies or through insurance agents. In Québec, the Autorité des marchés financiers supervises life insurers while the Chambre de la sécurité financière oversees insurance agents.

Recommendation 30 (Structure and resources of the supervisory authorities)

967. Due to the number of existing supervisors and regulators liable to intervene in the area of AML/CFT, a complete overview of their resources and efficiency would be quite complex, so for the purpose of this report, only the principal authorities, namely, FINTRAC, OSFI and IDA will be assessed in more detail.

968. With regard to the level of resources made available to the different supervisory authorities, there are contrasting situations. Generally, FINTRAC, as the primary regulator specifically empowered with ensuring compliance with PCMLTFA has resources that are too limited to ensure proper supervision in the AML/CFT area. It has to rely on other primary regulators in a number of cases (securities dealers, FRFIs, credit unions, etc.) who themselves do not always have sufficient resources to dedicate to the task.

969. Professional standards applicable to the staff of the main regulators and supervisors are quite comprehensive. The quality and frequency of training for combating ML and TF are also satisfactory as far as FINTRAC, OSFI and IDA are concerned. Again, the assessors believe that training of FINTRAC staff is essential to carry out properly its supervisory responsibility in a very diverse range of businesses.

FINTRAC

970. *Resources*. In its budget of May 2006, the Government of Canada announced its priority to bolster existing capacity to combat money laundering and terrorist financing by providing incremental resources to FINTRAC in the amount of CAD 16.2 million and 102 employees. FINTRAC has a total of 233 employees (as of September 30, 2006) and a current budget of almost CAD 51 million.

971. Although the total headcount may seem adequate, the deployment of staff between the different FINTRAC departments appears to be unbalanced, with the bulk being dedicated to IT management (FINTRAC was created as an FIU that would rely heavily on technology) and comparatively fewer human resources assigned to AML/CFT inspections, especially if compared with the vast number of entities that are subject to supervision.

972. Within FINTRAC, Regional Operations and Compliance (ROC), is responsible for the development, implementation and monitoring of the national compliance program. This includes interpreting policy and regulations, providing advice and assistance to reporting entities; conducting risk assessment and examinations; monitoring data quality, timing and volume; providing feedback to reporting entities; making disclosures of non-compliance to law enforcement; conducting regional liaison with disclosure recipients (*i.e.* law enforcement agencies); and developing and implementing new programs.

973. ROC is comprised of the Compliance and Program Development Units in Ottawa and three regional offices with responsibilities for compliance and for liaison with law enforcement. The Western regional office in Vancouver covers British Columbia, Alberta, Saskatchewan, and the Yukon. The Central regional office in Toronto covers Manitoba, the Northwest Territories, Nunavut, and Ontario. The Eastern regional office in Montreal covers Quebec, New Brunswick, Nova Scotia, Prince Edward Island and Newfoundland & Labrador.

974. ROC has a budget, for the fiscal year of 2006-07, of approximately CAD 5 million. ROC in Ottawa, which includes the Compliance and Program Development Units, as well as the Assistant Director's Office, has a total of more than 20 staff members. The three regional offices have approximately 10 staff members each.

975. With approximately 50 people dedicated to compliance, FINTRAC manages to perform about 150 examinations in financial institutions annually which has to be compared with an estimated

number of reporting financial entities exceeding 150,000 (not taking into account DNFBPs). However, it should be noted that the examinations are targeted at firms and in most cases, a single FINTRAC examination of a parent entity will cover a number of reporting entities, as the parent entity may cover hundreds of individual entities (for example, in a corporate entity securities dealers or an MSB). Therefore, FINTRAC exams cover significantly more than 150 reporting entities in a year, but there are no statistics on the exact number of entities effectively assessed.

976. Moreover, in order to optimize the allocation of its supervisory resources, FINTRAC has adopted a risk-based approach, based on the risk profiles both of the sector and the individual entities, which are regularly updated through the collection of information from a large range of various sources. Reporting entities are mainly selected for examination on the basis of the scores resulting from this approach, while 10% of the examined entities are selected randomly. The assessment team believes that FINTRAC has developed a sophisticated risk-based model that certainly helps FINTRAC to prioritise its supervisory functions.

977. From a technical resource perspective, ROC makes use of the FINTRAC Risk Assessment Tool (FRAT), database software that was developed in-house. This tool helps to ensure that Compliance Officers have access to accurate and up-to-date information, as well as ensuring the timely maintenance of reporting entity information and risk assessment information. This is an important element in meeting information management needs and helping to manage effectively FINTRAC's national compliance program. In addition, FINTRAC Compliance Officers are equipped with various types of technological hardware.

978. However, the FRAT does not cover all reporting entities, as it is mainly focused at the firm level: it covers about 26 000 entities. Moreover, under the risk-based approach, lots of entities included in the FRAT would never have an examination by FINTRAC, even if a limited number of examinations are selected randomly each year. In these conditions, it is the opinion of the assessment team that, unless FINTRAC can rely to a greater degree on primary regulators and SROs in the future, its current organisation and resources dedicated to supervision do not allow it to perform its compliance function in a totally effective way.

979. It is to be noted that ROC is currently expanding as the result of new legislative initiatives that were introduced by the Government of Canada in late 2006.

980. *Professional standards*. ROC is comprised of a diverse group of people with relevant experiences and skills from both the public and private sectors such as the financial industry, accounting, law enforcement, customs, revenue, and public safety. In general, Compliance Officers possess a university degree in such disciplines as the social sciences, accounting, commerce and administration. In addition, many FINTRAC employees are affiliated with professional associations such as Chartered Accountants and Certified Fraud Examiners.

981. ROC team members must conform to the enhanced security measures that FINTRAC has implemented. Like all other FINTRAC employees, compliance officers must obtain 'Top Secret' security clearance as a condition of employment.

982. Further to this, ROC team members receive Compliance Officer Authorisation Training, which assists in preparing the Compliance Officer for conducting examinations in the field, including on how to comport themselves in this kind of environment. A number of policies and procedures have also been developed to guide Compliance Officers, including one on the Professional Expectations for Compliance Officers which comprises fair treatment, courtesy and consideration, privacy and confidentiality, bilingual service, information.

983. Moreover, the following provisions apply to all FINTRAC compliance officers, who are the public face of FINTRAC :

- *Integrity*: perform their work with honesty, diligence, and responsibility; observe the law and make disclosures expected by the law and the PCMLTFA; not knowingly be a party to any illegal activity, or engage in acts that are discreditable to the organization; and respect and contribute to the legitimate and ethical objectives of the organization.
- *Objectivity:* not participate in any activity or relationship that impairs or will be seen as impairing their unbiased assessment; not accept anything that may impair or be presumed to impair their professional judgment; and disclose all material facts known to them that, if not disclosed, may distort the reporting of activities under examination.
- *Confidentiality:* be prudent in the use and protection of information acquired in the course of their duties; and not use information for any personal gain or in any manner that would be contrary to the law.
- *Competency:* engage only in those services for which they have the necessary knowledge, skills, and experience; perform compliance examinations in accordance with FINTRAC policies and procedures; and continually improve their proficiency and the effectiveness and quality of their services. Compliance Officers are required to pass a written course examination in order to become an authorised compliance officer. Compliance officers also then undergo an annual review to maintain their authorisation.

984. FINTRAC Compliance Officers are expected to apply and uphold these principles and rules in addition to the FINTRAC Code of Conduct and Ethics for all employees, available on FINTRAC's Intranet. This is consistent with the Code of Values and Ethics for the Public Service of Canada which came into effect in September 2003. In addition, there are severe penalties in place for any unlawful disclosure made by a FINTRAC employee.

985. *Training.* FINTRAC's Compliance Officers receive rigorous training. New team members receive Orientation training shortly after their arrival. This training focuses on the following: FINTRAC's Legal Framework; the Canadian AML/CFT Regime; International Efforts and Cooperation; Regional Operations and Compliance; Macro Analysis and Integration; Tactical Financial Intelligence (Analytical and Disclosure Process; Production Orders; Sanitized Cases); Macro Analysis and Integration (Strategic intelligence; Operational Statistics; Research and Analysis).

986. In addition, FINTRAC Compliance Officers also receive Compliance Officer Authorisation Training, a nine day comprehensive course that covers numerous areas relating to risk assessment and compliance examinations with cases study.

987. Following the successful completion of the training, all Compliance Officers are authorised in writing by FINTRAC's Director, which then permits them to perform examinations of reporting entities.

988. FINTRAC's Regional Operations and Compliance Section also holds training sessions twice yearly. These are usually a week long and address various subject matters relevant to the work undertaken by Compliance Officers. Team members also attend various AML/CFT conferences and a number are members of the Association of Certified Anti-Money Laundering Specialists (ACAMS).

OSFI

989. *Resources*. OSFI is the sole supervisor of banks and other federally incorporated financial institutions. The OSFI Act provides that the Minister of Finance is responsible for OSFI. It also provides that the Superintendent is solely responsible for exercising the authorities under the financial legislation and is required to report to the Minister of Finance from time to time on the administration of the financial institutions legislation. The Superintendent is given operational independence through an appointment for a fixed term of seven years.

990. The OSFI Act authorises the Superintendent to act independently in order to meet staffing and other resource requirements to fulfil the supervisory obligations. The Superintendent is authorised to

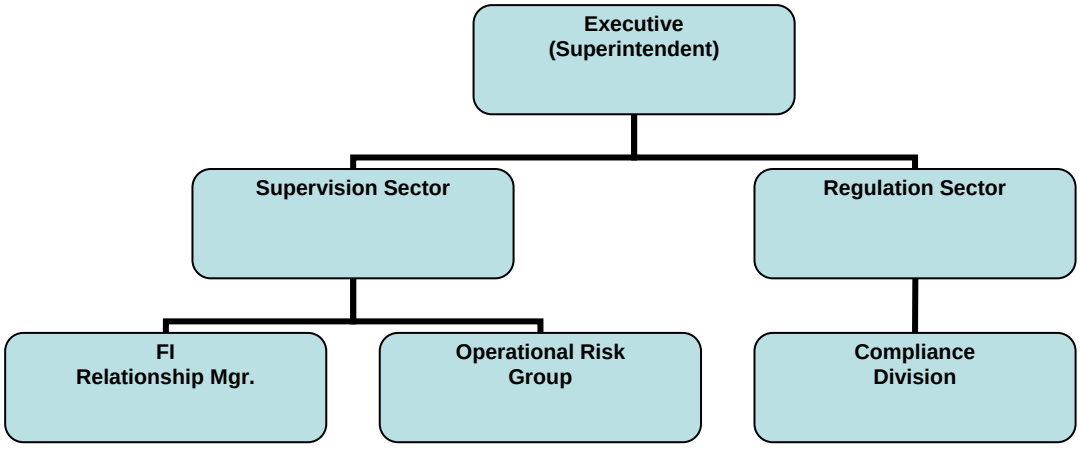
exercise the powers and perform the duties and functions of Treasury Board under the Financial Administration Act that relate to personnel management, including the determination of terms and conditions of employment and the responsibility for employer/employee relations.

991. OSFI's revenue attributable to the regulation and supervision of FRFIs is raised through asset-based, premium-based or membership-based assessments on the financial services industry, and a user pay program for selected services. In the fiscal year ended March 31, 2007, this revenue amounted to CAD 69.7 million. Assessments are allocated to industry sectors based on the approximate amount of time spent on supervising and regulating the industry. Costs are then assessed to individual FRFIs in each sector based on a formula, with a minimum or base level assessment for the smallest FRFIs. The assessments are required by law to be paid and there is no appeal on assessments allocated to FRFIs. Thus, OSFI's program of supervision and regulation of FRFIs is not funded by the government. This affords OSFI a further measure of operational independence from government.

992. OSFI has a staff complement of about 450 and is organized primarily into three sectors:

- The Regulation Sector (123 personnel) is primarily concerned with rule-making, administering registrations and approvals, compliance, and the supervision of pension plans.
- The Supervision Sector (162 personnel) is responsible for supervising and monitoring federally regulated financial institutions.
- The Corporate Services Sector (115 personnel) is responsible for administrative, human resources, systems and technical services.

993. The Compliance Division, which is a part of the Regulation Sector, is responsible for leading AML/CFT assessments of financial institutions in conjunction with the Supervision Sector. The following diagram illustrates the placement of the AML/CFT unit within the OSFI organizational structure:



994. In 2001 two factors contributed to OSFI's decision to allocate more resources to AML/CFT as well as introduce a specific AML/CFT assessment program: the passage of the legislation creating FINTRAC and the introduction of mandatory transaction reporting, and the events of September 11, 2001 with the implementation shortly thereafter of the requirement of financial institutions to search for listed terrorist and terrorist entities and to freeze their assets, with mandatory monthly reporting of frozen assets to regulators.

995. In September 2002, OSFI designated two fulltime employees from OSFI's Compliance Division to commence an AML/CFT assessment program. By 2006, the resources allocated to AML/CFT had grown to 10 employees, of which 8 perform on-site assessments. In addition to this, three employees were redeployed internally from the Supervision Sector in 2006 to support AML/CFT assessments of Canadian conglomerate banks.

996. This increase in staff allowed OSFI to extend its program of examinations into smaller institutions for the first time in 2005. With the current staffing level, it manages to perform 10 to 30 examinations per year, eventually covering a higher number of individual entities when subsidiaries are also concerned (40 entities covered in 2006 for a total number of missions of 13). Excluding from the 215 FRFIs subject to the PCMLTFA those that are otherwise part of conglomerate groups already included or which bear no inherent AML/CFT risk (*e.g.* reinsurers, restricted foreign branches), OSFI is supervising 135 reporting entities. OSFI has instituted a target frequency of about 3 years for institutions presenting higher inherent risk. This includes all conglomerate banks and most conglomerate life insurance companies, and is generally consistent with OSFI's regular prudential examination cycle. Smaller entities will be risk ranked using various ML/TF risk criteria unrelated to financial risk (capital, earnings, liquidity, etc.). Smaller entities that present medium to high inherent risk (due to their business profile matched against the AML/CFT criteria) will also be cycled through an assessment approximately every 3 years. The small, low- to no-risk entities will be the subject of regular monitoring with on site work taking place at longer intervals.

997. *Professional standards*. OSFI's minimum qualification for employment includes a degree from a recognized university or college in a relevant field and/or being a member in good standing in a professional organization. All OSFI employees are subject to a Code of Professional Conduct, and are also subject to an annual review to ensure compliance. The Code requires that OSFI staff act in a professional manner in undertaking their responsibilities. Among other things, the Code requires staff to treat all information obtained in the course of their work as confidential. This refers particularly to any information regarding the affairs of a financial institution and of persons dealing with them. Unauthorised disclosure of any information or use of information for personal reasons by OSFI staff is prohibited in accordance with section 22 of the Office of the Superintendent of Financial Institutions Act, the Privacy Act and employees' oaths of office and secrecy.

998. The Code also contains a Conflict of Interest Code to which staff must adhere. The Conflict of Interest Code minimizes the possibility of conflicts arising between an OSFI employee's private interests and the employee's public service duties and provides for the resolution of unavoidable conflicts in a timely fashion. Failure to comply with the Code of Professional Conduct or the Conflict of Interest Code can lead to appropriate disciplinary measures including termination of employment.

999. All new OSFI staff must pass an enhanced reliability check. At a minimum this involves a background check by law enforcement (RCMP), a credit check and a check of the employee's references to determine the employee's suitability. In situations where the employee will deal with information classified beyond the normal confidentiality level, the check will also include a more extensive review that is conducted by security intelligence officials.

1000. Finally, as part of the employment contract, OSFI employees are required to take an oath of allegiance to Her Majesty in Right of Canada, and each employee's performance is assessed annually to ensure that work is completed in a satisfactory manner.

1001. Taken together, all these controls ensure that OSFI employees are competent in undertaking their responsibilities, subject to high professional and ethical standards and treat information that they deal with during the course of their duties in a confidential manner.

1002. *Training.* All OSFI supervisory staff receive compulsory training on OSFI's Supervisory Framework. Most OSFI staff involved in AML/ CFT assessments were originally general supervisors before transferring to the Compliance Division.

1003. The staff in Compliance Division receive both formal and on-the-job training related to money laundering and terrorist financing. All staff assigned to AML/CFT assessments are experienced examiners and many have extensive industry experience.

1004. To date, six OSFI staff members (four of which are in the Compliance Division) have attended training at the Office of the Comptroller of the Currency (OCC) AML School in Washington, DC. In addition nine Compliance employees are members of the Association of Certified Money-Laundering Specialists (ACAMS) and three of these employees have qualified as Certified Anti-Money Laundering Specialists. OSFI employees have attended financial crime and AML/CFT conferences in Canada, the United States and Europe. In addition senior Compliance Division staff have made numerous presentations on the subject of AML/CFT at industry conferences in Canada and elsewhere.

IDA

1005. *Resources.* The Investment Dealers Association of Canada has four offices across Canada: Montreal, Calgary, Vancouver and its head office located in Toronto. Its 280 employees fulfill its mission of protecting investors and enhancing the efficiency and competitiveness of the Canadian capital markets. It has attracted a group of highly skilled professionals with collective experience in all facets of the securities industry, as well as expertise in various fields including law and accounting.

1006. The IDA Sales Compliance Department has an authorised staff complement of 48. The Enforcement Department has 83. It manages to review all reporting entities at least every five years, but the most important firms may be reviewed yearly.

1007. *Professional standards*. The IDA has a set of values that shapes the way its employees and members carry out their responsibilities and work with each other and the industry. The IDA maintains integrity by conducting itself in an honest and ethical manner and ensures a high degree of professionalism. It is dedicated to carrying out its duties in a timely and reliable fashion. It is accountable through a transparent process with open communication with stakeholders.

1008. The IDA also has a Code of Business Conduct, a Privacy Policy and a Whistleblower policy and process.

1009. *Training.* The IDA's training program for new Sales Compliance Officers includes AML training. The IDA Enforcement Department also organise seminars the AML/CFT topic.

MFDA

1010. *Resources.* The Mutual Fund Dealers Association of Canada has three offices across Canada: Calgary, Vancouver and its head office located in Toronto. Its 155 employees fulfill its vision of raising the standard of firm, fair and transparent regulation in Canada for the protection of investors through commitment to collaboration, staffing excellence and regulatory best practices. MFDA staff is comprised of highly skilled professionals with expertise in various fields including the securities industry, securities regulation, law and auditing and accounting.

1011. The MFDA Compliance Department is comprised of 52 compliance staff, the majority of which or members of a professional association. The Enforcement Department has 45 staff. The MFDA reviews all Members at least once every three years but may perform more frequent examinations if necessary.

1012. *Professional standards and training*. The MFDA has established policies and procedures for the conduct of its activities. These standards are continually reviewed and assessed annually by the MFDA and subject to oversight by the Canadian Securities Administrators. The MFDA had devoted significant resources to staff training and has conducted AML seminars for staff including sessions with FINTRAC.

1013. The MFDA also has a Code of Business Conduct, a Privacy Policy and a Whistleblower policy and process.

Other regulators

1014. During the on-site visit, several regulators asserted that they could not perform on-site reviews or in-depth AML assessments as they are not mandated to do so and lack resources. In particular, resources within the AMF, DICO and the MFDA are limited to deal with AML/CFT issues especially in carrying out supervisory visits and examinations.

Authorities' powers and sanctions (Recommendations 29 & 17)

Recommendation 29

FINTRAC

1015. FINTRAC has responsibility for ensuring compliance with the PCMLTFA. The PCMLTFA includes certain key provisions that assist FINTRAC in meeting its responsibility.

1016. FINTRAC has the right to enter any premises (other than a dwelling-house), to access any document, computer system or data and to reproduce any document under Sections 62(1) and 62(2) of the PCMLTFA, and records that are required to be kept by the reporting entity under the regulations must be retained in such a way that they are accessible to an authorised person (including a FINTRAC Compliance Officer, Section 70). However, this provision authorises a possible period up to 30 days to deliver the information, which seems somewhat excessive (see comments in Section 3.5 of the report). If consent is not granted by the reporting entity for a compliance officer to enter a dwelling, FINTRAC must obtain a warrant to allow a compliance officer to do so although to date this has not been necessary. Reporting entities located in dwelling houses represent a small percentage of the total number of reporting entities. To date, whenever consent has been requested by FINTRAC, it has been granted.

1017. In most circumstances, a FINTRAC compliance officer will contact the reporting entity to be examined a minimum of 30 days before an examination is to commence to allow adequate time for the reporting entity to prepare the requested records for examination. FINTRAC, however, still maintains the authority to conduct on-site compliance examination activities, with no advance notice to the reporting entity.

1018. Subsections 65(2) and 65(3) of the PCMLTFA also provide FINTRAC with an important tool to ensure effective supervision of financial institutions which enables it to exchange compliance information with federal and provincial agencies that regulate entities and individuals with obligations under the PCMLTFA. Subsection 65(10) allows FINTRAC to exchange information with foreign regulators regarding the compliance of reporting entities.

1019. In addition, Section 63.1 of the PCMLTFA provides FINTRAC with the authority to require reporting entities to provide any information that FINTRAC needs for compliance purposes. Reporting entities are therefore obliged to complete and return compliance questionnaires sent by FINTRAC.

1020. Finally, FINTRAC currently has no powers to sanction non compliant institutions and the only action it can take is to transmit the file to law enforcement for investigation related to the criminal sanctions provided by the PCMLTFA (see comments below)[129].

OSFI

1021. OSFI has no mandate under PCMLTFA to ensure compliance of FRFIs with the PCMLTFA. Its mandate, under the Office of the Superintendent of Financial Institutions Act is to supervise financial

[129] Part 4.1 of the PCMLTFA, Notices of Violation, Compliance Agreements and Penalties, provides for an administrative and monetary penalties regime for FINTRAC with reporting entities that do not comply with their AML/CFT obligations. The regulations implementing this regime were enacted in December 2007 and will come into force in December 2008.

institutions in order to determine whether they are in sound financial condition and are complying with their governing statute law and supervisory requirements under that law as well as to promote the adoption by management and boards of directors of financial institutions of policies and procedures designed to control and manage risk. OSFI also has specific powers of supervision under the governing statutes of all federal financial institutions.

1022. More specifically, Subsection 6(1) of the OSFI Act indicates the Superintendent's powers and duties in relation to the *Bank Act*, the *Trust and Loan Companies Act*, the *Cooperative Credit Associations Act* and the *Insurance Companies Act.* The supervisory powers of the Superintendent are uniform under these Acts. The Bank Ac (Articles 643 and 644), for instance, illustrates the Superintendent's power as follows: "*the Superintendent, from time to time, but at least once in each calendar year, shall make or cause to be made any examination and inquiry into the business and affairs of each bank that the Superintendent considers to be necessary or expedient to determine whether the bank is complying with the provisions of this Act and whether the bank is in a sound financial condition and, after the conclusion of each examination and inquiry, shall report on it to the Minister. (2) The Superintendent or a person acting under the Superintendent's direction (a) has a right of access to any records, cash, assets and security held by a bank; and (b) may require the directors, officers and the auditor or auditors of a bank to provide information and explanations, to the extent that they are reasonably able to do so, in respect of the condition and affairs of the bank or any entity in which the bank has a substantial investment. The Superintendent has all the powers of a person appointed as a commissioner under Part II of the Inquiries Act for the purpose of obtaining evidence under oath, and may delegate those powers to any person acting under the Superintendent's direction."*

1023. The indirect involvement of OSFI in ensuring AML/CFT compliance tends to place a limit on its powers. It is only insofar as incidences of AML non compliance can be considered as an unsafe or unsound practice in conducting the business of the bank, that the Superintendent may take enforcement actions and direct the bank or person to cease or refrain from pursuing the course of conduct or to perform such acts as in the opinion of the Superintendent are necessary to remedy the situation. Unlike FINTRAC, it cannot make a direct disclosure of non compliance with PCMLTFTA to law enforcement authorities.

1024. The assessment team was told that OSFI has never been denied access to any information or documentation it requests to conduct an AML/CFT assessment.

Securities regulators including IDA

1025. The SRAs are not mandated by PCMLTFA to ensure compliance of reporting entities with the AML legislative requirements. Nevertheless, they may also rely on the principle of "safe and sound business practice" and on the fact that compliance with the law and regulations is part of the fit and proper criteria that a financial entity must meet to be granted and to maintain registration or a license. In general, the investigation and enforcement powers of the SRAs are comprehensive but specific powers may vary among the provinces and territories. Generally, the SRAs have the power to compel testimony and evidence as well as large powers of sanction. There is also authority in some jurisdictions for the SRA to recover investigation and hearing costs.

1026. The IDA is given the authority to ensure compliance by financial institutions through the individual SRAs. For example, in the case of Ontario, section 21.1 of Ontario's Securities Act recognizes the IDA as a self-regulatory organization, and sets conditions that the IDA must meet. For example (this list is not exhaustive), the IDA shall enforce compliance by its members to IDA rules, provide prompt report and notification of any misconduct by its members to the SRA, advise the public and media of any disciplinary settlement hearing, provide monthly notifications to the SRA of all new investigations, operational reviews and similar matters.

1027. As the national self-regulatory organization of the Canadian securities industry, it has enforcement rules and regulations of member firms and their registered employees, including non-compliance with obligations that are similar to those of the PCMLTFA. These conditions can be found in the IDA By-Laws. The IDA reports all compliance deficiencies to FINTRAC and has on occasion provided extra notice of egregious cases.

1028. Concerning AML issues, the IDA may be considered to have more direct enforcement powers than some other regulators since it has its own set of enforceable by-laws, which sometimes go beyond FINTRAC's requirements and have been used previously to sanction some of its members.

Recommendation 17

FINTRAC

1029. Canada has designated FINTRAC as the authority responsible for determining if a violation has occurred and when appropriate for forwarding that information to law enforcement for investigation. The PCMLTFA outlines the sanctions that can be imposed on reporting entities if they fail to comply with their AML/CFT obligations. In addition, FINTRAC uses warning letters (deficiency letters) and can order action plans to enforce compliance.

1030. Under the current version of the PCMLTFA and its Regulations, FINTRAC itself has very limited powers of enforcement against reporting entities and their directors or senior management for failure to comply with or properly implement AML/CFT requirements. FINTRAC cannot impose penalties but only has the option of referring cases to law enforcement for investigation. The PCMLTFA provides for a series of criminal sanctions for contraventions of various provisions of the Act. This can lead to criminal penalties of up to CAD 2 million in fines and five years in prison for non-compliance.

1031. Until the recent amendments brought to the PCMLTFA enacted in December 2006, these sanctions were applicable in a limited range of cases, namely for the violations of: (1) the record keeping duties, (2) the duty to answer and comply with the request of an officer in the reporting of currency and monetary instruments during cross border movements; (3) the limitations related to disclosure and use of information; (4) the duty to assist and provide information to FINTRAC; (5) the obligation of retention of documents as it applies to legal counsel who claims privilege, as well as (6) the reporting obligations (STRs, TPRs and prescribed transactions). For instance, failure to implement a compliance program was not subject to sanctions under the law. The recent amendments have expanded the regime of criminal sanctions to the violations of most of the law and regulations provisions.

1032. Sanctions are applicable to any officer, director, or agent of the person or entity who directed, assented to, acquiesced in, or participated in its commission, as described in Section 78 of the PCMLTFA.

1033. Most of the sanctions provided by Sections 74 to 77 of the PCMLTFA are punishable (a) on summary conviction to a fine of not more than CAD 50 000 or to imprisonment for a term of not more than six months, or both, or (b) on conviction on indictment, to a fine of not more than CAD 500 000 or to imprisonment for a term of not more than five years, or both. Knowingly contravening to the obligation of reporting suspicious transactions or transactions suspected of being related to terrorist financing is an offence punishable (a) on summary conviction, (i) for a first offence, to a fine of not more than CAD 500 000 or to imprisonment for a term of not more than one year, or both, or (ii) for a subsequent offence, to a fine of not more than CAD 1 000 000 or to imprisonment for a term of not more than one year, or both, or (b) on conviction on indictment, to a fine of not more than CAD 2 000 000 or to imprisonment for a term of not more than five years, or both. Contraventions to the reporting of prescribed financial transactions are punishable (a) on summary conviction to a fine of not more than CAD 500 000 for a first offence and of not more than CAD 1 000 000 for each subsequent offence.

1034. Finally every person or entity that contravenes Section 8 is (a) guilty of an offence punishable on summary conviction, or (b) guilty of an indictable offence and liable to imprisonment for a term of not more than two years.

1035. In nearly 4 years, FINTRAC has disclosed 7 such cases of egregious non-compliance by reporting entities including financial institutions, to law enforcement agencies. In the event a disclosure is made, the responsibility falls to law enforcement to investigate and, where appropriate, pursue criminal sanctions for non-compliance. Disclosures have so far resulted in only one conviction for non-compliance with the PCMLTFA. The person convicted was also convicted for money laundering.

Non-Compliance Disclosures					
	2003/04	**2004/05**	**2005/06**	**2006/07***	**Total**
Number of disclosures	0	2	3	2	7

*As of end of the second quarter.

1036. In the absence of other powers of sanction and, especially, of administrative and monetary penalties, FINTRAC has favoured a "cooperative approach" to compliance, based on the principle "trust but verify" and deals with less severe non compliance issues by issuing deficiency letters, which require the reporting entity to respond with an action plan.

1037. In the majority of cases where FINTRAC has identified deficiencies in a reporting entity's compliance with the PCMLTFA, the entity takes corrective action based on a letter from FINTRAC that outlines these deficiencies.

1038. Once the detailed examination findings have been communicated to the reporting entity identifying the need for corrective action ("deficiency letter"), the reporting entity is required to submit a corrective action plan to FINTRAC. The action plan, which must be submitted in writing, must include timelines for correcting the identified deficiencies. If an action plan is received that does not adequately address the deficiencies identified during the examination, the FINTRAC Compliance Officer contacts the reporting entity compliance officer, both verbally and in writing, to request that they provide a new action plan in order to rectify the deficiencies in a timely manner. The written correspondence is sent to the senior executive of the reporting entity, with a copy to the reporting entity's compliance officer. The letter clearly outlines that the reporting entity is in non-compliance with its legislative obligations under the PCMLTFA.

1039. Should a reporting entity submit a further inadequate action plan, the reporting entity is clearly informed of the shortcomings and is required to re-submit an acceptable plan. The action taken by the reporting entity may influence FINTRAC's decision to refer to the non-compliance disclosure to law enforcement. The compliance officer then follows up with the reporting entity to ensure that the action plan is being undertaken in a timely manner and that deficiencies are being corrected appropriately.

1040. Where a reporting entity makes no demonstrable effort to address deficiencies identified by FINTRAC, FINTRAC can disclose such a case of non-compliance to law enforcement for investigation and prosecution.

1041. The current regime of sanctions administered by FINTRAC is clearly insufficient as it does not allow FINTRAC to apply a graduated and proportionate range of sanctions and limits the possibilities of imposing prompt corrective actions in cases where criminal sanctions would not apply. Thus, it cannot be considered as effective, proportionate and dissuasive[130].

[130] In order to enhance the effectiveness of the system and provide greater flexibility and authority for FINTRAC in ensuring compliance with the PCMLTFA and its regulations, it was decided to create an administrative and monetary penalties regime. Such a measure has been incorporated in the December 2007

OSFI

1042. The federal financial institutions' governing legislation gives OSFI the power to oversee financial institutions' AML/CFT risk management controls. OSFI has the power under the Office of the Superintendent of Financial Institutions Act to impose sanctions when the nature of the non-compliance is determined to be an unsafe and unsound practice.

1043. OSFI has a range of supervisory tools and sanctions at its disposal, including written interventions, staging (which involves higher CDIC – Canada Deposit Insurance Corporation – premiums), directions of compliance, placing terms and conditions in the FRFI's Order To Commence And Carry On Business (operating licence) and imposing an Administrative Monetary Penalties (AMP) under the OSFI Act. Section 25 of the OSFI Act sets out a range of administrative monetary penalties that OSFI can use. However, these AMPs, which were introduced in 2005, only apply in case of a contravention of a provision of a financial institutions Act or in case of non-compliance with any order or Direction of Compliance, any terms and conditions imposed, any undertaking given or any prudential agreement entered into under a provision of a financial institutions Act. Thus, they cannot be administered directly in cases of non-compliance with the PCMLTFA or its regulations which do not amount to unsafe or unsound practice, which would have justified such an intervention in any event. Stronger sanctions include the ability to go to court to obtain an order to stop the unsafe or unsound practice, or in extreme cases OSFI can remove a director from the board or senior officer for his or her position. These supervisory tools or sanctions are further detailed in the following paragraphs.

1044. OSFI issues Supervisory letters after each AML/CFT assessment. The letters contain "required actions" on compliance issues or "recommendations" as follows:

- "Required action" speaks to a deficiency that relates to non-compliance with a specific provision of the PCMLTFA. Failures to comply with Guideline B-8 are met with a "requirement for action" when it also involves a breach of the PCMLTFA or in some cases, when OSFI feels it necessary to deliver a strong signal to the financial institution.

- "Recommended action" speaks to a deficiency in risk management controls or other supervisory requirement not directly related to a legal requirement. Failures to comply with Guideline B-8 provisions that are not requirements under the PCMLTFA are in principle subject to recommended actions (for instance when a financial institution fails to have measures in place in relation to PEPs for which legal requirements are not in force yet).

1045. OSFI can also impose a more intrusive supervisory schedule on institutions, called Staging, which consists of raising the stage rating of a FRFI (normal stage, for no problem institutions being 0, the other stages ranging from 1 "early warning" to 4 "not viable/insolvency imminent"). Elevation from stage 0 to stage 1 results in more intense oversight by OSFI. It also results in a higher OSFI assessment fee and in an increase in their deposit insurance premiums charged by the Canada Deposit Insurance Corporation. Further increases in stage ratings attract additional deposit insurance premiums.

1046. If OSFI determines that directors or senior management of a FRFI have, or are about to, fail to comply with or properly implement AML/CFT requirements in a manner that amounts to the commission of an unsafe or unsound practice in conducting the business of the FRFI, or that would constitute a course of conduct that is an unsafe or unsound practice in conducting the business of the FRFI, the Superintendent has authority to issue unilateral instructions called Directions of Compliance under the FRFI's governing statute. For example subsection 645(1) of the Bank Act provides as follows: "*(1) where, in the opinion of the Superintendent, a bank, or a person with respect to a bank,*

---

amendments to the PCMLTFA that were enacted on 14 December 2006 and in a new set of regulations, the PCMLTF Administrative Monetary Penalties Regulation, enacted on 26 December 2007. These provisions will come into force in December 2008.

is committing, or is about to commit, an act that is an unsafe or unsound practice in conducting the business of the bank, or is pursuing or is about to pursue any course of conduct that is an unsafe or unsound practice in conducting the business of the bank, the Superintendent may direct the bank or person to (a) cease or refrain from committing the act or pursuing the course of conduct; and (b) perform such acts as in the opinion of the Superintendent are necessary to remedy the situation."

1047. The failure of a FRFI to comply with a Direction of Compliance is an offence under the financial institution's governing statute and is sanctionable under the OSFI Act.

1048. The Superintendent of OSFI also has the power to enter into a Prudential Agreement with a FRFI. For example section 644.1 of the Bank Act provides as follows: "*the Superintendent may enter into an agreement, called a "prudential agreement", with a bank for the purposes of implementing any measure designed to maintain or improve its safety and soundness."*

1049. In extreme cases, OSFI can remove directors or officers from office and take control of a financial institution. In addition, OSFI can require external auditors to extend the scope of their audit and request that the board of directors meet with the Superintendent.

1050. In summary, these measures constitute a progressively more intrusive array of supervisory measures that can be utilized to change undesirable behaviour by financial institutions in order to meet ongoing regulatory requirements and expectations.

1051. Concerning AML/CFT issues, the usual way of intervention is via written communication: the 78 assessments between 2002 and the end of the first quarter 2007 resulted in supervisory letters containing 247 required actions on compliance issues with PCMLTFA/PCMLTFR and 381 recommended actions to strengthen risk management controls.

1052. No measure of direction of compliance, terms or conditions imposed or prudential agreement was ever taken on AML/CFT issues. However, in the period 2004 – 2006 inclusive OSFI staged four financial institutions primarily for AML/CFT control deficiencies (one in 2004, 2 more in 2005 and the fourth in 2006). Further, a fifth assessment conducted in 2005 led to the institution, already at Stage 1, remaining there for an extended period of time. These stagings (to stage 1) led to OSFI and/or CDIC surcharges ranging from CAD 45 000 up to CAD 500 000.

1053. In addition, OSFI brings matters related to non-compliance with the PCMLTFA to the attention of FINTRAC immediately following each on-site assessment.

1054. Thus, OSFI has a wider range of possible enforcement actions or sanctions than FINTRAC. Nevertheless, even if these tools exist, sanctions remain rarely used which may be due to the fact that the "sound and safe business practice" principle on which OSFI's intervention is based, imposes a higher threshold than simple non compliance.

1055. It is worth mentioning that, when the proposed PCMLTF Regulations comes into force, the Administrative & Monetary Penalties scheme for non compliance with PCMLTFA will be administered only by FINTRAC and will not be accessible to OSFI or other regulators.

Securities regulators

1056. SRAs have a range of measures they can choose from to rectify circumstances where a market intermediary fails to meet ongoing requirements and protect the public. They include suspending or terminating the intermediary's license, imposing terms and conditions on the intermediary requiring for instance restrictions on the type or amount of business that the intermediary may conduct or the number of salespersons or advisers a firm may hire.

1057. Additionally, the SRAs may order that exemptions contained in the securities laws in the jurisdiction do not apply to the intermediary. This order is often made if an intermediary has been suspended or terminated in order to prevent the intermediary from conducting business based on registration and prospectus exemptions. In Ontario and Quebec, the SRAs also may order a registrant to submit to a review of practices and procedures and institute such changes as recommended by the SRA where the SRA has concerns about the practices and procedures of the intermediary.

1058. In certain other provinces, the SRA can appoint a person to review the business and conduct of a registrant or former registrant to determine whether the registrant is complying, or has complied, with the legislation in the jurisdiction, any decision made under that legislation or any requirement of an exchange or SRO to which the registrant belongs. An SRA also may order that a document be produced by a registrant if the SRA is satisfied that securities laws have not been complied with. Additionally, most SRAs may reprimand a registrant or issue a caution letter when the SRA determines that the behaviour of the registrant merits a reprimand or caution, for example, where the behaviour of the registrant is contrary to the public interest.

1059. Compliance officers and branch managers can be sanctioned for contravening a specific requirement to supervise conduct within the firm. In addition, pursuant to this power, an SRA can make an order against a person or company whose behaviour or inaction contributed to the violation, for example, a director, officer or partner of the registrant or parent company of the registrant, if the SRA concludes that it is in the public interest to do so. Certain SRAs have the authority to impose a financial penalty on a registrant for contraventions of securities laws. These SRAs and the other SRAs also have the authority to apply to the court for such an order, for example, where the court finds that there has been a violation of securities laws.

1060. Similarly, the IDA and MFDA may suspend a member's membership rights and privileges, suspend the approval of an individual and/or impose conditions on the continued membership of a member or approval of an individual if, for example, the member or individual fails to meet ongoing requirements, contravenes Canadian securities laws, or engages in any business conduct or practice that the SRO concludes is unbecoming or contrary to the public interest.

1061. The SROs can also impose sanctions against their members (and registered employees of members) for contraventions of SRO requirements, including AML and supervision requirements.

1062. The IDA and MFDA have the power to impose financial penalties on their members and approved individuals if the SRO determines that, for example, the member or individual fails to meet ongoing requirements, contravenes Canadian securities laws or engages in any business conduct or practice that the SRA concludes is unbecoming or contrary to the public interest.

1063. The IDA can discipline its member firms and their employees using a broad range of sanctions that are proportionate to the severity of the situation. For instance, IDA penalties can include fines, up to a maximum of the greater of CAD 1 million per contravention or an amount equal to three times the profit made or loss avoided by reason of the contravention for registered employees or fines up to a maximum of the greater of CAD 5 million per contravention or an amount equal to three times the profit made or loss avoided by reason of the contravention for member firms. The IDA can also suspend or ban individuals for life from registration as a broker, or suspend and expel firms from membership. The latter has the effect of closing down firms from operating in the securities industry.

1064. The IDA's Enforcement Process is an essential element in assuring investors that the IDA's member firms are effectively regulated and that each adheres to the highest standards of conduct. It is comprised of three stages that ensure that sanctions are proportionate to the severity of the situation. All matters presented to the Association are initially considered during the Complaint Review process. If this initial review indicates that further investigation is warranted, the matter is referred to Investigations staff. If the investigation finds sufficient evidence of a regulatory breach, the matter is subsequently referred to Enforcement Counsel for disciplinary action. The IDA's Enforcement

Counsel reviews the investigation file and, if appropriate, prepares charges, penalty recommendations and a settlement offer for the respondent. If Enforcement Counsel is successful in negotiating a settlement with the respondent, the settlement agreement is put before the Hearing Panel, which may accept or reject the settlement agreement. If a settlement offer is not successfully negotiated between Enforcement Counsel and the respondent, a Notice of Hearing and Particulars is issued and a contested hearing is held. Hearing Panels are comprised of two industry representatives and a member of the public who acts as Chair. The public members are not associated with any investment dealer and have legal training, usually as an experienced securities lawyer or retired judge.

1065. IDA hearings are generally open to the public. Notice is provided to the public in advance of any hearing and the IDA subsequently makes information on its disciplinary decisions public.

1066. In general, it has to be noted that, except for IDA which has effectively applied in a number of cases heavy sanctions to its members for non compliance with AML/CFT standards (for instance, CAD 600 000 fine and revocation of the firms membership along fines and suspensions applied to the firms directors for violation of IDA Regulation 1300.1 (a) which requires each member to use due diligence to learn and remain informed of the essential facts relative to every customer and to every order or account accepted and subsequent violation of the PCMLTFA requirements for verifying client identity), it has emerged from the meetings that the assessment team has had with professionals during its on-site visit, that these powers of sanction have generally not been used by SRAs or SROs in that area, as they have rarely issued specific rules or regulations related to AML/CFT and consider it to be mainly FINTRAC's responsibility.

Other regulators

1067. The other regulators are not entrusted with the responsibility of ensuring compliance with the PCMLTFA but, as already stated, some of them include controls related to AML/CFT requirements in their compliance programs, based on their various statutory powers: their intervention in that area is based either on the "safety and soundness" principle, or on the mandate given to them to ensure compliance with any federal law or regulation or still on codes of conduct or mandatory guidance that they have developed at their level for their regulated entities.

Recommendation 23 – Market entry and ongoing supervision

1068. The number of regulators, both federal and provincial, as well various SROs makes this a complex regulatory system.

1069. Although there is no systematic harmonization of the requirements in terms of market entry among the federal and provincial levels and among the different provinces, the information that the assessment team could obtain shows that the measures aimed at preventing criminals or their associates from holding a significant or controlling interest or holding a management function in a financial institution, as well as the "fit and proper" principle are widespread. However, provinces have variations in their supervisory treatment. For instance, for finance companies, not all provinces have adopted such a requirement in their respective Acts regulating the sector.

1070. Currently, MSBs are supervised by FINTRAC for AML/CFT purposes while not subject to registration or licensing.

1071. The following section will further elaborate on the requirements imposed by the main regulators or in the main sectors but they cannot be considered as exhaustive.

Financial institutions supervised by OSFI

1072. All applications to incorporate or register FRFIs must be approved by the Minister of Finance (who issues the letters patent) and Licences To Commence And Carry On Business must be approved by the Superintendent. Such approvals are required by the federal statutes governing the specific financial institution.

1073. Each application is subject to the proposed financial institution meeting a number of criteria, and submitting detailed information in support of the application.

1074. The suitability and integrity of individuals responsible for the oversight and management are important prudential concerns for OSFI. The integrity and suitability of owners, directors and senior managers are verified upon incorporation or authorisation of a FRFI. The Minister of Finance considers an applicant's character, integrity, business record and experience and the competence and experience of the directors and senior officers. To incorporate a FRFI in Canada, the major direct and indirect (*i.e.* all beneficial) shareholders (detaining above 10 % of the shares), and the directors and senior officers of the applicant, must submit personal information on themselves including place and date of birth, current address, curriculum vitae, etc. This information is used by OSFI to evaluate whether they have the required qualifications and expertise to manage or direct a financial institution's business and affairs. They must also submit a completed OSFI Security Information Form so that the RCMP and CSIS can conduct security assessments. There are similar requirements in respect of the senior officers of foreign financial institutions that make applications to establish branches in Canada.

1075. Whenever there is a change in ownership through the acquisition of significant interest of a federally regulated financial institution, it has to be submitted to the approval of the Minister who will rely on the same type of controls as those performed at the time of the initial incorporation.

1076. However, there is no specific legal obligation in federal financial institutions legislation for FRFIs to implement screening procedures for those who are hired, or appointed to the Board, after the initial incorporation or authorisation procedures are concluded. In May 2007 OSFI issued a draft Guideline E-17: Assessment of Responsible Persons by FREs[131]. The purpose of the Guideline is to ensure that FRFIs implement policies and procedures to ensure that those individuals responsible for the oversight and management of financial institutions (defined in the Guideline as "Responsible Persons") are evaluated, both initially and on a regular basis, with respect to suitability and integrity (*i.e.* Fit and Proper).

Securities dealers

1077. The SRAs and SROs regulate the activities of securities dealers and other intermediaries from both a prudential and market conduct basis, including registering qualified member firms and employees. Participants in this sector must meet stringent capital requirements, demonstrate an ability and willingness to conduct its business in a manner consistent with securities legislation, and SRO rule books and are subject to ongoing supervision.

1078. Canadian securities laws contain various fundamental provisions regarding the licensing of market intermediaries. They set out: (1) the requirements to be registered, (2) exemptions from the registration requirements and (3) certain basic standards and requirements for registrants (for example, the duty to deal fairly, honestly and in good faith with clients), as well as rights of registrants. These fundamental provisions generally are incorporated into securities statutes.

1079. Canadian securities laws also contain more detailed requirements respecting registration. These more detailed requirements generally are incorporated into subordinate instruments such as regulations and rules. These more detailed provisions also may establish additional exemptions from the registration requirements. In addition to the requirements in Canadian securities laws, the IDA and the MFDA rulebooks contain complementary requirements which apply to their members as a matter of contract.

1080. The Canadian Securities Administrators (CSA), the coordinating body of Canadian SRAs, has undertaken a project to modernize the regulation of securities registrants. The CSA's Registration

131 This includes FRFIs.

Reform Project is intended to update, streamline and harmonize the categories of registration and the regulation of securities registrants in Canada, effective July 2008.

1081. There are three important general criteria to the fit and proper standard that applicants for registration must meet to be considered acceptable for registration: (1) proficiency; (2) financial stability; and (3) suitability, a concept that encompasses but is not limited to integrity. The core principles and most of the detailed provisions for registration are set out in Canadian securities laws. If an SRO has been authorised by an SRA to carry out certain registration functions, additional requirements may be set out in the SRO's rules.

1082. To be registered, a securities intermediary must demonstrate: (1) the appropriate financial resources to carry on the proposed business, such as the minimum capital requirements are met; and there are additional capital resources available to meet the continuing demands of the business; (2) adequate operational systems and controls for the businesses it proposes to carry on, such as proper books and records, internal controls, risk management, and supervisory systems; (3) senior management, with the appropriate knowledge, resources, skills and ethical attitude (including a consideration of past conduct) necessary to perform their proposed roles; (4) directors with the appropriate knowledge, resources, skills and ethical attitude (including a consideration of past conduct) necessary to perform their proposed roles; and (5) substantial owners/shareholders with the appropriate resources and ethical attitude (including a consideration of past conduct) necessary to perform their proposed roles.

1083. While Canadian securities laws do not provide detailed minimum criteria of suitability for registration, a general fit and proper requirement applies. Canadian securities laws authorise the SRAs to refuse to register a person or company if the applicant is not suitable for registration or the proposed registration is objectionable. An SRA will examine the applicant's past conduct, including the applicant's criminal record, employment history, history with the SRA and other regulators, civil actions against the applicant making allegations relating to the applicant's integrity and any other information that the SRA believes may reflect upon the applicant's suitability. The IDA and MFDA consider criteria similar to those considered by the SRAs in deciding whether to grant membership status to a firm or to approve an individual.

Provincially supervised insurance companies, agents and brokers

1084. A number of life insurance companies (about 10 %), representing a limited share of the sector in terms of premiums, are provincially registered and regulated. The requirements applying to them could not be examined and assessed in detail but it may be generally assumed that the registration process is subject to a similar scheme to OSFI's one, relying on a complete review of the business case and of the individuals' files. It is worth mentioning that the Canadian Council of Insurance Regulators has engaged a process aiming at harmonizing practices among the different provinces.

1085. Insurance agents are licensed and registered provincially in Canada. For example, FSCO issues licences authorizing persons to conduct business as insurance agents. There are three classes of agent licences: Life Insurance (including accident & sickness), Accident & Sickness, General. Agents listed may hold a combination of the insurance licences listed above. An insurance licence is issued by FSCO for a two-year term. Any person who acts as an insurance agent without being licensed is guilty of an offence under the Insurance Act, and may be prosecuted for such violation.

Licensing or registration of money or value transfer services

1086. The current legislation does not provide for a registration regime for persons or entities that are engaged in the business of money service business or foreign exchange dealing, that is persons and entities engaged in the business of foreign exchange dealing, of remitting funds or transmitting funds by any means or through any person, entity or electronic funds transfer network, or of issuing or redeeming money orders, traveller's cheques or other similar negotiable instruments.

1087. The PCMLTFA currently requires these entities to abide by reporting, client identification, record-keeping and internal compliance requirements. FINTRAC has conducted significant outreach to identify MSBs, including presentations to community groups that use remittance services, searches of telephone records, reviews of ethnic newspapers, and advertising. The objective is to inform MSBs of their obligations and ensure they are included within the compliance program (i.e., Compliance Questionnaires, examinations, etc.).

1088. The sector is diverse, ranging from large multinational firms with many agents, which have developed strict checks before accepting their agents and oversight functions upon them, to individuals "operating in relative obscurity"[132], making the sector highly attractive to money launderers.

1089. In these conditions and in order to comply with FATF recommendations, Canada decided to create a registration regime in force in June 2008[133].

1090. To date, FINTRAC has been able to identify some 700 MSBs and foreign exchange dealers in Canada, largely located in major urban areas.

1091. FINTRAC has focused its examination resources in the MSBs sector with over 50% of all examinations over the last three years covering this sector. This reflects, in part, the risks associated with the MSB sector, as well as the absence of a flow of information from a primary regulator.

Ongoing supervision and monitoring – Recommendation 23

FINTRAC

1092. In order to effectively fulfill its role, FINTRAC has developed a National Compliance Program to ensure that reporting entities are complying with their obligations under the PCMLTFA. FINTRAC's compliance program makes use of risk management strategies to identify those sectors and reporting entities most in need of improving compliance. Efforts are focused on areas where there is the greatest risk of non-compliance and in which the failure to comply could have significant impact on FINTRAC's ability to detect and deter money laundering and terrorist financing.

1093. FINTRAC has developed the FINTRAC Risk Assessment Tool (FRAT) to assist compliance officers in assessing the risk of non-compliance by reporting entities and to centralize compliance information. When assessing the level of risk for reporting entities, FINTRAC looks at a range of factors, including such elements as open source information, reporting volumes, observations gleaned from outreach activities, voluntary information which FINTRAC has received on non-compliance, results from compliance questionnaires completed by reporting entities (see below), other database checks, information received from regulators, quality and quantity assurance reviews, and the results of compliance examinations.

---

[132] See "Enhancing Canada's Anti-Money Laundering and Anti-Terrorist Financing Regime" Consultation Paper, of June 2005.

[133] The PCMLTFA requires that all money service businesses register and creates a criminal penalty for operating an unregistered business. The application of the registration requirement includes informal money remitters commonly known as Hawala and is also applicable to departments and agencies of Her Majesty in Right of Canada, for example, postal orders. Section 11.11 of the PCMLTFA specifies persons or entities that are ineligible for registration, such those that have been previously convicted of a money laundering offence, a terrorist financing offence, an organized crime offence, any other criminal offence under the PCMLTFA and certain serious offences under the Controlled Drugs and Substances Act such as drug trafficking. FINTRAC is designated by the PCMLTFA to function as the Registrar and is responsible for accepting, denying, revoking and verifying applications for registration, maintaining the information contained in the registry and verifying compliance with the registration requirement. Registrants will have to inform FINTRAC of any material changes to their information within 30 days and renewal of registration will have to take place every 2 years or longer if prescribed by regulation

1094. Based on these risk factors, FINTRAC has assigned a general risk level to each reporting entity sector. This guides FINTRAC's overall compliance work (outreach, examinations, etc.) as in general, FINTRAC focuses more of its compliance resources on entities in higher risk sectors. FINTRAC also conducts assessments to rate the relative risk of non-compliance of entities and individuals within each sector. 26 000 entities are currently rated, which represents all big players and firms as well as some individuals.

1095. Compliance Questionnaires (CQs) are also used by FINTRAC to help focus examination resources, primarily for those entities at highest risk for non-compliance. FINTRAC developed the CQ as a tool to support its risk assessment and examination function. CQs are particularly useful as they can assist in assessing compliance levels in a large number of entities using relatively few resources.

1096. While the exact content of a CQ varies by sector, the CQ assists FINTRAC's Compliance team in assessing the risk of non-compliance within a particular entity by asking questions related to the size and scope of the reporting entity's operation, the institution where the entity does its banking (this information allows FINTRAC to cross-reference this entity with any reports that may have been filed by the bank), the entity's business lines, the implementation of a compliance regime, compliance policies and procedures, review of compliance policies and procedures and ongoing compliance training. CQs have proven to be an effective supervisory tool for FINTRAC.

1097. FINTRAC has sent over 3 000 CQs to financial institutions as of March 31, 2006. In 2006-07, FINTRAC is disseminating an additional 4 000 CQs to reporting entities (including DNFBPs) and 1 500 of these will be to the life insurance sector. The average response rate among financial institutions to CQs sent by FINTRAC is 89%: It should increase in the future since responding to these CQs is now mandatory as the amendment to the PCMLTFA, under section 63.1, which came into force in February 2007, requires reporting entities to "provide (…) the documents or other information with respect to the administration of Part 1 that [an] authorized person may reasonably require".

1098. In order to make it easier for reporting entities to respond to a CQ, they are now done electronically. Reporting entities receive a letter informing them that they have been selected to fill out a CQ. They are given a login and password and requested to go to FINTRAC's website to fill out the CQ on-line. In addition to facilitating responses, electronic forms assist FINTRAC Compliance Officers in scoring responses.

1099. Another key element that assists FINTRAC in its assessment of the risks of entities being non-compliant with their AML/CFT obligations is its consultation and coordination with other agencies that have responsibility for regulating entities covered under the PCMLTFA.

1100. The PCMLTFA permits FINTRAC to exchange compliance-related information with regulators at the federal and provincial levels. FINTRAC has signed Memoranda of Understanding to govern these information-sharing relationships (12 to date) with regulators of financial institutions. Under these MOUs, FINTRAC and the regulators on a regular basis exchange statistics, risk assessment information, examination results, and examination plans. FINTRAC also makes presentations and provide training to staff of MOU partners. In 2005-06, FINTRAC staff had 86 meetings with regulators and in 2004-05, 100 meetings of that type took place. The relationship with the regulators is still in its early stages, the first MOU having been signed in mid-2004 and the most recent in February 2007.

1101. As of September 30, 2006, FINTRAC had conducted almost 400 examinations of financial institutions, while its MOU partners had carried out more than 100 further examinations of financial institutions. These figures have to be compared to the total number of financial reporting entities which exceeds 100 000 (this figure includes individuals such as life insurance agents or securities dealers). However, FINTRAC examination may cover a large number of reporting entities (*e.g.* in the case of life insurance companies/agents and securities firms/dealers) and it is difficult to draw

definitive conclusions about supervisory coverage by comparing the reported examinations each year with the total number of reporting entities.

1102. The on-site portion of the examinations conducted by FINTRAC can, in practice, and depending on the size and complexity of the reporting entity, take anywhere from 3-4 hours to more than five days (in the case of a large, national reporting entity) to perform, which is somewhat less than average time spent by OSFI (see below). FINTRAC's examinations include sample testing of customers' transactions and files. The pre-examination stage, which can take weeks of preparation, consists of a review of documentation (including the results of audit reviews by FINTRAC MOU partners, a review of the entity's policies and procedures, etc.) that assists FINTRAC in scoping the on-site portion of the examination.

1103. A FINTRAC compliance examination will determine if the entity is meeting its obligations under the legislation. Areas of review can include:

- *Implementation of a compliance regime*: (1) The FINTRAC compliance officer will determine if a compliance officer has been appointed within the reporting entity and if this person is at the appropriate level and has the appropriate access to senior management; (2) The compliance officer will review the policies and procedures for compliance with the PCMLTFA that the reporting entity has established and assess them to determine if they are appropriate for the scope of the reporting entity's business and obligations under the PCMLTFA; (3) He will assess the entity's policies and procedures to determine their effectiveness. For example, large entities would be expected to have an annual external audit of their policies and procedures; (4) He will assess the on-going compliance training program that the entity has in place for any employees, agents or any other individual authorised to act on behalf of the reporting entity, including a review of such documentation as training materials, schedules, and agendas.
- *Reporting of all required transactions*: the compliance officer, who will have a detailed account of the entity's reporting history, will examine transaction records kept by the reporting entity to determine if a report (suspicious transaction, large cash transaction, electronic funds transfer or terrorist property) should have been filed by the entity.
- *Implementation of client identification requirements*: the compliance officer will examine records to determine if the reporting entity has identified its clients in a manner consistent with the PCMLTFA and regulations
- *Record keeping requirements*: the compliance officer will examine the reporting entity's records to determine if the entity has kept records in accordance with the PCMLTFA and regulations.

1104. So far, FINTRAC has concentrated most of its examination activities in the MSB, real estate, Credit union, *caisses populaires* and securities sectors: 86% of the examinations conducted by FINTRAC took place in these sectors.

1105. With regard to financial institutions, the following table shows the total examinations conducted by FINTRAC in each sector by fiscal year:

FINTRAC Examinations Conducted in Financial Institutions				
Sector	**2004-05**	**2005-06**	**2006-07 (as of end of Q2)**	**Total (by sector)**
Bank	0	1	0	**1**
CU/CP*	8	29	23	**60**
LI**	1	4	3	**8**
Securities	3	29	14	**46**
Trust & Loans	0	1	0	**1**
MSB	164*	56	43	**263***
TOTAL	**176**	**120**	**83**	**379**

**Note*: In fiscal year 2003-04, FINTRAC began to conduct examinations and completed a total of 26 examinations during the latter part of this time period. The focus of these examinations was largely on the MSB sector.

1106. At the end of 2005/06, FINTRAC had identified an average of 2.75 deficiencies, in general evenly spread across all categories: reporting, ascertaining identification, record keeping and compliance regime elements, as a result of its examinations.

OSFI

1107. FRFIs are subject to ongoing supervision by OSFI, based on its Supervisory Framework, a risk-based process to assess the safety and soundness of FRFIs developed in 1997/98, and released in 1999.

1108. The Framework evaluates the risk profiles of FRFIs, their financial condition, risk management processes and legislative compliance. The Framework evaluates inherent risks in the following areas: credit risk; market risk; insurance risk; operational risk; liquidity risk; legal and regulatory risk; and strategic risk. The Framework applies a risk-based supervisory approach to all types and sizes of FRFIs and which is administered on a consolidated basis. FRFIs are informed of OSFI's overall risk assessment, including a consolidated net risk rating. The risk assessment determines the type and extent of prudential supervisory work carried out on financial institutions.

1109. OSFI's AML/CFT methodology is broadly based on the approach taken in the Supervisory Framework. However, inherent risk measurement for AML/CFT purposes is based primarily on the product mix offered by financial institutions, together with the geographical spread of operations. For example, institutions which focus heavily on retail deposits and lending, or which offer correspondent banking services, or where insurance products have large cash values are ranked at higher risk than those that focus primarily on term insurance products or that have little or no deposit taking.

1110. OSFI considers inherent risks associated with money laundering and terrorist financing as a factor of operational risk as well as legal and regulatory risk. Therefore, at the highest level, issues such as weak AML/CFT controls can potentially harm the reputation of FRFIs. Although the Framework does not formally recognize reputation risk as an identified area of risk, OSFI typically treats reputation risk as a composite inherent risk arising from underlying risks, especially operational risk and legal & regulatory risk.

1111. The quality of risk management controls for prudential supervision is viewed from the following perspectives; operational management; financial analysis; compliance; internal audit; risk management; senior management and board oversight. Net risk is defined as inherent risks, mitigated by risk management control functions. Similarly, for AML/CFT purposes, OSFI examines the risk management controls exerted by the Board, senior management, compliance and internal audit when conducting AML/CFT assessments to conclude whether the inherent risks of ML/TF are being managed appropriately. Because this process differs from the analysis of traditional prudential risks to capital and earnings, OSFI has placed AML/CFT assessment into a separate unit (Compliance Division) and not in its Supervision Sector.

1112. OSFI supervises a large number of institutions that deal in a very significant amount of total assets and that offer a broad range of financial sector activities as shown by the following table.

Type of Federally Regulated Financial Institution	No. of federal institutions FRFIs	Total Assets (CAD 000) Q3 2006	%
Six largest Conglomerate Domestic[134] banks and affiliates	9	CAD1 990 039 189	69.4
All other Domestic Banks	13	CAD 37 044 174	1.3
Subsidiaries of Foreign Banks	21	CAD 120 204 087	4.2
Branches of Authorised Foreign Banks	24	CAD 48 262 271	1.7
Trust and Loan Companies	30	CAD 16 852 035	0.6
Trust and Loan Companies subsidiaries of	20	CAD 212 553 043	7.4

[134]. "Domestic " means the entity was incorporated in Canada by Letters Patent under the appropriate governing legislation and is not a subsidiary of a foreign bank.

Type of Federally Regulated Financial Institution	No. of federal institutions FRFIs	Total Assets (CAD 000) Q3 2006	%
Canadian banks			
Cooperative Credit Associations [1]	7	CAD 11 889 712	0.4
Cooperative Retail Associations	1	CAD 3 236 524	0.1
Three largest Conglomerate Domestic Life Insurance Companies and their affiliates	9	CAD 365 692 000	12.8
All other domestic Life Insurance Companies	30	CAD 45 506 966	1.6
Branches of Authorised Foreign Life Insurance Companies	41	CAD 16 291 088	0.5
Total	215	CAD 2 866 584 842	100

[1] 4th quarter 2005.

1113. Since 2002, OSFI has conducted on-site assessments to assess FRFIs AML/CFT programs. These assessments assess both the quality of AML/CFT risk management at such institutions, including their subsidiaries and branches both within and outside Canada, as well as their ability to comply with their obligations under the PCMLTFA and Regulations. The results of these assessments are shared regularly with FINTRAC. Quarterly meetings are also held with FINTRAC to, among other things, review these results.

1114. OSFI's current AML/CFT methodology was developed in 2002 and subsequently refined to reflect its experience in assessing financial institutions. OSFI has instituted a target frequency of about 3 years for institutions presenting higher inherent risk. This includes all conglomerate banks and most conglomerate life insurance companies, and is generally consistent with OSFI's regular prudential examination cycle. Smaller entities will be risk ranked using various ML/TF risk criteria unrelated to financial risk (capital, earnings, liquidity, etc). Smaller entities that present medium to high inherent risk (due to their business profile matched against the AML/CFT criteria) will also be cycled through an assessment approximately every 3 years. The small, low- to no-risk entities will be the subject of regular monitoring with on site work taking place at longer intervals.

1115. On-site assessments typically involve:

- Iinterviews with senior management of risk control functions (AML, Internal Audit, and Risk Management) and selected lines of business.
- Review of systems technology used to support transaction reporting to FINTRAC, including business rules and lines of accountability.
- review of account opening procedures and sample customer files in business lines selected for their exposure to ML and TF.
- Exit meeting to verbally communicate principal findings and recommendations in advance of the written supervisory letter.

1116. Moreover, OSFI also administers a program to support implementation of, and ensure compliance with, section 83 of the Criminal Code, section 7 of the PCMLTFA, FINTRAC Guideline 5, the Regulations Implementing the United Nations Resolutions on the Suppression of Terrorism (RIUNRST), United Nations Al-Qaida and Taliban Regulations (UNAQTR), the United Nations Democratic People's Republic of Korea Regulations and the regulations to implement the United Nations Security Council Resolution 1737 on Iran. Under this program OSFI includes in its AML/CFT assessment methodology a review of the policies and procedures in place at FRFIs to assure compliance with their obligations to search for terrorist and terrorist entities and freeze their assets and report thereon to the RCMP, CSIS and OSFI. OSFI has emphasised to all federal financial institutions that the terrorist name searches must be done on a regular basis to comply with the "continuous" search requirement in the UN regulations and the Criminal Code regulations. Generally, deposit taking institutions and large conglomerate life insurance companies are expected to perform a full search for listed persons' names at least weekly, with larger institutions, including the five largest conglomerate banks, scrubbing customer name databases as frequently as daily.

1117. The examination of a conglomerate bank takes on average 2 to 3 weeks of preparation and 3 weeks of on-site work involving a team of about six persons. On-site work comprises a review of AML/CFT policies and procedures and reports generated by or for risk management control functions, interviews with senior management of risk control functions and selected lines of business, review of system technology used to support transaction reporting to FINTRAC and review of account opening procedures and sample customer files in business lines selected for their exposure to ML and TF.

1118. OSFI supervises financial institutions on a consolidated basis. It regularly reviews the operations of conglomerate banking and insurance companies with significant operations outside Canada, and the AML/CFT assessment program is included in this approach. Since the inception of the AML/CFT assessment program OSFI has reviewed selected financial institutions' offshore operations to test the effectiveness of their enterprise-wide AML/CFT standards. From 2002 to date OSFI has conducted reviews, of varying scope, in subsidiary and/or branches of FRFIs located in the UK, Jamaica, Mexico, Cayman Islands, Jersey, and Guernsey.

1119. In recent assessments of conglomerate financial institutions with securities subsidiaries, and as part of its consolidated supervision responsibilities, OSFI has also tested the effectiveness of these standards in securities dealer subsidiaries of a number of banks. Such securities dealers are regulated by the IDA.

1120. OSFI conducted 73 AML/CFT assessments from November 2002 to December 2006, including 6 follow-up assessments on institutions identified as having significant weaknesses in AML/CFT controls. OSFI has also conducted 5 projects consisting of thematic work associated with cross-sector activity, or assessments of selected Canadian Bank subsidiary operations located outside Canada. In 2006, OSFI upgraded the quality of its assessment work and focused primarily on more labour intensive second generation AML/CFT assessments at Canada's 6 largest banks. These banks had previously been assessed in either 2003 or 2004. Although the total number of assessments conducted by OSFI in 2006 (13) was lower than in 2005 as a result, each assessment was far more significant in scope. Five of the 13 assessments conducted by OSFI in 2006 therefore covered a grand total of 40 FRFIs (comprising 12 banks, 5 life insurance companies and 23 trust and loan companies).

1121. In summary, the 2006 AML/CFT assessment program covered a total of 40 FRFIs, which in turn comprised 87% of the assets of all federally regulated deposit-taking institutions and about 75% of the assets of all FRFIs, gave both FINTRAC and OSFI quite a thorough view of the state of AML/CFT compliance and risk management controls in the federally regulated sector in Canada.

1122. In 2004, OSFI entered into a Memorandum of Understanding with FINTRAC under which OSFI and FINTRAC agreed to share information related to federal financial institutions' compliance with Part 1 of the PCMLTFA. The MOU was authorised under the Public Safety Act, which removed previous restrictions in the PCMLTFA on the ability of FINTRAC to share such information with financial regulators. It also removed similar restrictions under the Office of the Superintendent of Financial Institutions Act, which had prevented OSFI from sharing compliance information with FINTRAC. As a result of the MOU, the PCMLTFA and its Regulations, when combined with FINTRAC Guidelines and OSFI Guideline B-8 represent the primary instruments for reviewing the implementation of AML/CFT requirements in the federally regulated financial sector in Canada. FINTRAC now receives each examination findings letter sent to a FRFI and discusses each in detail at regularly scheduled quarterly meetings with OSFI, unless more urgent discussions are required. FINTRAC also sees all of the action plans.

1123. The following table summarizes the number of OSFI on-site AML/CFT assessments and projects from 2002 to 2006:

Type of actions	2002	2003	2004	2005	2006	Total
Assessments undertaken	5	12	11	29	10	67
Follow-up Assessments	0	0	1	2	3	6
Sub Total	**5**	**12**	**12**	**31**	**13**	**73**
Thematic Projects	0	0	2	2	1	5
Total Assessments and Projects	**5**	**12**	**14**	**33**	**14**	**78**
Required Actions	5	29	31	128	29	222
Recommended Actions	21	66	49	185	62	383
Total Actions	**26**	**95**	**80**	**313**	**91**	**605**

1. The following table summarizes the reasons for intervention that OSFI has made at FRFIs.

Subject	Required Action	Recommended Action	Total
AML/CFT Policy Development & Implementation	17	69	86
Self-Assessment Program Implementation	14	57	71
Independent Procedures Testing & Reporting	11	47	58
Role of the CAMLO	6	43	49
Total Oversight Recommendations	**48**	**216**	**264**
Training	16	26	42
Large cash transactions, Suspicious transactions and Electronic fund transfers	7	43	50
Customer Identification Issues	69	65	134
Other Business Line Specific Issues	26	18	44
Retention of records	2	2	4
Outsourcing	1	3	4
Terrorist Searching and Freezing	55	8	63
Total Operational Recommendations	**176**	**165**	**341**
Grand Total	**224**	**381**	**605**

1124. In 2005 OSFI improved the scope of AML/CFT assessments by including more detailed assessments of the various lines of businesses at the conglomerate banks (including lines believed to have a higher vulnerability to ML/TF) and a consistent focus on customer record keeping. The conglomerate reviews post-2005 are referred to as "second generation assessments".

IDA

1125. The IDA's Sales Compliance Department ensures that member firms implement policies and procedures to comply with all non-financial regulatory requirements, including those of the IDA, provincial securities acts and federal legislation including the PCMLTFA. The IDA's Sales Compliance staff conducts regular reviews and on-site examinations of member firms, focusing on issues of compliance, anti-money laundering due diligence, supervision, corporate finance and research, employee activities and internal controls; 70% of staff time is spent directly on member firm reviews.

1126. The Sales Compliance Risk Assessment Model helps identify, define, assess and weigh risks in respect to IDA member business activities and behaviour patterns to assist in determining the frequency, scope and principal focus of the individual Sales Compliance Reviews to be conducted for each firm. The objective of the Risk Assessment Model is to identify member firms having a higher than average probability of being found to be non-compliant. To achieve this, the Association runs both qualitative and quantitative evaluations for every dealer and combines their respective outcomes into a single Net Residual Risk score. With this information, the IDA ensures that its regulatory focus is placed on higher risk firms. These objectives are enhanced by the model's ability to indicate the comparable risk assessed for each member firm relative to all other firms under the jurisdiction of the IDA – and to subsets, or "peer groups," of firms engaged in comparable activities.

1127. Providing best practice guidance and rule interpretations is also part of Sales Compliance's work, as well as providing feedback on policy development to the Regulatory Policy Department.

1128. The IDA uses its sales compliance risk assessment model to assist in assigning firms to examination cycles. The cycles are: annual for high risk firms; every 18 months for large, integrated firms; 2 years for low risk firms; a five-year cycle is assigned to minimal risk firms, such as dealers of Alternative Trading Systems (which provide facilities through which other dealers and large institutions trade) and proprietary-trading only firms that have no clients and therefore do not present any risk to IDA rules.

1129. In other respects, the Enforcement Department of the IDA may undertake investigations into the conduct, business or affairs of its members and their employees. Investigations can also be undertaken on the basis of: a complaint received from a member of the public; a directive from the IDA's Board of Directors; a request from an SRA; or any information obtained or received by the IDA.

1130. The Investigator reviews the findings of the investigation and makes a recommendation as to whether there appears to be sustainable evidence that a breach of the Association's By-laws, Regulations or Policies has occurred. Files with insufficient evidence are closed and files with sufficient evidence are sent to the Association's Enforcement Counsel for prosecution.

1131. The IDA provides AML/CFT findings to FINTRAC under an MOU, and had previously provided such information voluntarily. The IDA provides FINTRAC with its review schedule, periodic compendia of deficiency findings involving AML/CFT issues and the remedial action taken by firms. The IDA also provides information to FINTRAC to assist it in the risk assessments it uses to determine what reporting entities it will audit.

1132. From 2001 to 2005 the IDA conducted 526 head office and 100 branch office reviews. Some separate reviews of large branches were also conducted, however, the IDA generally conducts branch reviews in conjunction with a head office reviews to understand how compliance controls are operating at all levels.

MFDA

1133. The activities of the MFDA's Enforcement Department are integral in providing firm, fair and transparent regulatory processes in enforcing the MFDA requirements that enhance investor protection. The activities of the Enforcement Department also directly support the MFDA's goal of participating in the Canadian securities regulatory framework, by developing and maintaining collaborative working relationships with other securities regulatory authorities and law enforcement agencies. The MFDA's Enforcement Department investigates when MFDA member firms and their registered persons breach its rules.

1134. The Enforcement Department receives referrals of the results of sales compliance examinations done by the MFDA Compliance Department, where the nature or extent of the examination results exceeds a threshold that the MFDA has established to identify areas where Enforcement action is required in addition to resolution through normal Compliance follow-up process. The MFDA has committed by letter to FINTRAC that it will report any such referrals that identify situations of non-compliance with AML detected during MFDA Sales Compliance examinations. To date, there have been no findings of conduct exceeding the threshold that would require reporting to FINTRAC under this arrangement.

OSC

1135. The OSC, in its reviews of registrant firms, assesses firms according to an internally developed risk management tool to help focus its resources on the relatively higher risk firms. A regular field review includes a review of the operations of the firm including, for example, detailed testing of portfolio management functions, trading functions, conflicts of interest, financial condition, money laundering, etc. Know your client and suitability reviews are done as part of testing of the portfolio management and trading functions. The review of money laundering is limited to ensuring there are policies and procedures in place to comply with money laundering legislation, and testing of client

identification procedures as part of know your client and suitability reviews. The OSC does not publicly disclose its review cycles.

DICO

1136. DICO conducts inspections of its members' compliance with AML/CFT legislation during its regularly scheduled on-site verifications and reviews. DICO inspects all member institutions on a regular basis with frequency determined by size, complexity and risk. At a minimum, each institution is reviewed at least once every three years. Inspections of the money laundering policy and anti-terrorism aspect of the inspection module is rather marginal and the controls in that area remain limited to a rapid examination of procedures and policies (2 hours on average), without sample testing of transactions or files but can take a longer timeframe should major deficiencies were noted. A copy of the report is also provided to FINTRAC.

1137. During the course of the review, should it come to the attention of the inspector that the member has failed to comply with the requirements of the Money Laundering Legislation review, DICO requires the member to provide an Action Plan to address the identified issue. The Action Plan is also provided to FINTRAC for their agreement. DICO will follow to ensure the Action Plan is implemented as set out.

AMF

1138. Under the AML Act, the Desjardins federation, the joint supervisor of the *caisses populaires* with the AMF, must inspect the internal affairs of each *caisse populaire*, including that AML/CFT requirements are being followed, at least once every 18 months and must transmit to the AMF its findings. AMF relies mainly on these reports and performs seldom on-site reviews at Desjardins *caisses populaires*, favouring a "second level" control on this sector.

FSCO

1139. FSCO licenses and regulates insurers that sell life and health insurance in the province of Ontario to ensure they comply with the provincial market conduct legislation. In Ontario, life and health insurance products are sold to consumers directly by companies or through insurance agents. All agents (as defined in the Insurance Act of Ontario) are required to be licensed with FSCO.

1140. FSCO monitors, investigates and takes appropriate regulatory action when there is non-compliance with legislation and regulations that relate to the regulated sectors. Non-compliance may result in enforcement action.

Comments from the assessment team in relation to Recommendations 29 & 17

1141. The previous developments illustrate the unequal degrees of regulation and supervision, depending on the sectors and provinces although OSFI is responsible for regulating well over 80% of the financial sector, by total assets.

1142. The number of examinations performed by FINTRAC appears to be small compared with the total number of reporting financial entities (more than 100, 000) although FINTRAC examination may cover a large number of reporting entities (*e.g.* in the case of life insurance companies/agents and securities firms/dealers). Even including examinations conducted by FINTRAC's MOU partners, which except for OSFI's are not always as detailed as FINTRAC's (see in this respect DICO's assessments which are generally made in 2 hours), the figures remain rather low, except for the banking and federally regulated trust and loan companies sectors which have a good supervisory coverage by OSFI.

1143. The securities sector seems to be regularly controlled, though on a lesser extent, as non IDA or MFDA members are regulated by provincial SRAs which do generally review policies and procedures but do not perform a thorough testing of AML controls in their on-site reviews.

1144. The on-site AML/CFT assessments conducted by OSFI since 2003 at the major life insurance companies have represented 90% of the industry measured by its assets but less than 10% of the supervised population. The supervision appears to be weak for life insurance agents as AML/CFT controls relies mainly upon FINTRAC's actions. In addition, despite the focus put on that sector, FINTRAC had managed to perform controls on only 60 credit unions and *caisses populaires* up to mid-2007, out of a total population of 1 250 reporting entities.

1145. It should also be noted that except for the main sectors like FRFIs, FINTRAC does not take into account the quality of the supervision by the primary regulators in its risk assessment tool, and the assessment tool is focussed significantly on the risk of non-compliance with the legislative and other requirements, as compared to the risk of money laundering and terrorist financing.

Statistics

1146. Canada provided statistics regarding the on-site examinations conducted by FINTRAC and its MOU partners relating to or including AML/CFT during the last three fiscal years. On the other hand, there was no statistics centrally available concerning the involvement of supervisors which have not signed an MOU with FINTRAC in AML/CFT compliance oversight (number of on-site reviews, sanctions taken). Such information would certainly be useful to help FINTRAC implement an effective risk-based compliance supervision program.

Guidelines – R.25 (Guidance for financial institutions other than on STRs)

FINTRAC

1147. FINTRAC provides Guidelines on its website for reporting entities and the general. Cumulatively, these Guidelines provide reporting entities with an understanding of all of their requirements and obligations under the PCMLTFA. Furthermore, these Guidelines all include a section on how to contact FINTRAC for more information if it is required.

1148. Aside from the Guidelines themselves, FINTRAC's website also contains information tailored specifically to the needs of the various reporting sectors. The information on the website for each of the sectors covers what needs to be reported, record keeping, ascertaining identification, third-party determination, and information on the compliance regime requirements and compliance questionnaires. For each reporting sector, the information can be found on FINTRAC's website.

1149. In addition, FINTRAC launched, in March 2005, an additional type of guidance in its FINTRAC Interpretation Notices (FINs), which are documents developed by FINTRAC to provide explanations and clarifications regarding certain provisions contained in the PCMLTFA and its Regulations. FINs are primarily used by FINTRAC staff, reporting entities and their legal counsel, and other individuals who have an interest in having clear interpretations of some key aspects of the PCMLTFA. To date, four FINs, have been developed, dealing with specific topics concerning money services businesses/foreign exchange dealers, accountants, securities dealers and banks. The following FINs are available on FINTRAC's website: (1) Criteria for determining if an entity is "Engaged in the Business of Money Services Business or Foreign Exchange Dealer" (Annex B10); (2) Accountants - Giving Instructions Versus Providing Advice (Annex B11); (3) Opening an Account for a Person or Entity Engaged in the Business of Dealing in Securities Only Outside of Canada (Annex B12); and (4) Large Cash Transaction and Electronic Funds Transfer Reporting Requirements: Two or More Transactions in a 24-Hour Period (The '24-Hour Rule') (Annex B13).

1150. FINTRAC is currently in the process of updating the guidelines and FINs to take into account amendments to the PCMLTFA and regulations.

1151. FINTRAC also undertakes an extensive outreach and assistance program for reporting entities that includes information sessions, presentations at industry conferences (in 2004-05 and 2005-06, FINTRAC participated in nearly 1 300 presentations involving more than 27,000 participants), articles

in trade magazines, and has developed and published sector-specific information sheets and pamphlets for distribution to reporting entities. FINTRAC provides these publications to reporting entities free of charge, and they are also available on FINTRAC's website. In addition, FINTRAC operates a call centre that is open 12 hours a day from Monday to Friday, to answer general inquiries about FINTRAC's operations, as well as more specific questions about reporting requirements and systems. In 2005-2006, FINTRAC received 3,253 inquiries through the call centre, mostly from reporting entities.

1152. In general, FINTRAC guidance is aimed at explaining and detailing the obligations that different sectors have under the PCMLTFA and its regulations. The Guidelines are supplemented by significant outreach activity undertaken by FINTRAC through regular meetings and presentations at conferences and meetings of industry associations. However, they give few indications on how tailoring them and putting them effectively into practice in the various financial sectors. Further guidance to assist their respective financial institutions in complying with AML/CFT requirements that may be detailed in various statutes may be provided by prudential regulators but it is not yet generalised (see life insurance sector, for example).

OSFI

1153. In early 1990, in support of the initiatives resulting from the 1989 G-7 Paris Summit, OSFI implemented for adoption by federal deposit-taking institutions, a Best Practices Paper to Deter and Detect Money Laundering. The key best practices contained in the paper focused on the following areas: (1) designating an officer within the financial institution to be responsible for compliance with the procedures; (2) implementing a system of formal internal controls procedures to deter and detect money laundering that included a source of funds declaration; (3) implementing a system of independent procedures testing; (4) implementing a record retention policy; (5) developing and providing appropriate training to financial institution staff on AML.

1154. In 1996, the Best Practices paper was converted to a formal OSFI guideline and revised to reflect changes implemented as a result of the promulgation of the Proceeds of Crime (money laundering) Act and Regulations. It also added further insights into deterring and detecting money laundering, such as the adoption of an annual Self Assessment Program, as well as a program of (voluntary) suspicious transaction disclosure to law enforcement.

1155. In addition the application of the guidance was extended to federal life insurers in 2001. In 2002 the guideline was further amended to add CFT requirements. Further changes are contemplated in the near future for the OSFI Guideline B-8, Deterring and Detecting Money Laundering and Terrorist Financing, which was last revised in November 2004. In addition, OSFI commenced offering information sessions to the industry in 2005 and continued to do so in 2006.

1156. It may be noted that this Guideline is more specifically suited to the banking sector than to life insurance companies The life insurance industry trade association (CLHIA) has developed in consultation with FINTRAC a guidance Manual intended for helping life insurance agents and brokers across Canada meet their AML obligations. CLHIA and LIMRA (Life Insurance Marketing and Research Association) have also developed jointly supporting on-line training lessons for Canada's life insurance agents and brokers. At the time of the evaluation the guidance Manual and the training lessons were not yet available. Representatives from OSFI have also spoken at a number of sessions on money laundering at various life insurance and banking sector industry educational events.

IDA

1157. The IDA provides regular notices to its members on developments in regulations, including the PCMLTFA, along with information on risks and trends. The IDA developed a guide, Deterring Money Laundering Activity: A Guide for Investment Dealers to help members effectively develop effective anti-money laundering programs in compliance with anti-money laundering and anti-terrorist financing obligations. In general, the guide discusses requirements under the PCMLTFA and refers to

guidance available from FINTRAC, know your client procedures, suspicious transaction reporting, monitoring of account activity, anti-money laundering training, audit program and relationship between introducing and carrying brokers.

1158. Representatives from the IDA have also spoken at a number of sessions on money laundering at various industry educational events.

3.10.2 Recommendations and Comments

1159. The Canadian AML/CFT supervisory structure has several significant weaknesses:

- The exclusion from the AML regime of a number of categories of financial institutions without proper and formalized prior risk assessments or without adequate justifications of low AML risks.
- Heterogeneous levels of AML compliance oversight in the different financial sectors, which is due to an insufficient level of compliance staff resources in FINTRAC compared to the number of reporting entities, and to variable levels of involvement by the various primary regulators (MSBs, life insurance intermediaries, some provincial credit unions and *caisses populaires*, etc.).
- The lack of adequate sanctions provided to FINTRAC under the PCMLTFA which is not compensated by the sanctions administered under their own statute by the other primary regulators (since the regime of administrative monetary penalties is not in force yet).
- The current absence of a registration regime for money service businesses and foreign exchange dealers (since the registration regime adopted in June 2007 will only be in force in June 2008).

1160. Canada could consider allowing FINTRAC to delegate formally its authority to examine financial institutions for AML/CFT compliance to its MOU partners and other primary regulators, so that the basis for their intervention in that area is sound and clear and in order to leverage existing examination resources and to avoid possible duplication of compliance inspections. Such a measure would also ensure a better knowledge by the AML compliance supervisor of the specifics of the sector. Such a delegation should go together with the settling by FINTRAC of objectives (frequency, coverage of risks) and common rules and standards for the conduct of examinations and inspections on its behalf by its partners.

1161. More generally, Canada should encourage the development of specific AML/CFT guidance by the various primary provincial regulators and a more active involvement in AML/CFT supervision. It could also envisage encouraging the creation of SROs in sectors which are less regulated, such as life insurance brokers or MSBs. It is essential too that sufficient resources be dedicated to the supervisory authorities responsible for AML/CFT oversight.

1162. The strengthening of the sanctions regime with the introduction of administrative and monetary penalties, as included in the amended PCMLTFA, should be a crucial enhancement for the effectiveness of the Canadian AML/CFT system. The delegation of the administration of these sanctions to the MOU partners could also be envisaged.

1163. Canada should ensure that market entry rules among the different provinces and sectors are compliant with FATF requirements.

1164. Finally, the creation of a registration regime for the MSBs will be an essential step in the necessary strengthening of the AML supervision of this highly risky sector.

3.10.3 Compliance with Recommendations 17, 23, 25, 29 & 30

Rec.	Rating	Summary of factors underlying ratings
Rec.17	PC	• With the exceptions of OSFI and IDA regulated institutions, only criminal sanctions are available to FINTRAC under the PCMLTFA for all other types of financial institutions and these are only applicable for the most serious failures, and need to be proved to the criminal standard. • OSFI only uses a limited range of actions/sanctions in the AML/CFT context (namely supervisory letters and in a limited number of cases, staging). • The lack of effective sanctions applied in cases of major deficiencies raises real concern in terms of effectiveness of the sanction regime, particularly taking into account that only one criminal sanction and a very limited number of administrative sanctions have been applied.
Rec.23	PC	• Exclusion from the AML/CFT regime of certain financial sectors (such as financial leasing, factoring, finance companies, etc.) without proper risk assessments. • For the financial institutions subject to the PCMLTFA, there is a very unequal level of supervision of AML/CFT compliance, with certain categories of financial institution appearing to be insufficiently controlled (MSBs, certain credit unions/*caisses populaires*, life insurance intermediaries…). This is due to the limited staff resources of FINTRAC dedicated to on-site assessments compared to the high number of reporting entities, which has not always been compensated by the involvement of the primary prudential regulators in AML/CFT issues. • "Fit and proper" requirements are not comprehensive. • At the time of the on-site visit, there was no specific obligation for FRFIs to implement screening procedures for persons who are hired, or appointed to the Board, after the initial incorporation or authorisation procedures are concluded. • There is currently no registration regime for MSBs.
Rec.25	LC	• There is a lack of specific guidelines intended for sectors such as life insurance companies and intermediaries.
Rec.29	LC	• FINTRAC has no power to impose administrative sanctions.

3.11 Money or value transfer services (SR. VI)

3.11.1 Description and Analysis

1165. *Definition*. Under the PCMLTF Regulations, "*money services business*" means a person or entity that is engaged in the business of remitting funds or transmitting funds by any means or through any person, entity or electronic funds transfer network, or of issuing or redeeming money orders, traveller's cheques or other similar negotiable instruments. It includes a financial entity when it carries out one of those activities with a person or entity that is not an account holder.

1166. To assist the private sector, FINTRAC Interpretative Note March 1, 2005 provides guidance on what it means to be "engaged in the business".

1167. A business is considered to be a MSB if any of the following applies: (1) the business issues or redeems money orders, traveller's cheques or other similar negotiable instruments for more than CAD1 000 with the same person on the same day; (2) the individuals running the business advertise (by means of newspaper, television, yellow pages, Internet, any other media, or by an interior or exterior sign) the fact that they engage in the activity; (3) the business holds a permit or licence related to the activity; (4) the business is registered as someone carrying on the activity; or reports the income of that activity as income from a separate business for tax purposes". Money services businesses include alternative money remittance systems, such as Hawala, Hundi, Chitti, etc.

1168. *Issue of registration/licensing*. At the time of the assessment, there were no federal licensing requirements in place for MSBs. Under the Canadian constitution, licensing of these types of businesses falls within the powers of the provincial governments. However, given that Canada's

AML/CFT legislation is a federal Act and after consultation with the provinces, Canada has moved to create a federal registration regime[135]. At the time of the on-site visit, some provinces regulated the sector, but only in relation to "payday" lending services and in respect of customer protection rules.

1169. FINTRAC has made use of different techniques in identifying MSBs and raising awareness in this sector, including: (1) searching telephone and business directories; (2) field research (walk/drive through neighbourhoods looking for commercial signs); (3) awarded contracts to conduct searches for advertisements in ethnic newspapers; and (4) held regional open house workshops on legislative obligations (all MSBs were sent an invitation). Generally speaking, FINTRAC's outreach activities with the MSB sector include overview presentations about FINTRAC, and presentations concerning reporting entities' obligations under the PCMLTFA and its associated regulations.

1170. With these measures, FINTRAC has been able to identify some 700 MSBs in Canada, largely located in major urban areas. The market is dominated by a few large firms but is also composed of a vast number of relatively small entities compared to other types of reporting entities in the financial sector. However, it has been very difficult to build a complete inventory of the sector since many money services are a part of other businesses such as travel agencies, small grocery stores and gas stations; and they might not advertise. Complicating the task further, these services go in and out of business at a high turnover rate.

1171. The MSB sector has generated more STRs than banks since 2001, with almost one third of all STRs received by FINTRAC coming from this sector. Nevertheless, detailed statistics show that only a limited number of MSBs (mostly the largest players) report STRs to FINTRAC. The following table shows the MSB sector compared with all reporting entities from 2002 to 2006:

	MSB	Total reporting entities	% of Total
Number of reporting entities	about 700	Over 300 000	0.2
Suspicious Transaction Reports	33 426	102 835	33
Large Cash Transaction Reports	214 247	15 800 939	1.4
Electronic Fund Transfer Reports	96 790	29 328 058	0.3

1172. One of the key challenges the larger players currently face is the selection of agents in which some of the bigger MSBs will conduct extensive checks on individual companies and criminal records checks on individuals but this does not apply in all cases. The key players met by the assessment team indicated that they would like the sector to be licensed as it would build market confidence and image.

1173. *Application of the FATF Recommendation*s. The MSB sector is subject to client identification, record keeping and reporting requirements under the PCMLTFA. However, the preventive measures currently applicable to financial institutions including MSBs in Canada (especially in relation to CDD, reporting of suspicious transactions or SRVII) present very serious weaknesses (see in particular Sections 3.2, 3.5 and 3.7 of the report). The MSB sector is therefore subject to a limited range of preventive measures that are not in compliance with international standards.

1174. *Monitoring.* FINTRAC is responsible for supervising the MSB sector for AML/CFT purposes[136]. *In order to* fulfill its responsibilities effectively under section 62 of the PCMLTFA, FINTRAC has established a compliance program. In particular, FINTRAC has made use of Compliance Questionnaires (CQs) (see Section 3.10 of the report). As part of its outreach activities,

[135] A registration system is due to come into force on 23 June 2008. Individuals and entities that engage in MVT services will be required to register with FINTRAC. The registration regime is designed to facilitate compliance with existing obligations under the PCMLTFA and to help FINTRAC supervise an otherwise unregulated sector. It will also create a new criminal offence for operating an unregistered MSB.

[136] Under regulations enacted in June 2007 and in force in June 2008, FINTRAC is responsible for accepting, denying, revoking and verifying applications for registration, maintaining the information contained in the registry and verifying compliance with the registration requirement.

FINTRAC has also had 149 meetings with entities in that sector since 2004-05, which involved over 400 participants (12% of FINTRAC outreach activities (presentations and meetings) over the last three years have been targeted at entities from that sector and 29% of all CQs having been sent to entities in the sector).

1175. The following table illustrates the percentage of positive responses to questions in the CQ about key compliance elements (as of the end of 2005-06):

AREA OF COMPLIANCE	MSB
Implemented Compliance Regime	85%
Designated Compliance Officer	75%
Implemented Compliance Policies & Procedures	91%
Review of Policies & Procedures	77%
Ongoing Compliance Training	71%

1176. The following table indicates the number of FINTRAC examinations conducted in the MSB sector:

Sector	2004-05	2005-06	2006-07 (as of end 09/06)	Total (by sector)
MSB	164	56	43	263*
All Other Financial Institutions	12	64	40	116
Total	176	120	83	379

Note: In fiscal year 2003-04, FINTRAC began to conduct examinations and completed a total of 26 examinations. The focus of these examinations was largely on the MSB sector.

1177. FINTRAC has, to a significant degree, focused its examination resources in the MSB sector, especially in the early years, with 69% of all its examinations of financial institutions having been conducted in that sector over the last 2.5 fiscal years (about 40% of the identified MSBs have been examined by FINTRAC) but clearly there is scope for further progress in this area although it should be noted that a single FINTRAC examination covers the parent entity and potentially may cover many agents of the MSB.

1178. *List of agents*. There is currently no legal requirement for each MSB to maintain a list of agents[137].

1179. *Sanctions applicable to MSBs failing to apply the AML/CFT requirements*. At the time of the on-site visit, under the PCMLTFA, FINTRAC could not impose penalties to MSBs failing to apply the PCMLTFA and its Regulations but only had the option of referring a case of non-compliance to law enforcement for investigation and prosecution (see Section 3.10 of the report)[138]. To date, FINTRAC has disclosed seven such cases of non-compliance to law enforcement agencies and one MSB operator has been convicted for non-compliance with the PCMLTFA and for money laundering. However, at the time of the on-site visit, the sanction regime available to FINTRAC was not effective, proportionate and dissuasive.

1180. *Additional element*. The Best Practices Paper for SRVI outlines five areas in which preventative measures should be considered, namely: licensing/registration; identification and awareness raising; AML Regulations; compliance monitoring and sanctions. In terms of compliance monitoring, a substantial body of work has already been conducted in this field by FINTRAC, along the

[137] The registration regime enacted in June 2007 and coming into force in June 2008 requires the MSBs to submit a list of agents to FINTRAC as part of the registration process (see Schedule 1 Part C of the PCMLTF Registration Regulations).

[138] The PCMLTFA enacted measures in December 2006 that come into force in December 2008 and introduce a new regime of sanctions.

recommended lines in the Best Practice Paper. Other elements were very partially in place at the time of the on-site visit although the overall implementation of the Best Practices Paper should significantly improve after the introduction of the regulatory changes under the PCMLTFA.

3.11.2 Recommendations and Comments

1181. Canada should ensure effective implementation of the registration system for MSBs in force in June 2008 and ensure that the requirements applicable to MSBs fully meet the FATF requirements.

3.11.3 Compliance with Special Recommendation VI

Rec.	Rating	Summary of factors underlying ratings
SR. VI	NC	• There is no registration regime for MSBs as contemplated by SR VI. • Overall, requirements and implementation of Recommendations 4-11, 21-23 and SR. VII is inadequate which has a significant negative impact on the effectiveness of AML/CFT measures for money transmission services.. • MSBs are not required to maintain a list of their agents. • The sanction regime available to FINTRAC and applicable to MSBs is not effective, proportionate and dissuasive.

4. PREVENTIVE MEASURES – DESIGNATED NON-FINANCIAL BUSINESSES AND PROFESSIONS

4.1 Customer due diligence and record-keeping (R.12) (applying R.5, 6 & 8-11)

4.1.1 Description and Analysis

Definitions and scope

1182. The PCMLTF Regulations currently cover casinos, real estate brokers and sales representatives, and accountants/accountant firms as reporting entities to FINTRAC. The AML/CFT preventive measures do not currently apply to lawyers, Quebec Notaries, BC Notaries nor to dealers in precious metals and stones[139].

1183. "*Casinos*" means a person or entity that is licensed, registered, permitted or otherwise authorised to do business under any of paragraphs 207(1)(a) to (g) of the Criminal Code and that conducts its business activities in a permanent establishment (i) that the person or entity holds out to be a casino and in which roulette or card games are carried on; or (ii) where there is a slot machine, which, for the purposes of this definition, does not include a video lottery terminal. It does not include a person or entity that is a registered charity as defined in subsection 248(1) of the Income Tax Act and is licensed, registered or otherwise authorised to carry on business temporarily for charitable purposes, if the business is carried out in the establishment of the casino for not more than two consecutive days at the time under the supervision of the casino.

1184. Gambling is permitted pursuant to the Criminal Code of Canada and regulated through provincial gaming legislation (along with its regulations, rules, directives, terms and conditions, and policies). Part VII of the *Criminal Code* makes it an offence to operate a commercial gaming enterprise. The two main exceptions to this prohibition are gambling activities conducted and managed by the province, or pursuant to a licence issued by the province. The *Criminal Code* does not contain any exceptions from the broad prohibition that would allow for the establishment of an Internet casino.

[139] The regulations enacted on 26 December 2007 extend coverage of the Act to these new sectors as of December 2008: legal counsel and legal firms, BC notaries public and notary corporations and dealers in precious metals and stones. See http://www.fin.gc.ca/news07/07-105e.html.

1185. Yet despite prohibitions against non-governmental Internet gambling, there are signs that the online gaming industry is growing in Canada and for some years now, a community in Quebec is hosting servers and has been selling "licences" for the operation of Internet gaming businesses. Interestingly, the RCMP advised it has limited capacity for handling illegal activity related to Internet casinos. Having tried previously to tackle the issue, they found they did not have the resources as the criminals were tracking investigations online and moving their servers off-shore. Internet casinos do not fall within the scope of the PCMLTFA.

1186. *Cruise ships*. Cruise ships operate out of Canadian waters and do offer casino facilities. As indicated by the Department of Transport, after the Caribbean and the Mediterranean, Alaska cruises through British Columbia's Inside Passage are the third most popular in the world. Large cruise vessels calling at Canada's ports are owned by foreign-based companies. Sailing under foreign flags, these vessels offer two basic types of extended cruises: the luxury cruise and the "pocket cruise", distinguished by vessel capacity of more or less than 150 passengers. Vancouver is the main hub in the Canadian cruise ship industry although Vancouver's share of this traffic is decreasing since 2001 to reach some 830 000 passengers in 2006.

1187. In March 1999, amendments to Canada's Criminal Code came into effect, easing restrictions on casino gambling aboard cruise ships. International cruise lines are now able to operate on-board casinos until they are within five nautical miles of a Canadian port of call (as compared to the 12 nautical mile limit for Canadian territorial waters). Previously, vessels had to close casinos as soon as they reached Canadian territorial waters. Some limitations exist: voyages must be at least 48 hours in length to offer gaming services, and passengers embarking in Canada cannot be scheduled to disembark without first calling at one or more non-Canadian ports. Cruise ships are not covered under the PCMLTFA as Canada believes that there is a limited capacity to misuse the casino facilities.

1188. **"***Accountant*" means a chartered accountant, a certified general accountant or a certified management accountant. Accountants and accountant firms are subject to the PCMLTFA when they:

a) Engage in any of the following activities *on behalf of* a person or entity:

- Receiving or paying funds.
- Purchasing or selling securities, real property or business assets or entities. Or
- Transferring funds or securities by any means.

b) Give instructions on behalf of any person or entity in respect of above activities.

c) Receive professional fees in respect of any activity referred to in a) or b).

1189. The Canadian Institute of Chartered Accountants (CICA) believes the accountant must be acting on behalf of a third party, i.e. to be an intermediary or a facilitator in the transaction. This means that the accountant has to be actually involved in the transaction, representing either the client or some third party.

1190. **"***Real estate broker or sales representative***"** means a person or entity that is registered or licensed under provincial legislation. Real estate agents are subject to the PCMLTFA when they engage in any of the following activities on behalf of any person or entity in the course of a real estate transaction:

- Receiving or paying funds.
- Depositing or withdrawing funds. Or
- Transferring funds by any means.

1191. *Real estate developers*. Home builders and real estate developers are two more sectors which the Government proposes to bring within the ambit of the PCMLTFA since they can carry out much the same role and activities as licensed real estate agents by selling homes directly to the public.

1192. *Lawyers and Quebec notaries* (who provide legal advice under the Quebec civil code) were exempted from complying with the provisions of the PCMLTFA in March 2003 when the Government revoked the regulatory provisions as they applied to legal counsel. This followed a legal challenge by the profession when the Government had initially proceeded to require mandatory suspicious and prescribed reporting, client identification, record keeping and internal compliance requirements of legal counsel when engaged in the following activities on behalf of a person or entity including the giving of instructions on behalf of any person or entity in respect of:

- Receiving or paying funds, other than those received or paid in respect of professional fees, disbursements, expenses or bail.
- Purchasing or selling securities, real properties or business assets or entities. Or
- Transferring funds or securities by any means.

1193. The professional legal bodies had argued that requiring lawyers to report information on their clients to the state is contrary to the right to solicitor-client privilege and the principle of an independent bar and judiciary.

1194. During the on-site visit, the legal profession acknowledged that there is a risk of money laundering in the "layering" stage in the business they conduct but seemed to imply money laundering was primarily a cash-based activity and that the Government was not explaining adequately where the risks lie in their discussions with the profession. The profession expressed willingness to the assessors to conduct identification and record keeping, while at the same time protecting access to that information but reporting remains an issue for them.

1195. The assessors were familiar with lawyer-client legal privilege argument but noted with interest that lawyers remain exempted when involved in the more routine purchase and sale of real property while real estate agents, engaged in exactly the same type of transaction, are required to report. The assessors were told that as a matter of business practice, the banking sector asks mortgage brokers and the legal profession to identify mortgage borrowers in accordance with the PCMLTFA at the closing of a real estate transaction.

1196. The amendments to the PCMLTF Regulations pre-published on June 30, 2007 propose to subject legal counsel and legal firms to Part I of the PCMLTFA when they engage in any of the following activities on behalf of any person or entity: (a) receiving or paying funds, other than those received or paid in respect of professional fees, disbursements, expenses or bail or (b) giving instructions in respect of any activity referred to in paragraph (a)[140].

1197. *BC Notaries* were not included in the PCMLTFA in 2001. They do not provide legal advice, undertake limited activities but they are allowed to hold trust accounts to carry out their duties and carry out real estate activities. While the number of BC Notaries is limited by statute to 332, they are at risk of being used for ML/TF. Regulations pre-published on June 30, 2007 extend coverage of the PCMLTFA to them when they act as financial intermediaries[141].

1198. *Trust and company service providers*. TCSPs are not separately recognised nor regulated as a separate business category operating in Canada although there was some acknowledgement during the on-site visit that there are businesses other than lawyers, accountants and trust companies that offer such services[142]. They do not fall under the scope of the PCMLTFA if they are not an entity or person otherwise covered by the legislation (trust and loan companies).

---

140 The PCMLTF Regulations were enacted in December 2007.

141 The PCMLTF Regulations were enacted in December 2007.

142 See for example businesses listed at:
http://ca.dir.yahoo.com/business_and_economy/business_to_business/corporate_services/incorporation_services

1199. *Dealers in precious metals and stones*. Dealers in precious metals and stones are not covered by the PCMLTFA. The profession has met with the Department of Finance to discuss their coverage by the AML/CFT regime. The proposed amendments to the PCMLTF Regulations pre-published on June 30, 2007 extend such coverage to them[143]. The assessors were told that the record keeping requirement is generally perceived as the most challenging issue due to the PIPEDA potential restrictions on customer's information retention and the very small size of the large majority of the retail businesses dealing precious metals and stones. The assessors were told that the industry would not oppose to any reporting requirement, in particular LCTRs since cash transactions are quite a limited practice in this sector (90% of the transactions seem to occur using a credit card).

Applying Recommendation 5

1200. No CDD requirements as set out in Recommendation 5 apply to Internet casinos, ship based casinos, lawyers and Quebec notaries, BC Notaries, trust and company service providers (except trust companies and accountants that may provide that type of services) and dealers in precious metals and stones.

1201. *Casinos*. Casinos are subject to special measures to identify the following individuals or entities (Section 60(b) of the PCMLTF Regulations):

- Any individual who signs a signature card in respect of an account that the casinos opens.
- Any individual who conducts a transaction with the casino for which a large cash disbursement record is required to be kept.
- Any individual carrying out foreign exchange transactions of CAD 3 000 or more or equivalent in foreign currency.
- Any individual conducting a large cash transaction.
- Any individual who conducts a transaction of CAD 3 000 or more for which an extension of credit needs to be kept.
- Any corporation or entity which opens an account.

1202. There is no requirement to carry out CDD measures when there is a suspicion of ML or TF and when financial institutions have doubts about the veracity or adequacy of previously obtained CDD data. There is no obligation to carry out customer identification for occasional transactions that are wire transfers[144]. The requirement to identify any individual for large cash transactions (above CAD10 000 which is a too high threshold) does not cover non-cash occasional transactions[145].

1203. Section 64 of the PCMLTF Regulations requires casinos to ascertain customer's identification by referring to the person's birth certificate, driver's licence, provincial health insurance card, passport or any similar record. FINTRAC Guidance 6F provides further indications on the type of documents to use (see Section 3.2 of the report for further developments).

1204. Casinos are subject to equivalent customer identification requirements as financial entities in relation to the identification of:

- Individual not physically present (Section 64(1(a)(ii) of the PCMLTF Regulations).
- Corporation or entity other than corporation (Sections 65 & 66of the PCMLTF Regulations).

143 The PCMLTF Regulations were enacted in December 2007.

144 Regulations enacted in June 2007 and which come into force in June 2008 will require that casinos identify clients in respect of these situations (see Section 60(b)(iv) of the amended PCMLTF Regulations).

145 Regulations pre-published in October 2007 will require casinos to identify clients, keep records and make reports with respect to all large disbursements regardless of the form of payment (e.g. chips, wire transfers, cash, etc.) (see Sections 42, 43(g), 44, 60(b)(i) and Schedule 8 of the PCMLTF Regulations, as amended by the regulations published in October 2007).

- Individuals acting on behalf of the customer (third party determination, Section 8 of the PCMLTF Regulations).

1205. Exceptions to ascertaining identity apply also to casinos: (1) if the customer has already an account (Section 62(2)(a) the PCMLTF Regulations); (2) if there are reasonable grounds to believe that the account holder is a public body or a corporation that has minimum net assets of CAD 75 million on its last audited balance sheet and whose shares are traded on a Canadian stock exchange or a stock exchange that is prescribed by section 3201 of the Income Tax Regulations and operates in a country that is a member of the FATF (Section 62(2)(a) the PCMLTF Regulations) or (3) for the opening of a business account for which the casino has already ascertained the identity of at least three persons who are authorised to give instructions in respect of the account (Section 60(a) of the PCMLTF Regulations).

1206. Casinos are not required to carry out customer identification in relation to: beneficial ownership; ongoing due diligence for accounts that the casinos open and higher risk categories of customers. Casinos are not required to collect information on the purpose and intended nature of the business relationship and on existing customers. There is no specific provision in the case casinos fail to complete CDD[146].

1207. The customer identification (natural or legal person) must be carried out before any transaction other than an initial deposit is carried out on an account.

1208. *Real estate agents and sales representatives.* Real estate agents and sales representatives are subject to customer identity verification (see Article 6.1 of the PCMLTFA) when they engage in any of the following activities on behalf of any person or entity in the course of a real estate transaction (Section 37 of the PCMLTF Regulations):

- Receiving or paying funds.
- Depositing or withdrawing funds. Or
- Transferring funds by any means.

1209. The PCMLTF Regulations also requires real estate brokers and sales representatives to ascertain the identity of their client when they receive §10,000 or more from the client in the course of a single transaction or two or more transactions carried out within a 24-hour period.

1210. In determining the identity of individuals, the PCMLTFA requires that brokers and sales representatives refer to a government issued identification document, such as a birth certificate, driver's license, passport, record of landing, permanent resident card or other similar record, and a provincial health card in certain provinces (see FINTRAC Guideline 6B of June 2005).

1211. When dealing with a corporation or any other entity, there is no specific requirement applicable to real estate agents and sales representatives to ascertain the identity of legal persons[147].

1212. The circumstances in which real estate agents and sales representatives have to carry out customer identification is too restrictive since they should be required to do so when they are involved

[146] Regulations which were enacted in June 2007 and come into force in June 2008, will close some of those gaps by requiring that casinos take reasonable measures to conduct ongoing monitoring; keep client information up-to-date in higher risk situations; and prohibiting casinos from opening an account if the identity of the client cannot be established (see Sections 71.1 and 53.2 of the amended PCMLTF Regulations).

[147] Section 59.2 of the PCMLTF Regulations enacted on 27 June 2007 and entering into force on 23 June 2008 requires real estate agents and sales representatives to confirm the existence and ascertain the name and address of every corporation/entity on whose behalf a transactions is conducted and the names of directors.

in transactions for a client concerning the buying and selling of real estate (see FATF Recommendation 12)[148].

1213. The CDD requirements applicable to real estate agents and sales representatives are substantially very basic and limited. They do not meet the FATF standards set out in Recommendation 5. Only Section 8 of the PCMLTF Regulations on third party determination (see Section 3.2 of the report "*Third party determination*" for a complete description of the provision) - that is applicable to every person or entity that is required to keep a large cash transaction report - applies to real estate agents and sales representatives. FINTRAC Guideline 6B for real estate agents and sales representatives states that what constitutes reasonable measures in making a third party determination will vary in accordance with the context in which they occur, and therefore could differ from one situation to the next. However, reasonable measures would include retrieving the information already contained in the agent's files or elsewhere within the business environment, or obtaining the information directly from the client.

1214. *Accountants and accountant firms*. Accountants are required to carry out customer identification when they (Section 34 of the PCMLTF Regulations):

a) engage in any of the following activities *on behalf of* a person or entity:
- Receiving or paying funds.
- Purchasing or selling securities, real property or business assets or entities. Or
- Transferring funds or securities by any means.

b) give instructions on behalf of any person or entity in respect of above activities

c) receive professional fees in respect of any activity referred to in a) or b).

1215. Accountants and accountant firms are subject to client identification obligations when they receive professional fees to engage in any of the activities listed above. This means that they would be subject to the client identification requirements when they engage in any of the activities mentioned above even if they were doing them on a volunteer basis. Activities of accountants or accounting firms other than those listed above, such as audit, review or compilation engagements carried out according to the recommendations in the Canadian Institute of Chartered Accountants (CICA) Handbook, do not trigger record keeping or client identification obligations. Giving advice to a client, in the context of your accountant-client relationship, is not considered providing instructions (FINTRAC Guidelines 6B of June 2005).

1216. The PCMLTF Regulations also requires accountants and accountant firms to ascertain the identity of their client when they receive CAD 10 000 or more from the client in the course of a single transaction or two or more transactions carried out within a 24-hour period.

1217. In determining the identity of individuals, the PCMLTFA requires that accountants refer to a government issued identification document, such as a birth certificate, driver's license, passport, record of landing, permanent resident card or other similar record, and a provincial health card in certain provinces (see FINTRAC Guideline 6B).

1218. When dealing with a corporation or any other entity, there is no specific requirement applicable to accountants/accountants firms to ascertain the identity of legal persons[149].

---

[148] This issue is addressed in the PCMLTF Regulations enacted on 27 June 2007 that will enter into force on 23 June 2008 (see Section 59.2 of the amended PCMLTF Regulations that must be read in conjunction with section 39 of the same regulations).

[149] Section 59.1 of the PCMLTF Regulations enacted on 27 June 2007 and entering into force on 23 June 2008 requires accountants and accountant firms to confirm the existence and ascertain the name and address of every corporation/entity on whose behalf a transactions is conducted and the names of directors.

1219. The circumstances in which accountants have to carry out customer identification are too restrictive since they should also be required to do so in the following circumstances (see FATF Recommendation 12):

- Management of bank, savings or securities accounts.
- Management of client money, securities and other assets (and not only purchasing or selling of these).
- Organisation of contributions for the creation, operation or management of companies.
- Creation, operation or management of legal persons or arrangements.

1220. The current CDD requirements applicable to accountants are substantially very basic and extremely limited. They meet a very limited range of requirements under Recommendation 5.

1221. Accountants and real estate agents and sales representatives must inform individuals concerning the collection of personal information about them. However, they do not have to inform individuals when they include personal information about them in any reports that they are required to make to FINTRAC (see FINTRAC Guideline 6B).

Applying Recommendation 6

1222. Canada has not implemented any specific AML/CFT measures concerning PEPs that are applicable to DNFBPs and discussions with the private sector representatives met by the assessment team suggest that this is not perceived as an area of high priority.

Applying Recommendation 8

1223. There are no specific legislative or other enforceable obligations for DNFBPs to take measures to prevent the misuse of technological developments in ML/TF schemes[150].

1224. The DNFBPs are not required to have policies and procedures in place to address any specific risk associated with non face-to-face business relationships or transactions[151].

Applying Recommendation 9

1225. There are currently no provisions for DNFBPs that address the issue of relying on intermediaries or third parties to perform elements of the CDD process (see Section 3.3 of the report). FINTRAC's current Guideline 6 indicates that DNFBPs may choose to use an agent/introducer or third party for customer identification purposes and, should they chose to do so, they need to enter into a written agreement with the agent/introducer which specifies what is expected from the agent/introducer. Where the DNFBP chooses to enter into such an agreement, it is ultimately responsible for ensuring that the identification requirements are met. This covers an outsourcing type of scenario that falls outside the scope of Recommendation 9.

---

150 The Regulations enacted in June 2007 and coming into force in June 2008 will require all reporting entities to conduct ongoing monitoring and keep client information up-to-date in higher risk situations, such as when new technologies are used to delivers products and services (see Sections 71 and 71.1 of the amended PCMLTF Regulations).

151 Section 64 of the PCMLTF Regulations enacted on 27 June 2007 (and due to enter into force on 23 June 2008) requires real estate agents and sales representatives, casinos and accountants/accountant firms to take specific customer identification steps if the person is not physically present at the time the business relationship is established.

Applying Recommendation 10

1226. No record keeping as described in Section 6 of the PCMLTFA apply to Internet casinos, ship based casinos, lawyers and Quebec notaries, BC Notaries, trust and company service providers (except trust companies) and dealers in precious metals and stones.

1227. *Casinos*. The record keeping requirements in relation to casinos are comprehensive. Casinos have to keep the following records: (1) large cash transaction records; (2) large cash disbursement records; (3) certain records about client accounts; (4) extension of credit records; and (5) foreign currency exchange transaction tickets. The record keeping requirements for the large cash transaction reports as well as the large cash disbursement records (Section 41 & 42 of the PCMLTF Regulations) are as follows:

	Large cash transaction reports	**Large cash disbursement records**
Type of transactions for which a record has to be kept	▪ The sale of chips, tokens or plaques. ▪ Front cash deposits. ▪ Safekeeping deposits. ▪ The repayment of any form of credit, including repayment by markers or counter cheques. ▪ Bets of currency. ▪ Sales of your casino's cheques.	▪ The redemption of chips, tokens or plaques. ▪ Front cash withdrawals. ▪ Safekeeping withdrawals. ▪ Advances on any form of credit, including advances by markers or counter cheques. ▪ Payments on bets, including slot jackpots. ▪ Payments to clients of funds received for credit to that client or any other client. ▪ Cashing of cheques or other negotiable instruments. ▪ Reimbursements to clients of travel and entertainment expenses.
Record keeping exemption	If the cash is received from a financial entity. (bank, credit union or caisse populaire; trust and loan company; or an agent of the Crown that accepts deposit liabilities)	-
Contents of the record[152]	▪ The amount and currency of the cash received. ▪ The name of the individual from whom you received the cash and that individual's address and principal business or occupation. ▪ The date of the transaction. ▪ The purpose, details and type of transaction (for example, the cash was used to buy chips, etc.), including whether any other individuals or entities were involved in the transaction. ▪ How the cash was received (for example, in person, by mail, by armoured car, or any other way). ▪ If an account was affected by the transaction, include the following: the number and type of any such account; the full name of the client that holds the account; and the currency in which the account's transactions are conducted.	▪ The name of the individual to whom the disbursement is made. ▪ That individual's address and principal business or occupation. ▪ The date and what kind of disbursement it is.
Extra record to keep for client identification	▪ The individual's date of birth. ▪ The type of document used to confirm the individual's identity, the document's reference number and its place of issue.	▪ The individual's date of birth. ▪ The type of document used to confirm the individual's identity, the document's reference number and its place of issue.

[152] Information on individual's date of birth will have to be kept from June 2008 (see the definition of "large cash transaction record" in 1(2) and paragraph 42(2)(d) of the amended PCMLTF Regulations. Please note that once the large disbursement reporting requirement comes into force (as introduced in the regulations that were published in October 2007), casinos will be required to keep a copy of the large disbursement report instead of a large cash disbursement record. However, the report also contains the date of birth of the person requesting the disbursement (see new Schedule 8, Part D, item 8 under PCMLTF Regulations).

1228. The record keeping requirements for client accounts are as follows (Section 43 of the PCMLT Regulations):

- *Account operating agreements*: an account operating agreement is any document that is received or created in the normal course of business and outlines the agreement between the casino and its client about the account's operation. If the casino has to identify the individual, the account operating agreement for that individual also has to contain the following information: (1) the individual's date of birth; and (2) the type of document used to identify the individual, its reference number and its place of issue. If the casino has identified the individual based on a cleared cheque, the account operating agreement has to contain the financial entity and account number of the account on which the cheque was drawn.
- *Deposit slips:* casinos have to keep a deposit slip for every deposit made to an account. A deposit slip means a record that sets out the date of a deposit, the amount of the deposit, and any part of it that was made in cash. A deposit slip also sets out the holder of the account in whose name the deposit is made and the number of the account.
- *Debit or credit memos*: casinos have to keep any debit or credit memo that they create or receive regarding an account in the normal course of business.
- *Accounts for corporations*: if the account is opened for a corporation, casinos have to keep a copy of the part of the official corporate records showing the provisions that relate to the power to bind the corporation regarding the account. This could be the articles of incorporation that set out those duly authorised to sign on behalf of the corporation, such as an officer, the comptroller, etc. If there were changes subsequent to the articles, then the board resolution stating the change would be included in this type of record.
- *Accounts for an individuals or entities other than corporations*: if the account is opened for an individual or any entity that is not a corporation, the casinos have to keep a record of the name, address and principal business or occupation of that individual or entity.
- *A signature card in respect of every account holder*: casinos have to keep a signature card in respect of any account they open, which must include the date of birth of the person, the type and number of the identification document used to identify the individual and its place of issue.

1229. Casinos have also to keep an extension of credit record for every extension of credit to a client of CAD 3 000 or more. This record has to indicate the following information: (1) the name of the client; (2) the client's address and principal business or occupation; (3) the terms and conditions of the extension of credit; and (4) the date and amount of the extension of credit (Section 43(d) of the PCMLTF Regulations).

1230. Third party record requirements in relation to third party determination are equivalent to these applicable to financial entities (see Section 3.5 of the report).

1231. Casinos are recommended to maintain an effective record keeping system to enable FINTRAC to have access to the records in a timely fashion. Such records have to be kept in such a way that they can be provided to FINTRAC within 30 days of a request to examine them (Section 69 of the PCMLTF Regulations and FINTRAC Guideline 6F).

1232. *Real estate agents and sales representatives and accountants*. Real estate agents and sales representatives and accountants have record keeping obligations when they engage in one of the activities described above (see this section of the report in relation to "Applying Recommendation 5") as well as for large cash transactions and third party determination (see Section 3.5 of the report that sets out the details of the record keeping requirements in the case of large cash transactions and third party determination). However, the circumstances in which real estate agents and sales representatives

and accountants have to keep record are not satisfactory since the list of activities covered is too restrictive (see this section of the report in relation to "*Applying Recommendation 5")*[153].

1233. Large cash transactions records must be kept for a period of at least five years following the date they were created. The records' retention rules are otherwise described in Section 69 of the PCMLTF Regulations and are equivalent to those applicable to financial entities (see Section 3.5 of the report). FINTRAC Guideline 6B recommend real estate agents and sales representatives and accountants to maintain an effective record keeping system to enable FINTRAC to have access to the records in a timely fashion. Such records have to be kept in such a way that they can be provided to FINTRAC within 30 days of a request to examine them. Records must be in a machine-readable or electronic form, as long as a paper copy can be readily produced. Also, for records that are kept electronically, an electronic signature of the individual who must sign the record has to be retained.

Applying Recommendation 11

1234. There is currently no explicit provision requiring that DNFBPs pay special attention to all complex, unusual large transactions that have no apparent or visible economic or lawful purpose. Similar to financial institutions, such a requirement may only be indirectly deduced from the requirement to report to FINTRAC suspicious transactions that may be related to money laundering or terrorist financing, as well as the obligation to report large international electronic funds transfer reports involving CAD 10 000 or more (EFTRs) and large cash transaction reports of CAD 10 000 or more (LCTRs).

4.1.2 Recommendations and Comments

1235. *Scope issues*. The assessors noted that Canada is working on addressing the outstanding scope issues and such an effort should continue in order to bring all DNFBPs in line with FATF Recommendations[154]. The participation of lawyers in the AML/CFT effort is essential since their current exemption leaves a very significant gap in coverage. The circumstances in which real estate agents and sales representatives and accountants have to carry out customer identification and keep records should be extended to be in line with the types of activities targeted under Recommendation 12[155].

1236. *Recommendation 5*. Canada should ensure that the entire set of requirements under Recommendation 5 apply to all non-financial professions.

1237. *Recommendations 6, 8, 9 and 11*. Canada should require the non-financial professions to implement requirements in relation to Recommendations 6, 8, 9 and 11.

1238. *Recommendation 10.* Canada should ensure that all types of transactions carried out by the non-financial professions are subject to proper record keeping requirement that permits their reconstruction so as to provide, if necessary, evidence for prosecution of criminal activity. Canada should ensure that all customer and transactions records and information collected by the non-financial professions are available on a timely basis to domestic competent authorities.

---

153 These circumstances are expanded in regulations enacted in June 2007 and coming into force in June 2008 (see Section 39 of the amended PCMLTF Regulations).

154 Canada enacted regulations on December 2007 to extend coverage of the PCMLTFA to the following sectors as of December 2008: legal counsel and legal firms, BC notaries public and notary corporations and dealers in precious metals and stones.

155 Canada indicates that the regulations coming into force in June 2008 will resolve this issue.

4.1.3 Compliance with Recommendation 12

Rec.	Rating	Summary of factors underlying ratings
R.12	NC	*Scope issue* • Lawyers, Quebec Notaries, BC Notaries, dealers in precious metals and stones, Internet casinos, ship based casinos and TCSPs are not captured by the PCMLTFA and therefore are not subject to the requirements under Recommendations 5, 6 and 8-11. *Application of Recommendation 5 to casinos* • The requirements applicable to casinos are insufficient in relation to: (1) when CDD is required; (2) required CDD measures; (3) identification of persons acting on behalf of the customer; (4) third party determination and identification of beneficial owners ; (5) purpose & intended nature of the business relationship ; (6) ongoing Due Diligence; (7) ML/FT risks and (8) failure to satisfactorily complete CDD. *Application of Recommendation 5 to real estate brokers and sales representatives and accountants* • The circumstances in which real estate agents and sales representatives and accountants have to carry out customer identification are too limitative. • The CDD requirements that real estate agents and sales representatives and accountants are subject to are substantially very basic and extremely limited. *Application of Recommendation 6 to casinos, real estate brokers and sales representatives and accountants* • Canada has not implemented any specific AML/CFT measures concerning PEPs that are applicable to DNFBPs. *Application of Recommendation 8 to casinos, real estate brokers and sales representatives, accountants* • There are no specific legislative or other enforceable obligations for DNFBPs to take measures to prevent the misuse of technological developments in ML/TF schemes. • The DNFBPs are not required to have policies and procedures in place to address any specific risk associated with non face-to-face business relationships or transactions. *Application of Recommendation 9 to casinos, real estate brokers and sales representatives and accountants* • There are currently no provisions for DNFBPs that address the issue of relying on intermediaries or third parties to perform elements of the CDD process outside the outsourcing type of scenario. *Application of Recommendation 10 to casinos, real estate brokers and sales representatives and accountants* • The circumstances in which real estate agents and sales representatives and accountants have to keep records are too limitative. • Real estate agents and sales representatives, casinos and accountants institutions must ensure that all records required to be kept under the PCMLTFA can be provided within 30 days which is not in line with the FATF requirement to make CDD records available on a timely basis to competent authorities. *Application of Recommendation 11 to casinos, real estate brokers and sales representatives and accountants* • There is currently no explicit provision requiring that DNFBPs pay special attention to all complex, unusual large transactions that have no apparent or visible economic or lawful purpose (the monitoring obligation is implied and indirect (it flows from reporting suspicious transactions, large international electronic funds transfer and large cash transactions) and it does not cover the full range of monitoring situations as stipulated in Recommendation 11). The other requirements under Recommendation 11 are not met either.

4.2 Monitoring transactions and other issues (R.16) (applying R.13-15, 17 & 21)

4.2.1 Description and Analysis

Applying Recommendation 13

1239. Every person or entity subject to Part I of the PCMLTFA is required to report to FINTRAC financial transactions for which there are reasonable grounds to suspect that the transaction is related to the commission of a money laundering or a terrorist financing offence (Section 7 of the PCMLTFA). Since 2002, reporting persons or entities have to send a terrorist property report to FINTRAC if they have property in their possession or control that they know is owned or controlled by or on behalf of a terrorist or a terrorist group. This includes information about any transaction or proposed transaction relating to that property. In addition to making a terrorist property report to FINTRAC about this type of property, there is also a requirement under the Criminal Code that applies to anyone in Canada and any Canadian outside Canada. Whether or not they are a reporting person or entity, they must disclose to the RCMP and CSIS, the existence of property in their possession or control that they know is owned or controlled by or on behalf of a terrorist or a terrorist group. Reporting entities are also required to report all cash transactions of CAD 10 000 or more.

1240. No suspicious transaction reporting requirement applies to Internet casinos, ship based casinos, lawyers and Quebec notaries, BC Notaries, trust and company service providers (except trust companies and accountants that may provide that type of services) and dealers in precious metals and stones.

1241. The PCMLTFA explicitly excludes, under Section 10.1, legal counsel and legal firms from STR and LCTR requirements "when they are providing legal services", which seems to be interpreted widely, as the profession considers that legal services cannot be in practice distinguished from financial services. It is worth mentioning that the Federation of Law societies is preparing a model rule on Client identification and verification requirements, which will be incorporated in the regulatory instruments of each law Society. It would apply when a lawyer acts as financial intermediary for a client and would include a provision stating that if a lawyer reasonably suspects that he might be assisting a client in dishonesty, fraud, crime or illegal conduct, he must withdraw from representation of the client and record the results of his reasonable suspicions.

1242. *Suspicious transactions reporting for casinos*. Under Article 5 of the PCMLTFA, casinos as defined in the regulations (see Section 4.1 of the report, "*definitions and scope*") are subject to the suspicious transactions reporting requirement. FINTRAC has elaborated indicators (Guideline 2 "*Suspicious Transactions*" of March 2003) for casinos to detect suspicious transactions.

1243. Under Section 40 of the PCMLTF Regulations, casinos are required to report to FINTRAC the receipt of an amount of cash of CAD 10 000 or more in the course of a single transaction unless the amount is received by a financial entity.

1244. *Suspicious transactions reporting for real estate agents and sales representatives*. Real estate agents and sales representatives have to submit STRs to FINTRAC according to Section 7 of the PCMLTF Suspicious Transaction Reporting Regulations when they engage in any of the following activities on behalf of any person or entity in the course of a real estate transaction: (1) receiving or paying funds; (2) depositing or withdrawing funds; or (3) transferring funds by any means. However, the circumstances in which they have to report suspicious transactions are not satisfactory since the list of activities covered is too restrictive (see comments in Section 4.1 of the report).[156]

[156] Canada indicated that the amendments to the PCMLTF Suspicious Transaction Reporting Regulations enacted in June 2007 and coming into force on 23 June 2008 extend these circumstances to any situation where real estate agents and sales representatives act as an agent in respect of the purchase or sale of real estate.

1245. *Suspicious transactions reporting for accountants and accountant firms*. Accountants and accountant firms are required to submit STRs to FINTRAC when they (Section 34 of the PCMLTF Regulations):

a) Engage in any of the following activities *on behalf of* a person or entity:
- Receiving or paying funds.
- Purchasing or selling securities, real property or business assets or entities. Or
- Transferring funds or securities by any means.

b) give instructions on behalf of any person or entity in respect of above activities
c) receive professional fees in respect of any activity referred to in a) or b).

1246. However, the circumstances in which accountants have to carry out customer identification are too restrictive (see comments in Section 4.1 "*definitions and scope*").

1247. The CICA has been active in developing comprehensive guidelines for compliance with the PCMLTFA (the guidelines were published in November 2004). These guidelines provide the CGAs with an overview of the obligations under the legislation and assist them developing a "knowledge base" from which the accountants can exercise their judgement in carrying out their obligation to report suspicious transactions. The assessors believe that such guidelines provide useful information to the profession.

1248. In practice, professionals face some difficulties to clearly determine which firms or individuals are subject to the requirement and what should be reported.

1249. With regard to accountants and real estate agents, it is worth noting that the effective implementation of the STR requirement is limited by the fact that these professions are only required to identify and ascertain identity of their clients in the case of large cash transactions.[157]

1250. *Provisions in relation to Recommendation 16 applicable to casinos, real estate agents and sales representatives and accountants/accountant firms*. The PCMLTFA requires the reporting of all completed transactions, where there are reasonable grounds to suspect that they relate to the commission of a money laundering or a terrorist financing offence, regardless of the involvement in tax matters. Attempted suspicious transactions are not yet covered by the Suspicious Transaction Reporting requirement[158].

1251. Casinos, real estate agents and sales representatives and accountants/accountant firms have to submit suspicious transaction reports to FINTRAC, containing specific information (see FINTRAC Guideline 3A). Once they have determined that there are reasonable grounds to suspect that the transaction is related to the commission of a money laundering or terrorist financing offence, their report, including all required and applicable information, must be sent within 30 calendar days. This 30-day reporting time limit begins when their employees first detect a fact about a transaction that constitutes reasonable grounds to suspect that it is related to the commission of a money laundering or terrorist financing offence. If such a fact is detected at the time of the transaction, the reporting timeline begins at the time of the transaction. However, if the fact is not detected at the time of the transaction, the 30-day time limit could begin at some time after.

---

157 Canada indicated that the amendments to the PCMLTF regulations enacted on 27 June 2007 and coming into force on 23 June 2008 require that all reporting entities identify their clients in respect of a suspicious transaction or a suspicious attempted transaction.

158 The PCMLTF Suspicious Transaction Reporting Regulations enacted on 27 June 2007 introduces an obligation to report attempted transactions as of 23 June 2008 (the requirement is in section 7 of the PCMLTFA. The PCMLTF Suspicious Transaction Reporting Regulations provide more details on the person or entities subject to the reporting requirement and on the information that must be reported).

1252. FINTRAC has elaborated indicators (Guideline 2 "*Suspicious Transactions*" of March 2003) for casinos to detect suspicious transactions including: (1) any casino transaction of CAD 3 000 or more when an individual receives payment in casino cheques made out to third parties or without a specified payee; (2) client requests a winnings cheque in a third party's name; (3) acquaintances bet against each other in even-money games and it appears that they are intentionally losing to one of the party; (4) client attempts to avoid the filing of a report for cash by breaking up the transaction; (5) client requests cheques that are not for gaming winnings; (6) client enquires about opening an account with the casino and the ability to transfer the funds to other locations when you do not know the client as a regular, frequent or large volume player; (7) client purchases large volume of chips with cash, participates in limited gambling activity with the intention of creating a perception of significant gambling, and then cashes the chips for a casino cheque; (8) client exchanges small denomination bank notes for large denomination bank notes, chip purchase vouchers or cheques; (9) client is known to use multiple names or (10) client requests the transfer of winnings to the bank account of a third party or a known drug source country or to a country where there is no effective anti-money-laundering system.

1253. Equivalent guidelines have been published by FINTRAC for the real estate agents and sales representatives as well as for accountants.

1254. *Statistics*. The following table indicates the number of STRs per fiscal year and by DNFBPs:

	2001/2002	2002/2003	2003/2004	2004/2005	2005/2006	2006/2007	**Total**
Accountants	7	20	20	40	20	12	**119**
Casinos	143	498	360	390	420	223	**2 034**
Legal counsel[159]	5	2	3	0	0	0	**10**
Real estate agents/sales representatives	2	8	6	6	12	1	**35**

1255. Some concern raised by the current STR requirement applicable to DNFBPs is the relatively low number of reports actually sent to FINTRAC by certain DNFBPs, in particular accountants and real estate brokers and sales representatives in spite of the outreach they have benefited from FINTRAC.

Applying Recommendation 14

1256. Section 10 of the PCMLTFA provides immunity provisions for reporting entities. No criminal or civil proceeding lie against a person or entity for making a suspicious transaction report, a terrorist property report, a large cash transaction report or an electronic funds transfer in good faith or for providing FINTRAC with information about suspicions of money laundering or the financing of terrorist activities.

1257. In addition to the immunity provision, Section 8 of the PCMLTFA specifies that no person or entity can disclose that they have made a suspicious transaction report, or disclose the contents of a report, with the intent to prejudice a criminal investigation, whether or not a criminal investigation has begun. Failure to comply with these requirements could lead to up to two years imprisonment.

Applying Recommendation 15

1258. Every person or entity subject to the Part I of the PCMLTFA, including DNFBPs, has to implement a compliance regime, *as far as practicable*, which means that, depending on the various size and activities of the reporting entities, a regime may be adapted. This includes the appointment of a person responsible for its implementation, the development and application of policies and procedures, a review of those procedures and policies to test their effectiveness by an internal or

[159] Legal counsel was removed from reporting obligations to FINTRAC in 2003.

external auditor or by the person or entity itself, *as often as necessary* and an ongoing compliance training program for the employees or agents (Section 71 of the PCMLTF Regulations, see Section 3.8 of the report)[160].

1259. Apart from the specific scope issues related to DNFBPs, the main deficiencies applicable to financial institutions apply also to DNFBPs, since the core obligations for both DNFBPs and financial institutions are based on the same general AML/CFT regime contained in the PCMLTF Regulations. The requirements to keep up to date internal procedures, that the policies include the detection of unusual and suspicious transactions and ensuring that the AML/CFT compliance officer has timely access to customer identification data and other CDD information, transactions records and other relevant information are only implicit. There is no mandatory requirement for an independent audit function to test AML/CFT regime compliance, even if certain provincial gambling Acts include such requirements. Measures exist in the casino industry to ensure the screening of key employees and employees with direct access to gaming facilities, so as to prevent criminals owning or controlling casinos. For some other categories of DNFBPs, there are entry requirements for the business or profession, but these do not amount to screening of employees as contemplated by R.15.

Applying Recommendation 21

1260. All reporting parties, including DNFBPs, received information from FINTRAC in relation to the NCCT process when that process was still under way (including the need to enhance the level of scrutiny in the case of counter-measures). However, there is no enforceable requirement to give special attention to transactions or business relationships connected with persons from or in countries which do not or insufficiently apply the FATF Recommendations, no effective measures in place whereby DNFBPs are advised of other countries that have specific weaknesses in their AML/CFT systems, and no requirement to examine the background and purpose of these transactions and to document the related findings.

4.2.2 Recommendations and Comments

1261. *Recommendation 13*. All DNFBPs as defined by the FATF should be subject in Canada to the suspicious transactions reporting requirement in all circumstances defined in Recommendation 16. The current incomplete coverage of certain DNFBPs has an impact on the effective implementation of the suspicious transactions report requirement. FINTRAC should address the issues raised by the low number of STRs provided by some non-financial professions (especially real estate agents and sales representatives and accountants).

1262. *Recommendation 15*. The current requirements should be expanded, specified and enforced, especially:

- The policies and procedures should be required to be written and their minimum mandatory content should include the detection of unusual and suspicious transactions for all DNFBPs.[161]
- There should be a requirement to ensure that the AML/CFT compliance officer has a timely access to customer identification data and other CDD information, transactions records and other relevant information.
- The requirement for an independent audit function (internal or external) to test on a regular basis the compliance of the AML regime should be strengthened.
- Canada should impose screening procedures when hiring employees to DNFBPs.

---

[160] The compliance regime requirements were expanded in regulations enacted in June 2007 which will come into force in June 23, 2008 (see Section 71 of the amended PCMLTF Regulations).

[161] Canada indicated thar the compliance regime requirements were expanded in regulations enacted in June 2007 which will come into force in June 23, 2008.

1263. *Recommendation 21*. The requirement to give special attention to business relationships or transactions with persons from or in countries which do not or insufficiently apply the FATF Recommendations should be included in an enforceable legal instrument applicable to DNFBPs. Effective measures should be put in place whereby DNFBPs are advised of other countries that have specific weaknesses in their AML/CFT systems. Finally a provision should be introduced requiring that the background and purpose of such transactions having no apparent economic or visible lawful purpose be examined and the findings documented.

4.2.3 Compliance with Recommendation 16

Rec.	Rating	Summary of factors underlying ratings
Rec.16	NC	*Scope issue* • Lawyers, Quebec Notaries, BC Notaries, dealers in precious metals and stones, Internet casinos, ship based casinos and TCSPs are not captured by the PCMLTFA and therefore are not subject to the suspicious transactions reporting requirements. *Application of Recommendation 13 to casinos, real estate brokers and sales representatives and accountants/accountant firms* • The circumstances in which real estate agents and sales representatives and accountants have to report suspicious transactions under the PCMLTFA are too limited. • Attempted transactions are not yet covered by the Suspicious Transaction Reporting requirement. • The relatively low numbers of STRs sent by real estate agents/sales representatives and accountants raise significant concerns in relation to the effectiveness of the reporting system in these sectors. *Application of Recommendation 15 to casinos, real estate brokers and sales representatives and accountants/accountant firms* • There is no explicit requirement to: (1) keep up to date internal procedures, (2) have policies to monitor for and detect unusual and suspicious transactions and (3) ensure that the AML/CFT compliance officer has timely access to customer identification data and other CDD information, transactions records and other relevant information. • There is no mandatory requirement for an independent audit function to test AML/CFT regime compliance. • Except for casinos, there are no requirements concerning screening procedures when hiring employees. *Application of Recommendation 21 to casinos, real estate brokers and sales representatives and accountants/accountant firms* • There is no general enforceable requirement for DNFBPs to give special attention to transactions or business relationships connected with persons from or in countries which do not or insufficiently apply the FATF Recommendations but only through general guidance or advisories sent on a case by case basis. • There are no effective measures in place whereby DNFBPs are advised of other countries that have specific weaknesses in their AML/CFT systems. • There is no requirement to examine the background and purpose of these transactions and to document the related findings.

4.3 Regulation, supervision and monitoring (R. 24-25)

4.3.1 Description and Analysis

Recommendation 24

1264. FINTRAC is responsible for ensuring that DNFBPs comply with their obligations under the PCMLTFA. In order to effectively use its powers to ensure compliance, FINTRAC has developed a comprehensive Compliance Program using a risk-based approach to ensuring compliance includes the development of comprehensive sector profiles and the active gathering of information on individual

reporting entities (see Section 3.10 of the report). However, given the very high number of persons or entities likely to be subject to the PCMLTFA as non-financial professions and the limited staff resources of FINTRAC dedicated to compliance, the assessment team is of view that FINTRAC is not in a position to ensure on its own an efficient monitoring of the effective application of AML/CFT legislation in these sectors. In these conditions, regulators and SROs have an important role to play to assist FINTRAC in ensuring compliance with the AML/CFT requirements.

1265. As already stated under Section 3.10 of the report, Subsections 65(2) and 65(3) of the PCMLTFA permit FINTRAC to exchange information with regulators for compliance purposes. As a result, FINTRAC works with regulators who, under their own powers, examine entities that are covered under the PCMLTFA. Information provided by these regulators to FINTRAC feeds into FINTRAC's risk assessment and assists FINTRAC to target the highest proportion of its compliance resources to the sectors and entities at highest risk for non-compliance. Where entities are covered by a regulator with a robust compliance program which includes examinations for issues related to compliance with the PCMLTFA (reporting, record-keeping, client identification, existence of a compliance regime), FINTRAC may decide to allocate fewer resources to examinations in that sector than in a sector that is not well regulated.

1266. Regarding DNFPBs, FINTRAC has currently entered only into 5 agreements with regulators of the gaming sector (see below). FINTRAC always reserves the right to examine the reporting entities covered by an MOU. For some regulators, if significant non-compliance is detected, they could issue sanctions under their respective legislation. In the case of other regulators, they will advise FINTRAC of the results and FINTRAC may complete an on-site examination of the reporting entity and take the appropriate action as necessary.

Casinos

General

1267. Under Section 207 of the Criminal Code, provinces have the responsibility to license, operate, and regulate legal forms of gaming, including the rules for gaming products and financial services available within the casinos. Gaming products include a wide variety of card games, roulette and slot machines. There are also a wide variety of financial services available at casinos, including some that resemble services provided by financial institutions. Depending on the province, casinos can open customer deposit or credit accounts, have facilities for transmitting and receiving funds transfers directly from other institutions, and offer cheque cashing and currency exchange services. These services are ancillary to their core activities, which is the sale and redemption of chips.

1268. Provinces permit the delivery of gaming services through one or a combination of the following operational models:

- *Commercial Casinos* – the province through a crown corporation or through service contracts with private corporations delivers gaming services at the casinos;
- *Charity casinos* – charities participate directly in the provision of the gaming activities at designated "charity" casinos or they are provided a direct grant from a fund generated from casino revenues;
- *First Nation Casinos* – based on either the charity or commercial casino models, First Nations operate casinos on First Nation land.

1269. The table below shows the distribution of casinos among categories and provinces.

Province	Commercial Casinos	Slots	Charity	First Nation	Seasonal	Total
Alberta	0	3	18	1	1	**23**
British Columbia	19	2	0	0	1	**22**
Manitoba	2	0	0	2	0	**4**
Nova Scotia	2	0	0	0	0	**2**
Ontario	4	17	5	1	2	**29**
Quebec	3	0	0	0	0	**3**
Saskatchewan	3	0	0	4	0	7
Yukon	1	0	0	0	0	1
TOTAL	**34**	**22**	**23**	**8**	**4**	**91**

1270. *Internet casinos*. Part VII of the *Criminal Code* makes it an offence to operate a commercial gaming enterprise. The two main exceptions to this prohibition are gambling activities conducted and managed by the province, or pursuant to a licence issued by the province. The *Criminal Code* does not contain any exceptions from the broad prohibition that would allow for the establishment of an Internet casino.

1271. Despite the legal prohibitions against online gaming, for a number of years the "Gaming Commission" of the Mohawk Territory of Kahnawake (Quebec) is hosting servers and has been issuing "licenses" for the operation of Internet gaming businesses. Licenses cost from CAD 5 000 to CAD 25 000 and it appears that there are now more than 400 "permit holders" operating Internet casino and gambling sites, with some reports suggesting that up to 60% of on-line casino gaming is passing through the Kahnawake based servers. In Canada, courts have explicitly rejected First Nations' claims to an inherent right to conduct gaming activities. The Quebec Minister of Public Security has spoken out against the operation of these online casinos, and in late 2007 one of the "licensees" that had offices in Montreal pled guilty to a charge of illegal gambling. However, no action has been taken against other "licensees". Despite this decision the Mohawks of Kahnawake continue to assert that they have jurisdiction to issue gaming licenses for gaming operations, and continue to host Internet casinos on their reserve.

1272. Having recognized the need to create a regulatory environment designed specifically for the interactive gaming industry, the Kahnawake community created the Kahnawake Gaming Commission which in turn enacted a "regulatory" framework for online gaming, under the "the Kahnawake Gaming Law" and the "Kahnawake Regulations Concerning Interactive Gaming". The measures were designed to ensure that all interactive gaming and gaming related activities conducted within, or from the Mohawk Territory of Kahnawake, satisfy three basic principles: (1) that only suitable persons and entities are permitted to operate within Kahnawake; (2) that the games offered are fair to the player; and (3) that winners are paid.

1273. However, these activities are not subject to AML/CFT regulations and Canada's federal and provincial governments are faced with substantial challenges in determining the appropriate course of action to be taken concerning Internet gambling. The industry has grown rapidly and huge revenues are generated. Canada must either enforce its prohibition effectively or introduce comprehensive AML/CFT regulation for the industry.

1274. *Cruise ships*. Cruise ships operate out of Canadian waters and do offer casino facilities (except within five nautical miles of a Canadian port). No AML/CFT measures apply to such casino gambling.

1275. Regarding the legal forms of casinos, the methods of licensing and registration depend on the operational model used. The measures in place to prevent criminals or their associates from holding or being the beneficial owner of a significant or controlling interest, holding a management function in, or being an operator of a casino are comprehensive (with the exception of Internet and ship based casinos).

Commercial Casinos

1276. Under section 207(1)(a) of the Criminal Code, provinces have the authority to operate gaming facilities or authorise a commission to operate gaming on their behalf. In practice, six provinces (British Columbia, Manitoba, Nova Scotia, Ontario, Québec, and Saskatchewan) have authorised casinos (including slot facilities) under section 207(1)(a) of the Criminal Code. Each has established a provincial gaming corporation to operate gaming within the province as described in the following table.

Province	Provincial Gaming Corporation
British Columbia	BC Lottery Corporation
Manitoba	Manitoba Lotteries Corporation
Nova Scotia	Nova Scotia Gaming Corporation
Ontario	Ontario Lottery and Gaming Corporation
Québec	Loto Québec
Saskatchewan	Saskatchewan Gaming Corporation

1277. In British Columbia, Nova Scotia and Ontario, the gaming corporations have contracted to private corporations to provide at least some of the day-to-day casino operations[162]. The contracts do not alleviate the crown corporations of their legal role of operator, as they are required to monitor the activities of the private corporations with whom they enter into contracts.

1278. To ensure the sound running of the casino industry, private gaming service providers must also disclose detailed corporate information to the provincial gaming regulator, including the structure, business relationships, and finances (including tax returns), as well as a documented history of criminal charges, civil proceedings, insolvency, gaming permits, and taxes.

1279. To ensure that criminals and their associates are unable to become involved in the casino industry, regulations under the provincial gaming legislation require that the following groups register with the regulator before becoming involved in gaming operations:

- The casino operator (private corporation).
- Executive members and key employees (*e.g.* the Chief Executive, Chief Financial, and Chief Operating Officers, floor managers, directors of security or any position that has direct gaming-related decision making responsibilities within the casino).
- And all other gaming employees (*e.g.* employees that have access to the casino floor or restricted areas of the casino as part of their regulator or continuing employment functions).

1280. An application for registration will be refused where there are reasonable grounds to believe that the applicant will not act as a supplier or gaming assistant in accordance with the law or with honesty and integrity. Suppliers are also required to meet high standards of financial responsibility.

1281. In assessing whether an applicant meets the requisite standards of honesty, integrity and financial responsibility, the applicant must disclose detailed information describing their past conduct, including work history, finances, criminal and civil proceedings, bankruptcies / insolvencies, as well as personal investments. In addition, information is required on interested persons of the applicant, including business partners, persons who have or may have a beneficial interest in the applicant's business, persons who exercise or may exercise direct or indirect control over the applicant's business, or persons who have or may have given direct or indirect financing to the applicant.

[162] The 17 slot facilities at racetracks (“racinos”) and 5 charity casinos in Ontario are operated by Ontario Lottery and Gaming Corporation while private corporations operate the four commercial casinos.

1282. On an ongoing basis, regulators must be notified if there is any change to the facility licensee's executive or key employees at the casino. Failure to disclose any changes to the regulator can result in sanctions, including the cancellation of registration and fine.

1283. The assessors were told that investigators from the provincial regulators undertake civil, criminal and credit history checks of individual registrants and conduct interviews with associates to ensure the information provided by a registrant is accurate. In cooperation with the RCMP, regulators query the Canadian Police Information Centre database for the disposition of charges for which a person had been fingerprinted (indicating they have a criminal record) and all outstanding charges currently before the courts. Local infraction checking is also conducted through any source that regulators deem appropriate.

1284. For corporations, investigators review the application information and evaluate the financial, business and criminal history of the corporation using information from international, national, provincial, state, county or municipal law enforcement or security agencies; police services and sheriff's offices; government ministries or regulatory agencies; banks, trust companies, brokerage houses, credit bureaus; professional or industry associations, licensing bodies or regulators; and former or current customers.

1285. The Provincial Gaming Corporations have developed corporate governance policies. For instance, the BC Lottery Corporation has corporate governance that refers to clearly defined processes with respect to the selection and composition of the board and senior management and the division of responsibilities, decision making and accountability among the Board, Senior Management and the Shareholder (Government of BC) to ensure the organization's short- and long-term success is consistent with its mandate and mission. The British Columbia Lottery Corporation practices and policies meet the Best Practice Guidelines on Governance and Disclosure for public sector organizations, which was issued by government in February 2005. The corporation has developed a Code of Conduct and Conflict of Interest Guidelines applicable to casinos' directors.

1286. In Manitoba, Québec and Saskatchewan, the crown corporations directly operate the commercial gaming facilities according to government and corporation standards, policies and procedures, including the establishment of new casino operations. Because they have been established to run the gaming in the provinces, they do not require gaming registrations or licenses. However, key gaming employees and gaming employees are required to register and must undergo a similar process as employees of private corporations. As well, Officers and Directors of the crown corporations are required to file a personal disclosure and are subject to a full background investigation prior to their involvement in gaming activities.

Charitable Casinos

1287. Under section 207(1)(b) of the Criminal Code, provinces have the authority to issue charitable gaming licenses to registered charities and religious organizations. Gaming takes place in established charity casinos operated by a private corporation in cooperation with the charity. Charity casinos are not allowed to operate without a participating charity.

1288. Of the 23 charity casinos operating in Canada, 17 are in Alberta. Religious and charity groups apply to the Alberta Gaming and Liquor Commission (AGLC) for 2-day[163] charitable gaming licences that allow the charity to assist in the operation of gaming at a casino. In return for their participation, charities receive a portion of the gaming proceeds to be used for an identified purpose.

1289. Private corporations own the charity casinos in Alberta. Each has a casino facility license with the AGLC that allows it to operate a gaming facility in conjunction with religious or charity group.

[163] Because licenses are only available for two-day events, compliance with the AML/CFT requirements under the PCMLTFA is the responsibility of the casino operator, not the charity.

The private corporation provides key operating personal including gaming employees, security and surveillance.

1290. Prior to obtaining a casino facility license, a corporation must undergo a multi-step screening process. The first step is providing the AGLC with an overview of the proposed casino. The AGLC then publicly advertises the proposal and solicits expressions of interest from other potential applicants to encourage the best possible proposal for a casino in a given market area. The ALGC evaluates the applications based on several factors, including financial footing of the applicant, proposed physical attributes and security features of the casino, and the applicant's understanding and compliance with relevant federal, provincial and municipal legislation and requirements.

1291. Once the market assessment is complete and the successful applicant is chosen, the AGLC will undertake a thorough due diligence investigation into the applicant and any other key persons associated with the applicant. According to the ALGC Casino Terms and Conditions and Operating Guidelines, the investigation is to ensure criminal interests, or those who otherwise would be a detriment to the integrity or lawful conduct of gaming in the province, are prevented from operating, having a financial interest in or having an association with a casino facility license. The ALGC can refuse to issue a casino facility license if they are not satisfied with the integrity of the applicants, individuals involved in the operation of the casino, or business associates, including the officers and directors of corporations controlled by the applicant, and their families. Part of the due diligence investigation on an applicant is a records check to determine whether anyone associated with the application has been charged or convicted with an offence under the Criminal Code, the Excise Act, the Food and Drugs Act or the Controlled Drugs and Substances Act.

1292. The Yukon uses a charity model similar to Alberta's and imposes the same stringent conditions. In Ontario's five "charity casinos", charities do not participate in the operation of casinos but are eligible to receive a percentage of the gaming proceeds from the designated casinos. The Ontario Lottery and Gaming Corporation, a crown corporation established by the province, owns and operates the charity casinos. Although considered charity casinos because of the fund raising component, Ontario's charity casinos are authorised under section 207(1)(a) of the Criminal Code.

First Nations Casinos

1293. First Nations casinos and slot facilities operate in Alberta, Manitoba, Ontario and Saskatchewan[164]. Subsection 35(1) of the Constitution Act, 1982, affirms and recognizes aboriginal rights in Canada. The Supreme Court of Canada in one ruling covering two cases R. v. Pamajewon and R. v. Gardiner Pitchenese and Gardiner (1996), 138 D.L.R. (4th) 204, ruled that gaming (or the regulation of gaming) was not integral to the cultures of the two First Nations claimants at the time of first European contact, which is the test for a claimed aboriginal right. As a result, the First Nations involved in the cases did not have the inherent right to regulate gambling on Indian reserves. Provincial legislation governs the operation of casinos on First Nation land. All First Nations casinos operate under either the charity model or the commercial model and are required to comply with the registration requirements of these models.

Compliance Risk Assessment and Examinations

1294. As of September 30, 2006, FINTRAC had conducted a total of 12 examinations in the commercial casino sector as follows:

[164] In Saskatchewan, First Nation gaming is conducted through an agreement between the provincial government and the Federation of Saskatchewan Indian Nations (FSIN). FSIN formed the Saskatchewan Indian Gaming Authority (SIGA) to operate the casino on its behalf.

FINTRAC Examinations Conducted in Casinos

	2004-05	2005-06	2006-07 (as of end Q2)	Total
Casinos	5	5	2	**12**

1295. As of the end of 2005-2006, the assessors were told that it had also sent 83 questionnaires regarding the implementation of an AML/CFT compliance regime (CQs) to reporting entities in the casino sector, all of which were returned, with globally high rates of positive responses to questions about key compliance elements.

1296. Moreover, to date, FINTRAC has signed five agreements with regulators having supervisory authority over casinos (see table below). Under these MOUs, the assessors were told that FINTRAC and these regulators regularly exchange statistics, risk assessment information, examination results, and examination plans.

Signed MOUs with Casino Regulators (to date)		
1	British Columbia Gaming Policy and Enforcement Branch (GPEB)	July 9, 2004
2	Saskatchewan Liquor and Gaming Authority (SLGA)	November 16, 2004
3	Alberta Gaming and Liquor Commission (AGLC)	December 20, 2004
4	Alcohol and Gaming Commission of Ontario (AGCO)	December 21, 2004
5	Nova Scotia Alcohol and Gaming Authority (NSAGA)	May 6, 2005

1297. These MOU partners had conducted additional 38 examinations in reporting entities for the fiscal years 2005-2006 and 2006-2007 (as of September 30, 2006). These examinations were not systematically dedicated to audit compliance with the PCMLTFA requirements.

Role of Provincial Regulators

1298. In addition to requirements under the PCMLTFA, casinos must comply with the provincial gaming legislation and regulations.

1299. Provincial gaming legislation imposes requirements on gaming service providers and gaming employees to ensure the integrity of the industry. These requirements include mandatory registration, internal control systems, and security and surveillance systems, gaming rules and permitted financial transaction. The legislation also identifies the regulator responsible for the administration of the legislation. The following table identifies the provincial regulator and the key gaming legislation within each province.

Province	Regulator	Primary Gaming Legislation
Alberta	Alberta Gaming and Liquor Commission	*Gaming and Liquor Act*
British Columbia	Gaming Policy and Enforcement Branch,	*Gaming Control Act*
Manitoba	Manitoba Gaming Control Commission	*Gaming Control Act*
Nova Scotia	Nova Scotia Alcohol and Gaming Authority	*Gaming Control Act*
Ontario	Alcohol and Gaming Commission of Ontario	*Gaming Control Act*
Québec	Loto Québec	*An Act Respecting Lotteries, Publicity Contests And Amusement Machines*
Saskatchewan	Saskatchewan Liquor and Gaming Authority	*The Alcohol and Gaming Regulation Act*

1300. Beyond the requirements in the PCMLTFA, most provinces have adopted AML/CFT measures into internal control procedures or provincial gaming legislation, which then become the responsibility of the provincial regulator to enforce, including:

Alberta

• Reporting large, suspicious, and large currency exchange transactions to FINTRAC; • Record-keeping of large cash and suspicious transactions; • Implementation of a compliance regime.	Section 5.9 of Alberta Casino Terms and Conditions and Operating Guidelines

British Columbia

• Reporting *Criminal Code* violations to the provincial regulator (which includes money laundering, possession of proceeds of crime and terrorist financing).	Section 86 of *BC Gaming Control Act*

Nova Scotia

• ID and record-keeping requirements for large cash transactions.	Section 248 of NS Casino Regulations

Ontario

• ID and record-keeping requirements for large cash transactions. • Record-keeping requirement for tracking multiple transactions of CAD 2 500 to an aggregate of CAD 10 000. • Compliance regime • Internal controls for AML/CFT requirements	Section 24, 27 and 28, Ontario Regulation 385/99 under the *Ontario Gaming Control Act*.

Saskatchewan

• Requirement for the Saskatchewan Gaming Corporation to maintain written procedures on recording large cash transactions.	Section 17 of the Saskatchewan Gaming Corporation Casino Regulations

1301. To ensure that casinos are complying with provincial gaming legislation, terms and conditions of registrations and internal control policies, regulators conduct regular and unscheduled audits, compliance reviews and investigate any alleged offences.

1302. The assessors were told that regulators perform audits at least annually to review the financial and reporting records, operating procedures and security systems in place. In addition, regulators conduct interviews with gaming employees to ensure they are familiar with all relevant legislation. Some provinces audit specifically for compliance with PCMLTFA. For example, British Columbia and Ontario have developed a module through which it determines compliance with all of the requirements for casinos under the PCMLTFA.

1303. When minor non-compliance issues are identified, the regulator will work with the casino to resolve the issue. However, when more significant non-compliance issues such as violations to a provincial gaming act are discovered, the regulator undertakes an investigation.

1304. Each province has established an investigative unit within its regulator. These units usually include former or active law enforcement officers with significant expertise in gaming and proceeds of crime investigations. Investigators work cooperatively with the gaming industry, other gaming agencies, law enforcement and other regulatory bodies to identify unlawful activity, and conduct timely and thorough investigations.

1305. Investigators are responsible for the investigation of gaming related complaints and allegations of illegal behaviour and will recommend charges relating to provincial gaming legislation. Law enforcement officials (either RCMP or municipal police forces), in cooperation and with the assistance of the investigative unit, will investigate and lay charges relating to offences found in the Criminal Code.

1306. In Ontario, for instance, the Casino Enforcement Unit provides 24-hour Ontario Provincial Police coverage in the casinos, and is responsible for conducting criminal investigations in relation to gaming inside the casino. The members of this unit liaise with casino security and surveillance staff and with the local police service according to formal protocol agreements. In addition, there are

Compliance Inspectors on-site at the casinos, who are responsible for monitoring the casino for compliance with the approved policies, procedures and internal controls.

1307. If an investigation concludes that there was a violation of the condition of licence or registration, regulators have the authority to impose administrative sanctions and prosecution.

1308. Administrative sanctions may include a warning; refusal to issue or renew a license; suspension or cancellation of a license; imposition of conditions on a license; the imposition of a fine; or other administrative settlements. Regulators can apply additional monetary or other penalties for offences that are contrary to provincial gaming legislation or the Criminal Code. Regulatory or criminal infractions may also result in administrative sanctions, including the cancellation of registration.

1309. In conclusion, casinos in Canada, except for Internet and ship based casinos, are globally subject to a reasonably comprehensive regulatory and supervisory regime. However, it is difficult to express a global opinion regarding the adequacy and effectiveness of the AML/CFT compliance supervision as it may vary a lot from one province to another. While FINTRAC is in principle the sole regulator of casinos for AML/CFT, based on a risk-based approach, the quality of supervision may nevertheless vary from one casino to another depending on whether its provincial supervisor has signed an MOU or not with FINTRAC and whether it performs or not controls in that area. As the provincial regulators are not directly responsible for ensuring compliance with PCMLTFA, their involvement in AML/CFT activities is unequal: some of them, like Alberta or Ontario have incorporated in their own regulatory framework detailed AML/CFT rules, covering most or all of the PCMLTFA requirements, while others, like Manitoba have not included such rules in their compliance program. The methodology and the frequency of examinations may also differ: Saskatchewan Liquor and Gaming Authority, for instance, has no AML/CFT compliance assessment methodology, while Alberta Gaming, Liquor Commission and Alcohol and Gaming Commission of Ontario perform regular and detailed audits. Moreover, the assessment team was not provided with any data or statistics regarding possible sanctions taken by these regulators on the ground of AML/CFT non-compliance issues.

Other DNFBPs covered by the PCMLTFA

1310. Due to the large number of potential entities within the accountants and real estate sectors (in total, about 146 000 accountants and accounting firms and 100,000 licensed real estate agents could be covered under the PCMLTFA if they perform certain activities), FINTRAC is not in a position to monitor closely their compliance with PCMLTFA requirements, even if a large majority of these persons or entities are not actually concerned (as they are not engaged in the specific activities covered by the requirements) and despite the risk-based approach for compliance adopted by FINTRAC.

1311. FINTRAC's compliance program makes use of risk management strategies to identify those reporting entities most in need of improving compliance (see comments below). In order to assist FINTRAC's Compliance team in assessing the risk of non-compliance within particular entities, almost 3 000 CQ had been sent, as of the end of 2005-06, to reporting entities in the accountants and real estate sectors. A further 1 500 have been forwarded to the accountants sector in early fiscal 2006/07, and an additional 1 500 are planned for the real estate sector later in the fiscal year.

1312. Due to the potentially large number of entities within the accountants and real estate sectors and high turnover, continued awareness raising campaigns/outreach are required to ensure obligations are understood. It should be noted that FINTRAC is committed to ongoing outreach with these sectors. As of the end of September 2006 FINTRAC had conducted 139 outreach meetings/presentations with the accounting sector with nearly 2200 participants and 272 meetings/presentations with the real estate sector, with more than 15 000 participants). However, the response rates to Compliance Questionnaires remains relatively low for accountants (75%) and real estate brokers (63%), compared to 89% for financial institutions and 100% for casinos.

1313. The results measured by the positive responses regarding compliance regime are somewhat lower than those for financial institutions or casinos: for instance, only 58% of responding accountants have declared having implemented a compliance regime and 34% an ongoing compliance training program in their entity. This can be partially explained by the fact that, for example, a number of accountants receiving a CQ are not engaged in any of the activities covered under the PCMLTFA (such as receiving or paying funds; purchasing or selling securities, real estate, business assets or entities; or, transferring funds or securities).

1314. As of September 30, 2006, FINTRAC had conducted a total of 26 examinations in the accounting sector, and a total of 95 examinations in the real estate sector. The assessment team was not given any detailed information about the results of these examinations.

	2004-05	2005-06	2006-07 (as of end Q2)	Total
Accountants	0	19	7	26
Real Estate	9	52	34	95

1315. Quite obviously, such a limited number of on-site examinations made by FINTRAC compared with the number of potential reporting entities cannot be considered as sufficient to ensure an effective monitoring of compliance even if FINTRAC targets its examinations based on a comprehensive risk assessment. It should be completed by interventions of provincial regulators or SROs. However, these institutions are not in charge of ensuring AML/CFT compliance and, as for the other sectors examined above, their level of involvement in that area, the regulatory basis on which they rely and the methodology adopted may strongly differ from one province or sector to another.

Provincial Regulation of DNFBPs

Accountants

1316. As mentioned earlier in the report, there are three designations of accountants, all of whom are represented by a national association: Canadian Institute of Chartered Accountants (CICA), Certified General Accountants Association of Canada (CGA) and the Society of Management Accountants of Canada (CMA). It is the role of the provincial institutes and associations to ensure that accountants are complying with the rules of professional conduct and corresponding by-laws to ensure that accountants are protecting the public interest.

1317. *Canadian Institute of Chartered Accountants*. For the purpose of outlining the monitoring and supervisory regime, focus will be placed on CICA, the group of accountants with the most likelihood of undertaking the types of financial transactions covered by the PCMLTFA.

1318. The CICA has developed a Guide (originally published in 2002 and updated in 2004) to assist CAs and CA firms in understanding the obligations imposed by the PCMLTFA. It indicates that CAs should be mindful of the possibility of money laundering and risks of becoming a party to the offence by failing to take the appropriate action. Early in 2006, the CICA established an Anti-money laundering advisory Committee whose objectives are to provide advice to Department of Finance on proposed changes to AML regime and to provide advice to CICA staff for updating the 2004 Guide. It is currently elaborating detailed guidance regarding the activities which should be considered as covered by the AML/CFT regime. Rules of professional conduct specifically address “unlawful activity” and establish the minimum level of ethical conduct for accountants.

1319. Provincial institutes of Chartered Accountants work in partnership to develop and enforce national standards, which are not relating specifically to money laundering but are designed to protect the public interest and maintain the good reputation and integrity of the CA profession. To help ensure that accountants are complying with the rules of professional conduct, provincial institutes undertake inspections of all members in public practice.

1320. Each year, approximately 25% of all firms in private practice are inspected. The selection of firms is made on an ongoing, cyclical, basis. New firms are selected within the first year of operation while other offices are normally selected every four years from the date of their last inspection. The inspection primarily focuses on the firm's quality control system and a review of current engagement files and related financial statements in order to assess adherence to professional standards. If inspection reveals significant shortcomings, the matter is referred to the professional conduct committee.

1321. After assessment, the committee may conclude that a breach of the rules of professional conduct has taken place and a charge or charges should be laid. In this event a formal hearing is held before the CICA discipline committee. The discipline committee has the authority to summon witnesses and require the production of evidence relevant to the case. The discipline committee has the power to impose administrative fines; suspend or expel a member; restrict a firm's practice; and publicize the decision of the committee. All cases that result in a finding of guilty of professional misconduct are made publicly available on provincial institutes' websites. Details of cases are made available to law enforcement authorities to assist in their investigation. No further information was provided to the assessment team on actions taken in relation to non-compliance with AML/CFT obligations.

1322. In addition to the role of the provincial accounting institutes and associations, the Canadian Public Accountability Board (CPAB) plays an oversight role of its member firms to ensure the integrity of financial reporting of publicly listed companies by promoting high quality, independent auditing. CPAB conducts inspections of public accounting firms that audit publicly listed companies to ensure compliance with professional standards and participation requirements. Firms with 50 or more clients that are publicly listed companies are inspected annually while those with less than 50 will be inspected on a three-year cycle. CPAB has entered into MOUs with the provincial accounting oversight bodies under which those institutes will inspect the smaller firms on behalf of CPAB. Where appropriate, CPAB imposes sanctions and restrictions on public accounting firms that publicly listed companies and, where necessary require remedial action, including referring matters to provincial accounting organizations for discipline purposes or to securities regulators.

1323. *General Accountants Association of Canada*. The Certified General Accountants Association of Canada has developed a Code of ethical principles and rules of conduct designed to protect the public and ensure that CGAs maintain the highest ethical standards. Specific provisions prohibit members from participating in or providing services to any activity that the member knows or which a reasonably prudent person would believe to be unlawful.

1324. Provincial associations have adopted the Canadian Association's standards of conduct contained in the Code of ethical principles and rules of conduct. In the case of breach of professional conduct as defined by the Code, members are subject to disciplinary action through the member's Provincial association or Ordre professionnel. Every registered public practitioner is required to have a peer review or audit at least every three years and to have a Policies and procedures Manual.

Real Estate Agents

1325. *General*. In addition to AML/CFT compliance supervision by FINTRAC, real estate agents are subject to monitoring by provincial regulators to ensure compliance with the provincial real estate legislation. In addition, real estate agents have industry associations that represent them at the local, provincial and federal levels. The associations also provide awareness and information on AML/CFT requirements for the real estate industry through training and workshops. The following section describes the compliance and oversight activities of the provincial regulators and the industry associations in the real estate industry.

1326. *Regulators*. Provinces are responsible for the regulation of real estate industry professionals. Provincial real estate legislation establishes the regulatory function within an agency or council in seven provinces (Alberta, British Columbia, Newfoundland and Labrador, Nova Scotia, Ontario,

Québec and Saskatchewan). In the other six provinces and territories (Manitoba, New Brunswick, Prince Edward Island, Northwest Territories, Yukon Territories and Nunavut), the government performs these activities directly.

1327. The responsibility of the regulator includes licensing of professionals (including admission exams and education requirements); setting and enforcing standards of conduct and business practices; and administering the provincial real estate acts and the bylaws and rules that have been established by the provincial regulating body.

1328. *Audit and investigation*. To ensure that real estate agents are complying with their requirements under provincial real estate legislation, regulators in Alberta, British Columbia, Nova Scotia, Ontario, Québec and Saskatchewan use a risk-based approach to determine which firms are selected for audit. In determining risk provinces include factors such as the size and location of the firm, deficiencies in accountant reports and previous audits and the amount of trust monies held. In addition, the regulator chooses some firms on a random basis for audit.

1329. Regulators provide courtesy audits to new brokers. A courtesy audit is an educational resource to ensure that new brokers are aware of the provisions of provincial real estate legislation as it applies to brokerage accounting. During the process, an auditor reviews the agent's books and records and provides assistance to make appropriate changes.

1330. During the audit, the auditor may review books and records, policies and procedures, trust and other account details and samples of open and closed files. Firms are required to keep records for a minimum of three years. Serious concerns discovered during an audit are forwarded to an investigation unit. Investigators determine whether there has been conduct that deserves sanction. Investigators have the power to collect all evidence relevant to the investigation, including interviews with the complainant and the industry member. The investigator has the authority to inspect or examine the books, documents and accounts (including the trust accounts) of any broker. In addition, industry members are required by the provincial real estate acts to cooperate with investigations, including responding to questions and providing requested documentation. If evidence of criminal activity is obtained during an investigation, it can be forwarded to law enforcement for a criminal investigation.

1331. Following an investigation, the regulator has the power to impose sanctions, including administrative penalties; suspension of the license to practice; and prosecution in the courts. It is worth noting that in provinces where the regulator does not conduct regular audits, each firm is required to submit reports from a public accountant verifying that transactions and accounts are being managed in accordance with provincial legislations.

1332. The assessment team did no get evidences that such audits and investigations are dedicated to check compliance with the AML/CFT requirements.

Dealers in Precious Metals and Stones

1333. Dealers in precious metals and stones do not have an established regulator. The Jewellers Vigilance Canada (JVC) has established a code of ethics and standards of practice to guide the professional behaviour of jewellers. Although it does not play an enforcement function, Jewellers Vigilance Canada provides members information and training on AML/CFT issues and has developed a crime prevention training package for members of the jewellery industry. In addition, Jewellers Vigilance Canada works closely with the RCMP to provide them educational support on the jewellery industry and information pertaining to specific crime. JVC also works closely with the Department of Finance on the new regulations covering the sector.

Lawyers and BC Notaries

Legal Counsel

1334. *General.* As described in Section 1.3, access to the profession and professional conduct for legal counsel is regulated and supervised at the provincial/territorial level of government through self-regulatory organizations (SRO). Each SRO is empowered through provincial/territorial legislation to regulate the profession to ensure a competent and ethical bar and authorises the SRO to educate, license and regulate the conduct, capacity and competence of legal counsel. Only members of an SRO can practice law in a given jurisdiction.

1335. There are nine provinces and three territories governed by the common law tradition and each jurisdiction has separately empowered SROs (law societies). The province of Québec follows the civil law tradition and has two separate SROs for the legal profession, the Barreau du Québec and the Chambres des notaires du Québec.

1336. Due to the differences between the civil and common law traditions, only notaries in Québec provide legal advice and are thus considered legal counsel. In the common law provinces, except British Columbia, licensed legal counsel only provide notary services. In British Columbia, a separate self-regulatory organization licenses 332 individuals to provide notary services and supervises the profession. These notaries are not considered legal counsel and the protections afforded under solicitor-client privilege do not apply.

1337. Legal counsel in Canada can be a member of multiple jurisdictions. In doing so, they must abide by the rules and conditions placed on them by the law society of that province/territory. In addition, each law society is a member of the Federation of Law Societies of Canada, the national coordinating body. In total the 14 SROs regulate Canada's lawyers and notaries.

1338. SRO by-laws and Rules of Professional Conduct set out the professional and ethical obligations for their members, including conduct and procedures relating to trust accounts and cash prohibition. Members failing to meet these obligations are subject to the SRO's disciplinary process. Each SRO has procedures and resources for dealing with professional misconduct and for taking action when appropriate. The SROs have the authority to impose fines, suspend the member from practicing, impose conditions on the member's practice and in serious cases, disbar the member.

1339. Each provincial and territorial law society, including both SROs in Québec, have implemented rules of professional conduct that prohibit legal counsel from accepting CAD 7 500 or more in cash in connection with a single client file or matter. This in essence limits the ability of criminals to place cash into the financial system through legal counsel. These rules are binding on the profession and enforceable by each provincial/territorial SRO. The SROs have incorporated the compliance examination of the cash prohibition rule into their standard compliance procedures pertaining to trust accounts. The standard compliance procedures include the use of an annual attestation by members indicating that they have not accepted cash of CAD 7 500 or more as well as spot and random audits of members' files and trust account statements. While the frequency of full audit varies amongst SROs, generally, each legal counsel undergoes an audit of their practice every three years, with every legal counsel being required to file annual reports to the appropriate law society. The cash prohibition rule has only been fully implemented in all jurisdictions since March 20006 and thus at the time of publication of the MEQ has not yet been subject to an annual report in all jurisdictions.

1340. There is no AML/CFT supervision *per se* as far as legal counsel is concerned.

British Columbia Notaries

1341. As indicated above, notaries in the province of British Columbia are supervised and regulated by a separate SRO. They are not considered legal counsel. The profession is governed by the British

Columbia Notaries Act, however, for the purposes of AML/CFT requirements, there is no authority for monitoring and ensuring compliance of BC notaries[165].

Recommendation 25 (Guidance for DNFBPs other than guidance on STRs)

1342. Guidance available to casinos, real estate agents/sale representatives and accountants is generally comprehensive and rather detailed.

1343. *Guidance for casinos, real estate agents/sale representatives and accountants*. FINTRAC provides casinos, real estate brokers and sales representatives, and accountants with specific guidance concerning the implementation of a compliance regime (Guideline 4), and record keeping and client identification (Guideline 6).

1344. FINTRAC has also developed a number of other resources to assist reporting entities in understanding their obligations under the PCMLTFA. These include Sector Specific Information Sheets and various pamphlets, which can be found on FINTRAC's website. Furthermore, a nine-minute video was produced to inform reporting entities of their legal obligations and helps explain FINTRAC's role. The video is accessible on FINTRAC's website and has also been distributed to reporting entities on DVD.

1345. Finally, FINTRAC also directs the operations of a call centre and a toll-free telephone line to serve the public and reporting entities. The service is available for 12 hours each day, from Monday to Friday.

1346. In addition to the guidance provided by FINTRAC, the industry associations and regulators in some provinces also provide AML/CFT guidance to their members.

1347. *Guidance for accountants*. As described above, CICA has developed a guidance document to assist CAs in their understanding of the requirements under the PCMLTFA and to outline the responsibilities of CAs flowing from those requirements. Ongoing money laundering information is provided through the CICA monthly magazine sent to all members called the CA Magazine. Articles inform members of ongoing changes to legislation, report on recent money laundering conferences and training, and inform on trends and cases.

1348. *Guidance for real estate agents*. Real estate industry associations at the local, provincial and federal levels provide members with significant guidance on their AML/CFT requirements under the PCMLTFA. The Canadian Real Estate Association (CREA) is comprised of provincial real estate associations and local boards throughout the country and is concerned with improving real estate practices across Canada. A key focus of CREA's activities is to educate members on federal issues, including providing awareness and requirements of real estate professionals on AML/CFT issues.

1349. In addressing this, CREA has developed an AML/CFT Internet site for members of the real estate industry called "*the Canadian Real Estate Money Laundering Compliance Centre*". Through this site, real estate agents (brokers and sales representatives) have access to online training, the procedures that real estate agents must have in place to be compliant with the PCMLTFA, as well as direct access to FINTRAC large cash, suspicious and terrorist property reporting forms.

1350. Continuous learning is a requirement of maintaining a real estate license in most provinces. To meet this requirement, provincial real estate associations have made available courses on money laundering that give real estate agents an awareness of the susceptibilities of the industry and their requirements under the PCMLTFA. In addition, a component of the required course to obtain a real estate license focuses on money laundering. Local boards work closely with local agents and promote the training available from the federal and provincial associations. In addition, local boards organize

[165] Canada indicated that BC Notaries are covered by regulations enacted in December 2007 and coming into force in December 2008.

discussions and presentations on topics of interest to their members. For example, the Ottawa Real Estate Board arranged for the RCMP and FINTRAC to give presentations to better inform members of their requirements under the PCMLTFA.

1351. *Other initiatives*. In order to provide advice and assistance to, as well as maintain relationships with the 91 casinos, FINTRAC has had 73 meetings with the majority of the reporting entities from that sector since 2004/2005. These meetings, in a number of cases, would have involved more than one reporting entity. These meetings and presentations are with, or are attended by, all levels of the organization in question. A total of 542 casinos' employees attended these meetings.

1352. In order to provide advice and assistance and maintain relationships with accountants and real estate brokers, FINTRAC had 411 meetings with these sectors since 2004/2005. 2 186 accountants and 15 316 real estate agents attended these meetings.

4.3.2 Recommendations and Comments

1353. *Recommendation 24*. Canada should ensure that supervisory action (especially on-site examinations) vis-à-vis casinos, but more importantly with respect to all other DNFBPs is strongly reinforced. The role, functions and monitoring powers of other regulators and SROs in ensuring compliance of DNFBPs with the AML/CFT requirements should be clarified. Canada should consider revisiting the supervision issue as a whole and give further consideration on whether FINTRAC should be the only authority in charge of ensuring compliance with the AML/CFT requirements (see conclusions in Section 3.10 of the report). The Department of Finance or FINTRAC should collect detailed information about the AML/CFT regulation and supervision role and action of all the provincial regulators/SROs in order to get a complete overview of the current situation.

1354. The sanction regimes applicable to DNFBPs, including casinos, should be reinforced and Canada should ensure that the sanctions available for failures to apply AML/CFT requirements are effective, proportionate and dissuasive.

4.3.3 Compliance with Recommendations 24 & 25

Rec.	Rating	Summary of factors underlying ratings
Rec.24	NC	*Scope issue* • Lawyers, Quebec Notaries, BC Notaries, dealers in precious metals and stones, Internet casinos, ship based casinos and TCSPs are not captured by the PCMLTFA and not subject to FINTRAC supervision. *Supervision of casinos* • The sanction regime available to FINTRAC is currently inadequate (see conclusions in relation to Rec. 17). Provincial regulators may have administrative sanctions at their disposal but there is no evidence that these are dissuasive, effective and proportionate, since no data or statistics regarding sanctions taken by these regulators on the grounds of AML/CFT non-compliance issues have been made available to the assessment team. *Supervision of other DNFBPs* • Limited staff resources deprives FINTRAC from closely and efficiently monitoring DNFBPs' compliance with the PCMLTFA requirements especially in sectors/provinces where the primary regulators or SROs are not or insufficiently involved in AML/CFT compliance supervision. • The sanction regime available to FINTRAC is currently inadequate (see conclusions in relation to Rec. 17). Provincial regulators may have administrative sanctions at their disposal but there is no evidence that these are dissuasive, effective and proportionate, since no data or statistics regarding sanctions taken by these regulators on the ground of AML/CFT non-compliance issues have been made available to the assessment team.
Rec.25	LC	• Lack of sufficiently sector-tailored guidance - see factors in Sections 3.7 & 3.10 of the report.

4.4 Other non-financial businesses and professions – Modern secure transaction techniques (R.20)

4.4.1 Description and Analysis

Considering applying AML regime to other non-financial businesses and professions at risk of being misused for ML

1355. As part of the development of the amendments to the PCMLTFA and in preparation of the Government of Canada June 2005 Consultation Paper, research and analysis was conducted on the domestic money laundering and terrorist financing risks and the operational feasibility of expanding the coverage of the Act to other non-financial businesses and professionals that are not explicitly subject to the FATF Recommendations.

1356. A number of new sectors were discussed, including auto dealers and auction houses. They have been targeted for further examination and ongoing monitoring. A lack of perceived risk led the Government to conclude that the application of PCMLTFA measures to these sectors was not warranted at this time.

"White label" automated banking machines

1357. White label ATMs in Canada provide alternative source of cash dispensing vis-à-vis traditional ATMs owned and operated by banks, other financial institutions and cash back debit services offered by retailers at the point of sale. In Canada, most deposit taking financial institutions have their own branded ATMs located throughout the country. These ATMs prominently display the logo of the financial institutions. A "white label" or no name ATM, which are usually located in non-traditional places (bars, shops, etc.), while branded, display no major financial institution labels on the actual ATM. After 1997, independent operators were allowed to operate ATMs, not owned by major financial institutions. In 2006, a little more than half of the 51 000 ATMs in operation in Canada were "white label".

1358. White-label ATMs are owned and operated by non-financial institutions. They are not under federal jurisdiction because they are not considered as financial institutions. However, concerns have been raised due to the unregulated nature of the business and the fact that the white label owner or operator can load these machines himself, thus creating an opportunity to "place" illicit cash into the financial system.

1359. Interac is the organization responsible for the development and operation of a national network of two shared electronic financial services: Shared Cash Dispensing at automated banking machines and Interac Direct Payment ("IDP"), Canada's national debit service. In June 1996, the Competition Tribunal ordered that Interac must broaden its membership to non-financial institutions and allow these non-financial corporations to deploy automated teller machines (ATMs).

1360. The Government's approach to date has been to rely on safeguards put in place by the Interac Association and on financial institutions holding the settlement account of the owner of the ATMs. When a small or unknown corporation applies for membership, Interac carries out corporate and other searches (*e.g.* background and bankruptcy checks). In 2003, Interac amended its regulations in order to enhance the safety and soundness of the network and assure the integrity of its system. The regulations increased due diligence requirements for all financial and non-financial organisations involved in the delivery of Interac services and strengthened inventory control procedures for ATMs and point-of-sale terminals. The regulations emphasized Interac members' accountability and responsibility for all their downstream business partners in order to address fraudulent attacks against their systems. Interac has developed new measures in the following areas:

- *New member process*: changes to the new member process to include an enhanced review of the business plans and enhanced background searches.
- *Regulations governing acquirers*: acquirers provide access to the Interac network and process ATM transactions for White Labels. Acquirers are required to conduct due diligence tests on business partners with whom they have a direct business relationship, such as independent sales organizations. Acquirers will have to actively monitor ATMs for fraudulent activity.

1361. However, there is currently no supervision of the acquirers themselves: the Shared Cash Dispensing service is built on a decentralized model with the individual members wholly responsible for their own business and their performance. Regulation and requirements regarding the monitoring of transactions by a third party (in order, for instance, to detect atypical profiles of transactions on certain ATMs such as withdrawals significantly above the norm in volume or value , or at atypical times, cash replenishments by the owner non consistent with his activity etc.) should be implemented.

1362. The assessors were told that the Department of Finance, the RCMP, FINTRAC and Interac continue to examine the AML/CFT risks created by white label machines and measures to address these risks. Measures could include a prohibition on self-loading and self-servicing of the ATM, and/or requiring a source of funds declaration from machine owners. The industry is committed to addressing any ML related risks and recognises that any gap poses a reputation risk. In addition, there is a clear recognition from the industry that these risks need to be addressed whether by industry or regulatory solutions. Possible measures contemplated include enhanced due diligence requirements on acquirers, including the requirement to obtain more information from the machine owner or operator, such as the source of funds, enhanced record-keeping (bearing in mind that every transaction from every machine is recorded and kept by the acquirer for a minimum of 7 years in order to comply with tax laws) and compliance enforcement.

1363. The legislative framework currently in place provides certain safeguards. For instance, the Minister of Finance has the authority under the Canadian Payments Act to designate and oversee a payment system, if it is in the public interest to do so. When a system is designated, the Canadian Payments Act requires that a copy of every rule be sent to the Minister of Finance and gives the Minister of Finance the power to disallow the whole or a part of a rule, as well as the power to issue guidelines and directives. In determining whether a system should be designated, a number of factors are considered, including the safety, efficiency, competitiveness and the best interests of the financial system. Further work needs to be done to address the risks of ML and TF with the industry. The risk issues are being addressed through further discussions with the industry.

1364. The assessment team believes that the current measures do not adequately address the risks and that it is important that the authorities undertake further action, possibly with the objective of introducing a registration and monitoring system for the owners of the ATMs.

Stored Value Cards

1365. Another new trend that is currently monitored is the use of stored value cards. An increasing number of these cards are put in circulation by certain financial institutions and a growing number of retailers. The assessment team was told that there is anecdotal evidence that stored value cards have been used to carry funds into and out of Canada.

1366. *Requirements of financial services provided via the Internet*

1367. Internet payments are an emerging area in Canada, with the largest industry player being PayPal. Finance is currently involved in discussions with PayPal and other Internet Payment Processors (IPPs) in an effort to better understand their business models and determine where the transactions are domiciled, who their client base are and whether the services offered by IPPs to Canadians carry money laundering and terrorist financing risks. In addition, Finance commissioned a research study by an outside consultant on this issue and is reviewing the findings of that study.

Real estate developers

1368. The sales of new homes or buildings are covered by the PCMLTFA and its regulations to the extent that home builders rely on a real estate broker or sales representative to sell the property. However, many real estate developers use an in-house employee to conduct the same work. The purchase of a new property often involves progress payments over the construction of the house or building, which offers criminals opportunities to place illicit funds in the system[166].

Reducing reliance on cash and secure automated transfer systems

1369. Canada's clearing and settlement system is secure and efficient, enabling consumers and businesses to make and receive payments and transfer funds throughout the country quickly and reliably. This has fostered a greater reliance and early adoption of non-cash payment mechanisms.

1370. The Canadian Payments Association operates national clearing and settlement systems that facilitate this flow of funds and mitigate risk to payment system participants. Its membership consists of financial institutions, which are reporting entities under the PCMLTFA.

1371. The Canadian Payments Act sets out the legal framework for the Canadian Payments Association, including its mandate, the types of organizations that are eligible for membership, the role of the Board of Directors and oversight responsibilities for the Minister of Finance. A key element of the Canadian Payments Association's mandate is facilitating the development of new payment methods and technologies.

1372. On average, some 20.6 million non-cash payment items, representing CAD 164 billion in transactions, were cleared and settled through the Canadian Payments Association's Automated Clearing Settlement System and Large Value Transfer System each business day during 2005. These include cheques, wire transfers, direct deposits, pre-authorised debits, bill payments and point-of-sale debits.

1373. Canadians have been early adopters of new banking technologies. Since the launch in 1986 of the Interac Association, the operator of the national debit card network, Canadians have been one of the highest per capita users worldwide of debit cards. According to the Bank for International Settlements, Canadians made 3.1 billion debit card transactions in 2005, or 95 transactions per person, worth over CAD 137.5 billion.

1374. MasterCard and Visa operate the principal credit card networks in Canada. In 2005, Canadians made 1.9 billion credit card transactions, or 60 transactions per person, worth CAD 209.5 billion according to the Bank for International Settlements. Other credit card networks operating in Canada include American Express, Discovery Card and Dinner's Club.

Discontinuation of the CAD 1 000 note

1375. On May 12, 2000 the Bank of Canada stopped issuing CAD 1 000 bank notes and began to withdraw them from circulation. The announcement followed the federal government's approval of an amendment to the Bank of Canada Notes Regulations to eliminate the CAD 1 000 note as part of the fight against money laundering and organized crime. This decision was recommended by the Department of Finance in consultation with the Bank of Canada, the federal Solicitor General, the Royal Canadian Mounted Police, and other Canadian law enforcement agencies.

1376. At that time, the Bank of Canada indicated that after it stopped issuing CAD 1 000 notes, the notes already in circulation would remain legal tender and would retain their full face value.

[166] The Department of Finance views this situation as a gap and, Canada indicated that, for this reason, Finance pre-published new regulations in October 2007 to subject the sector to the same requirements as real estate brokers and sales representatives.

Individuals are free to hold and use the notes for as long as they want. This is true for all Bank of Canada notes that are no longer issued, such as one- and two-dollar notes.

1377. The CAD 1 000 notes were withdrawn from circulation over time with the help of financial institutions, which return the notes to the Bank of Canada as they are deposited or exchanged by the public. All CAD 1 000 notes returned to the Bank of Canada are destroyed.

1378. The withdrawal of the CAD 1 000 note had little impact on Canada's currency system and its ability to meet the needs of businesses and individuals. The note was rarely used for cash transactions. In 1999, for example, there were about 3.8 million CAD 1 000 notes in circulation, representing less than 0.3% of all notes in circulation. As of October 31, 2006, 1.4 million CAD 1 000 notes were in circulation. The largest note in active circulation is the CAD 100 note.

4.4.2 Recommendations and Comments

1379. The authorities are engaged in considering the need to extend the AML/CFT requirements to a number of key areas, and this work should clearly proceed as quickly as possible. On the basis of comments by law enforcement, the money laundering risk appears to have been appropriately identified; however, insufficient AML/CFT measures have been implemented to address the risk for these businesses and products (especially "White Label" ATMs). Canada should take additional action to address this issue as soon as possible.

4.4.3 Compliance with Recommendation 20

Rec.	Rating	Summary of factors underlying ratings
Rec.20	C	• The Recommendation is fully met.

5. LEGAL PERSONS AND ARRANGEMENTS & NON-PROFIT ORGANISATIONS

5.1 Legal Persons – Access to beneficial ownership and control information (R.33)

5.1.1 Description and Analysis

Transparency concerning the beneficial ownership and control of legal persons

1380. The principal form of legal person in Canada is a company/corporation. Canadian corporate law (both federal and provincial) permits private, public and unlimited liability companies. The principle federal law is the Canada Business Corporations Act (CBCA); however, the laws of Alberta, Saskatchewan, Manitoba, Ontario and New Brunswick reflect most provisions of CBCA. The majority of corporations operating in Canada are incorporated under Ontario business corporation law but a substantial number of companies are incorporated under the laws of Alberta, Quebec and British Columbia and the federal jurisdiction. Given the similarity in systems, the assessment team focused primarily on the federal CBCA.

1381. The CBCA requires the following information on incorporation:

- Name of the corporation and descriptions of the business activities and intended clients.
- Provincial or territorial location and civic address of the registration office.
- Descriptions of the shares, classes of shares and the maximum share capital that the corporation may issue.
- Description of any limits on share transfer (companies will provide this information if they are registering as a private corporation and so will not have to comply with the registration and

prospectus filings requirements and other related procedures set out in the CBCA and provincial/territorial securities law[167]).

- Number of directors of the corporation and the name and residential addresses of the directors of the company.
- Names and addresses of the incorporators, who must be least 18 years of age and not in a state of bankruptcy.
- Additional rules and regulations that will govern the conduct of the company members and directors.

1382. CBCA also requires corporations to file an annual return with details such as the name of the corporation, the date of incorporation and any changes in corporate information, and to file notice of any changes to directors or the address of the registered office within 15 days. Broadly similar requirements exist in Ontario and Quebec.

1383. There is no requirement to list identifying information relating to shareholders when filing incorporation documentation. No information on the beneficial owners (as defined by the FATF) of the company being established is collected. The information provided in the incorporation process is reviewed by staff at the applicable corporate registries to ensure that the entity meets the legal requirements for incorporation, but there is no requirement in legislation for those registries to verify the accuracy of the information provided.

1384. Corporations are also required by the CBCA to prepare and maintain records at their registered office or at any other place in Canada designated by the directors and be available for inspection by directors, shareholders, creditors and incorporation authorities. These records must include a register of directors, officers and shareholders (including a list of the names and addresses of all shareholders by class of shares) and be available to directors, shareholders and creditors. Inspection of these records under the CBCA has to be supported by an affidavit that the information used shall be only in respect of the company's affairs. Also the CBCA requires that in the annual information circular companies should identify the shareholders who hold the largest number of shares. However, it is important to note that there is no requirement that the ultimate beneficial owners of shares be identified in the corporate records of private companies and, moreover, there is no legal requirement to indicate in these records if, or when, a transfer of shareholding has occurred. Public companies are, on the other hand, required to disclose on the company's information circular any shareholder who beneficially owns, directly or indirectly, or controls or directs, voting securities carrying 10% or more of the voting rights attached to any class of shares. This requirement is, however, limited to the persons who are the immediate holders of the beneficial interest and not the ultimate beneficial owners as required by Recommendation 33.

Access by competent authorities to information on the beneficial ownership and control of legal persons

1385. Regulatory, taxation, intelligence agencies, supervisory and law enforcement authorities (including Police, CRA, FINTRAC and securities regulatory authorities) have a variety of powers that enable them to secure information about the control and ownership of legal persons in Canada both from publicly available sources and through a variety of coercive measures. Regulatory and supervisory authorities also maintain records on persons who are the beneficial owners of their regulated/supervised institutions. For example, information is obtained by OSFI on persons that hold 10% of more of the shares in federally regulated banks & insurance companies, and the Director of Corporations Canada and securities regulators obtain information on persons that hold 10% or more of the shares in listed companies.

[167] To qualify as a private company, there must be fewer than 50 shareholders and shares must not be offered to the public.

1386. Coercive measures include production orders, search warrants in justifiable circumstances and court ordered inspections in others. Law enforcement authorities may also take statements from witnesses. Securities regulatory authorities have a wide range of powers to secure information including the authority to compel production of information, compel testimony and evidence, as well as other powers. For publicly available information those authorities may search the appropriate corporate registries in addition to other publicly available data bases relating to corporations for any relevant information.

1387. Through its regulatory reviews, civil audits and investigative actions, and information filed in tax returns, the CRA has access to a large amount of information. However, this does not extend to beneficial shareholder information. In addition, throughout the conduct of its administration, the CRA is bound by its own legislation and policies regarding the disclosure of information. The provision of information is permissible if the sharing of such information can reasonably be regarded as necessary for the administration or enforcement of the applicable Act, specifically the Income Tax Act or Excise Tax Act. This agency is constrained with regards to the information (and the circumstances) in which it can share information uncovered in the course of its administration of the tax statutes. For example, it can only share information with the RCMP when an information/indictment has already been laid. To obtain information via court order, the RCMP must prove that the information will be of substantial value to the case.

1388. As mentioned earlier in this report (see Section 2.5), FINTRAC is limited in the nature of information it is able to provide to law enforcement authorities[168]. In addition, the financial institutions that report to FINTRAC are not required by law to obtain information relating to the beneficial owner of legal arrangements. Under the PCMLTFA, the requirement is to establish the existence of the legal person, but not the ultimate beneficial owner (see Section 3.2 of the report).

1389. Law enforcement has a number of powers to gather information on control and beneficial ownership of legal persons from a variety of sources as outlined in this section, and also may use powers to access further information from non-public sources in the course of investigations. However, these powers are constrained insofar as several entities and persons that ought to be repositories of this type of beneficial owner information (*i.e.* company services providers, financial institutions and registries) do not currently maintain this sort of information. This is likely to affect the ability of the authorities to access accurate and current information on the ultimate beneficial owners and controllers of legal persons on a timely basis.

Bearer shares

1390. While s 24(1) of the CBCA provides that shares of a Canadian corporation must be in registered form and without nominal or par value, ss 48(1) and 187(9) of the CBCA appear to permit bearer shares to be issued by corporations. Similar provisions recognising the use of bearer shares also exist in the Manitoba Corporations Act (though not in Ontario). The CBCA provisions appear to establish that bearer shares remain a legal means of taking an ownership interest in a Canadian company. CBCA section 54 in particular indicates that securities (including shares) are fungible and that delivery may be effected either in bearer form or in registrable form. But there is no legal mechanism to require disclosure of the person or entity which holds, or is the beneficial owner of, bearer shares of any particular corporation incorporated under the CBCA.

1391. The assessment team were advised by Canadian officials, who had in turn been advised by various corporate share registrars, custodians/trustees, and securities participants in general, that they had not seen bearer shares in practice. However, it should be noted that it is most unlikely that bearer shares issued in private corporations would pass through registrars or custodians anyway, and the assessment team is not aware as to how broad a sample of private sector representatives provided

[168] Fintrac can disclose a broader set of information to law enforcement since 30 June 2007.

information. In practice it is likely that the number of bearer shares may be quite limited, but it is important that the right to issue such shares exists, and there are no mitigating measures.

Additional elements

1392. Outside the information contained in the corporate registry documents of corporations, which contains limited information on shareholders as indicated above, there are limited mechanisms to ascertain beneficial ownership information for corporations in the Canada.

5.1.2 Recommendations and Comments

1393. Although the authorities may be able to get some information on legal or beneficial ownership of a limited class of companies, such as public companies or certain classes of financial institution, these only constitute a small percentage of the total number of companies, and also those which appear to be lower risk. Canada's general corporate registry and information collection system does not focus on obtaining information relating to the beneficial owner or controller of bodies corporate in Canada. The information maintained (including changes in information) relates almost solely to persons and other corporations that are the immediate owners or controllers of a company through shareholdings.

1394. The assessors noted that the federal companies registry did not seem to be focussing on the issues relating to money laundering and the financing of terrorism and were not implementing any special measures in this regard. For example, the registry did not cross-reference applications for company formations against the terrorist lists issued by the other agencies of Government. Measures such as these could act to mitigate to some extent the threat that arises through the use of legal persons to perpetrate terrorist financing.

1395. Canada should ensure that competent authorities have access to accurate and current information on the ultimate beneficial owners and controllers of all legal persons on a timely basis. The current powers of the competent authorities are hampered to the extent that the repositories of information from which the authorities could obtain beneficial ownership information do not maintain beneficial ownership information, and for authorities such as CRA there are statutory barriers to the sharing of the information that is held with law enforcement or other competent authorities.

1396. The Canadian CBCA appears to allow for the ownership of companies through the use of bearer shares (as does the Manitoba legislation, though not Ontario) although it is likely that these shares have limited use in practice. Nonetheless, there do not appear to be any special measures in place, in particular with private corporations, to ensure that disclosure of beneficial owners of these shares so that they cannot be exploited by money launderers or those who would finance terrorism.

5.1.3 Compliance with Recommendation 33

Rec.	Rating	Summary of factors underlying ratings
Rec.33	NC	• There is no requirement to ensure adequate transparency, for instance there is no obligation that information on the beneficial ownership of shares in legal persons is required to be collected by either the corporate registry, within corporate records held by legal persons or by lawyers, accountants or TCSPs. • While law enforcement and other authorities have sufficient powers, those powers are not adequate to ensure the existence of adequate, accurate and timely information on the beneficial ownership of legal persons, which can be accessed or obtained in a timely fashion by competent authorities. • There are no measures to ensure that bearer shares are not misused for ML, particularly for private corporations.

5.2 Legal Arrangements – Access to beneficial ownership and control information (R.34)

5.2.1 Description and Analysis

General

1397. Under the Constitution of Canada, property and civil rights are a matter of provincial legislative jurisdiction. Except for the province of Quebec, all provinces are common law jurisdictions and have trust law which requires three essential components: a settlor, a trustee, and beneficiaries. Essentially, the establishment of a trust results in a transfer of proprietary rights. The trust property can be any form of property whether real or personal, tangible or intangible. In general terms, a settlor transfers legal title of specific property to a trustee but beneficial ownership to specified beneficiaries[169].

1398. In Québec, the fiducie results from an act whereby a person transfers property from his or her patrimony to another patrimony that he or she constitutes; the property is appropriated for a particular purpose and a trustee undertakes to hold and administer it (Article 1260 of the Civil Code). As a legal arrangement, the fiducie in Quebec is similar to the trust as defined above. The assessment team was not provided with information on measures taken to ensure adequate transparency concerning the beneficial ownership and control of fiducie in Québec.

1399. There are a number of different kinds of trusts in Canada with a range of purposes, but there is no general legal requirement that a trust be evidenced in writing. For those trusts that are evidenced in writing a trust instrument, such as a declaration or trust agreement (including a deed), setting out the rights and obligations of the trustees and beneficiaries, and in some cases certain third parties, is usually employed as the appropriate vehicle. Provincial legislation provides for the rules to be followed by trustees. Trusts are not separate legal entities however. Trustees are persons responsible for the trust property; hence, the trustee is liable for the obligations incurred in the name of the trust.

1400. A number of persons offer services to establish and administer trusts on behalf of trustees in Canada and they include: trust companies, lawyers and accountants (for the most part). Other trust and company service providers exist in Canada (which is discussed in Section 4.1 of the report) but limited information was available on the extent of the role of such service providers in the business of establishing or servicing trusts. There is no legal requirement that obliges these trust providers to collect information on the settlor, trustees and beneficiaries notwithstanding that as a matter of practice they would normally collect this information as vital to the establishment of a trust. However, for those entities which fall within the definition of "financial institution" under the PCMLTFA (to a large degree trust companies would be so defined), there are specific provisions requiring the collection of information relating to settlors, trustees and beneficiaries (see Section 3.2 of the report).

1401. Some pooled investment funds, such as mutual funds, or pension plans use trusts as vehicles to administer the funds on behalf of their beneficiaries. These types of trusts are frequently referred to as "pooled funds" or "pension trusts" (usually managed by a trust company or a board of trustees). In Canada, pension trusts are regulated by the federal government or by provincial governments. OSFI supervises federally regulated pension plans. These plans and the other investment plans noted fall within the definition of a "financial entity" within the PCMLTF and are therefore required to collect beneficial owner information. Income trusts are sometimes referred to as publicly-traded flow-through entities because they can flow income and the associated tax liabilities to their investors. These income trusts are registered and regulated by securities exchange commissions.

[169] Although the *Civil Code* in Québec provides for the creation of a "trust", the definition used differs from a common law trust because there is no division of ownership interest.

Prevention of the unlawful use of legal arrangements

1402. There are limited measures in place to prevent the unlawful use of trusts and fiducie in Canada. For instance, there is no system of central registration of trusts and there is no legal requirement for the recording of trusts and for maintaining the trust instrument by the settlor or any other party to the trust. The main situations where a legal obligation arises to maintain relevant information on trusts (i.e information on settlors, trustees, beneficiaries and protectors) are (a) where the trustee is also a "financial entity" such as a trust company under the PCMLTF regulations and (b) where the trust is required to lodge a tax return with the CRA. The examiners noted however that with respect to trust companies, the information requirements under the PCMLTF require the collection of "third party" information. But the term "third party" as defined in those regulations does not extend to cover the full scope of "beneficial owner"as defined in the FATF Recommendations. If a trust receives income, the trust is required to lodge a tax return with the CRA, and the information in that return may contain certain beneficial ownership/control information depending on the nature of the trust in question, but not necessarily.

Access by competent authorities to information on the beneficial ownership and control of legal arrangements

1403. Under certain conditions, trustees on behalf of a trust have to file income tax and information returns with CRA. In these returns, trusts are required to provide specific information on the name of the trust, type of trust, amounts of income and property for tax purposes, including amounts paid or payable to beneficiaries, whether the trust holds foreign property in excess of CAD 100 000 and the name, address and telephone number of trustees, executor, liquidator, or administrator. For the initial return, a trust must attach a copy of the trust document or will, and a list of assets at death (unless filed with the deceased final personal income tax return). The trust document or will contains information on the beneficiaries of the trust.

1404. Throughout the conduct of its investigations, the CRA is bound by the confidentiality provisions outlined within the Income Tax Act and the Excise Tax Act to ensure that tax information is used only for its intended purpose of administering or enforcing the applicable act. However, CRA is able to provide voluntary information reports to FINTRAC on ongoing investigations. These could include information about trusts. However the CRA may only disclose taxpayer information in the case of investigations relating to the administration of the Income Tax Act, the Canada Pension Plan, the Unemployment Insurance Act or the Employment Insurance Act, which then limits its usefulness.

1405. In addition to the information that is proactively disclosed to FINTRAC by federal tax authorities, law enforcement also has the powers to compel production of tax information on trusts held by the CRA in certain circumstances. There are two statutory exceptions that allow the CRA to provide taxpayer information to the RCMP. In both cases, the information being sought must be relevant to the substantive offences being investigated.

1406. First, the CRA will provide tax information to the RCMP where criminal proceedings, either by indictment or on summary conviction, have been commenced by the laying of an information or the preferring of an indictment under an Act of Parliament. Second, the CRA will also provide taxpayer information on trusts to the RCMP pursuant to a judicial order. This section authorises ex parte applications by the RCMP that are supported with a sworn affidavit. The judge must find that the information being sought will be of substantial value to the investigation.

1407. In addition, law enforcement may also approach trustees to ask for the voluntary provision of information on their control, ownership and activities. Law enforcement also has access to powers to compel the production of information from trustees themselves or information about trusts (via production orders or search warrants). There are no specific provisions in trust legislation that protects information from law enforcement apart from the usual confidentiality restrictions that the government imposes upon itself, e.g., the Privacy Act, section 241 of the Income Tax Act or the Personal

Information Protection and Electronic Documents Act for trusts engaged in business activities. Production orders or warrants may also be used by law enforcement to compel the production of information on the formation of a trust from the office of a lawyer that created the trust, provided that the information is not subject to legal professional privilege. Applications of this nature have been very rare. Law enforcement may also conduct interviews with persons connected with the trust as witnesses or suspects.

1408. If additional information from FINTRAC is required, law enforcement may seek a production order against FINTRAC. Law enforcement can obtain information from reporting entities through voluntary cooperation or various court orders described in Section 2.3 of the report (Recommendation 3). However given the fact that the reporting entities do not cover what could potentially be a significant portion of the persons providing trust services (i.e. lawyers and TCSPs), the law enforcement authorities may be handicapped in obtaining leads which can arise from the reporting regimes imposed on reporting entities.

1409. The assessment team believes that the agencies that receive information on legal arrangements (namely the CRA and FINTRAC) have significant limitations on their ability to disclose information. Tax information from certain trusts and law enforcement powers provide the means to access certain information on beneficial ownership and control of certain trusts. However, overall the mechanisms to obtain and have access in a timely manner to beneficial ownership and control of legal arrangements, and in particular the settlor, the trustee, and the beneficiaries of express trusts, are significantly weakened by the lack of legal record-keeping requirements and the limitations on information exchange.

5.2.2 Recommendations and Comments

1410. Canada relies on the investigatory powers of law enforcement to obtain or have access to information concerning the beneficial ownership and control of trusts and fiducie in Québec. These powers are generally sound and widely used. However, the system is only as good as the information that is available to be acquired. In the case of trusts, limited, partial information is available within the jurisdiction, and even where certain information is recorded by agencies such as CRA or FINTRAC, they can only share this information with law enforcement authorities in very limited circumstances, and the information may not be up to date. Canada should implement measures to ensure that adequate, accurate and timely information is available to law enforcement authorities concerning the beneficial ownership and control of trusts and fiducie in Québec.

5.2.3 Compliance with Recommendation 34

Rec.	Rating	Summary of factors underlying ratings
Rec.34	PC	• There are limited and indirect legal requirements to obtain, verify, or retain information on the beneficial ownership and control of trusts and fiducie in Québec; • While the investigative powers are generally sound and widely used, there is minimal information that is adequate, accurate and timely concerning the beneficial owners of trusts and fiducie in Québec that can be obtained or accessed by the competent authorities in a timely fashion. Where some information is held, such as by CRA, there are limits on the circumstances in which information on trusts can be shared.

5.3 Non-profit organisations (SR.VIII)

5.3.1 Description and Analysis

General

1411. The NPO sector in Canada is substantial and is comprised of various types of registered charities and corporations in relation to education, health, faith, human rights, social justice, environment, arts and culture, and sports and recreation. There are:

- More than 82 500 registered charities.
- An estimated 63 000 additional NPO corporations operating in Canada.

1412. Registered charities (which receive in excess of USD 5.5 BN annually) represent a significant portion of the financial resources of the NPO sector accounting for approximately 68% of all revenues and 95% of all donations. In addition, they account for a substantial share of the sector's foreign activities: 75% of international organisations in Canada are registered charities. In 2004, over 22 million Canadians made a financial donation to a charitable or other non-profit organisation.

Review of the non-profit sector

1413. Canada has conducted several reviews of the NPO sector, and the potential risks of terrorist financing. First, in 1999 the Senate examined "the international threat environment with particular reference to terrorism as it relates to Canada", including the issue of fundraising and it found that registered charities in Canada were particularly susceptible to abuse in this regard because of the credibility and deniability such status affords. Second, an inter-departmental group reviewed the adequacy of its laws and regulations as they relate to non-profit organizations in considering its anti-terrorism legislation. Lastly, in 2004 a five-year Regulatory Reform Action Plan for the Charities Directorate was announced based on the result of a comprehensive review of the regulatory framework for the non-profit sector in Canada undertaken as a joint voluntary sector and government initiative.

1414. In September 2004 Canada reviewed the adequacy of its laws and regulations in relation to risks of terrorist financing posed within the NPO sector as part of its obligations to the FATF. A report entitled "*A Review of the Canadian Non-Profit Organisation Sector* (A Discussion Paper for the FATF Working Group on Terrorist Financing)" was presented to the FATF WGTYP the following year.

Charitable registration

1415. All charities are required to apply to the CRA for registration and abide by the provisions of the Income Tax Act (IT*A). Charities that fail to meet these legal requirement*s can be de-registered. To qualify for charitable registration, an organisation must be established for charitable purposes and devote its resources to charitable activities. The charity must also be resident in Canada and cannot use its income for the benefit of its members. There are four kinds of recognised charitable purposes: relieving poverty, advancing education, advancing religion and providing certain other community benefits (including, homes for the elderly, hospitals, disaster relief efforts). To qualify for registration a charity must meet a "public benefit" test. An organisation must show that its activities and purposes are legal and (1) provide a tangible benefit to the public, (2) benefit the public or a significant portion of the public, and (3) do not serve a political purpose.

1416. A registered charity can be one of three entities: (1) a charitable organisation (which comprise 90% of registered charities), (2) a public foundation (which comprise 5% of the charities and generally funds the charitable activities of other charities), or (3) a private foundation (comprising the remaining 5% controlled by a group of related persons which can carry out charitable activities or fund the charitable activities of others).

1417. An organisation will not be registered under the Income Tax Act (or its existing registration will be revoked) when there are reasonable grounds to believe it is connected to terrorism. Most often, the regular rules and procedures under the Income Tax Act can be used to deny or revoke registration. To assist in cases where highly classified information must be used to substantiate a charity's links to terrorism, the Charities Registration (Security Information) Act was enacted as part of the Anti-terrorism Act. This legislation establishes a ministerial process whereby sensitive information can be used to determine whether to deny (or revoke) a charitable registration. In reviewing new applications and existing registered charities, the CRA requests information from the RCMP and CSIS when there are concerns an organization may be connected to terrorism.

Supervision, monitoring and data collection

1418. At the federal level, law enforcement and intelligence agencies monitor and investigate charities suspected of providing support for terrorist activities. In addition, the CRA closely monitors registered charities. Organisations seeking registration are required to apply to the CRA's Charities Directorate. Applicants use a standard form, which requires them to provide the organisation's current legal name, a list of the directors or trustees, key financial data and a detailed description of the organisation's programs. This description includes the location of the activities, the identity of the intended beneficiaries and the mechanisms to ensure that the organisation retains control of its resources. Applicants must also include copies of the governing documents under which they operate, such as certificates of incorporation or organisational by-laws.

1419. The Charities Directorate's compliance program is largely based on information from the annual returns, internal analysis of trends in the charitable sector, complaints from the public and tips from informants. The CRA is also authorised by statute to release certain other information regarding registered charities to the public. This includes: (1) the organization's governing documents and other prescribed information provided on applying for registration; (2) the notification of registration issued by the CRA; (3)the names of the persons who at any time were the charity's directors; and (4) any notice of the grounds for revocation of registration issued by the CRA. Certain other information, such as the addresses of trustees and directors, is reported to the CRA but remains subject to confidentiality rules

1420. These supervisory mechanisms appear to be effective for charities even though limited to the latter (and not applicable to other non profit organisations). Existing corporation law mechanisms under the Canada Corporations Act, which are administered or maintained by Industry Canada are utilized such as a mandatory submission of specific corporation information and requirements that compel corporations to maintain corporation records and financial reports available for inspection. If potentially illegal activities are detected by Industry Canada, it is standard practice to refer these matters to law enforcement. Canadian provinces generally have reporting and supervision mechanisms of a similar nature under their corporation laws.

1421. Canada also has a number of "umbrella organizations" that provide guidance and varying degrees of oversight such as the Canadian Council of Christian Charities which offers its members a certification program. Charities, which participate in this program, can display a special "seal of approval". Certification requires that the member organization has an independent board, audited financial statements, and that it has adopted the Council's "Code of Ethical Fundraising and Financial Accountability".

1422. Similarly, the Canadian Centre for Philanthropy encourages its members to adopt its "Ethical Fundraising and Financial Accountability Code". The 500 charities that have adopted this Code are committed to responsibly managing the funds that they receive and reporting their financial affairs accurately and comprehensively. The Association of Fundraising Professionals also encourages its members to adopt a code of ethics, a donor's bill of rights and put in place a mechanism to register complaints. Other charitable organizations with chapters or branches in Canada also play an important role in ensuring that high standards of accountability are observed by their affiliates.

1423. The specialized supervisory and monitoring measures under the CRSIA do not apply to the other parts of the NPO sector. This sector is estimated to be almost of comparable size to the registered charities sector, but the Canadian risk reviews suggest that it is far less significant in terms of risk profile. There is acknowledged coverage as regards outreach and data collection (insofar as the CRA does obtain substantial information as regards the operations of NPOs). However, if an entity does not register under the ITA, then there are no similar supervisory measures.

Sanctions

1424. The ITA provides CRA with the ability to apply a range of interim sanctions against registered charities that are non-compliant. These include financial penalties and/or the temporary suspension of certain privileges such as the ability to issue tax receipts. The scope of activities that can be subject to sanctions range from, but are not limited to, certain business activities, unjustly enriching principals of the organization, gifting resources to non-eligible recipients and furnishing false statements with respect to tax receipts. The severity of the penalty increases with subsequent infractions and may ultimately lead to revocation.

1425. Out of a pool of 82 500, about 2 000 charities have their registrations revoked each year. These are mostly organizations that have ceased operations or have failed to file annual returns. CRA conducts comprehensive field audits of about 800 registered charities each year. Recent experience suggests that, on average, about 10 charities a year lose their registrations as a result of serious non-compliance issues, including dubious fund-raising schemes, political activities, lack of proper books and records, and improper personal benefit. In addition, registered charities that have failed to demonstrate sufficient control over their foreign operations have been de-registered.

1426. Under the CRSIA, a special mechanism has been established to deny an organization's application for registration (or revoke its existing registration) when terrorist connections are suspected. As outlined above, the CRSIA establishes a ministerial process whereby sensitive information can be used to determine whether to deny (or revoke) charitable registration.

Record keeping requirements

1427. In the process of applying for registered status, a charity must provide key financial data to the CRA, including information on the mechanisms to ensure that the organization retains control of its resources. Once registered, a charity must annually provide the CRA with a copy of its financial statements and a return providing information on its board of directors, its sources of revenue, its types of expenditures and its general operations. A charity is required to maintain such records for a period of six years from the date of the last taxation year to which they relate. A revocation of a charity's registration could take place where the record keeping requirements are not met.

Information gathering and domestic co-operation

1428. Cooperation exists between law enforcement and intelligence and security agencies and other key agencies including the CRA, CSIS, RCMP and FINTRAC.

1429. Departments and agencies share information and cooperate in the charitable registration process. In reviewing new applications and assessing compliance, the CRA is able to obtain information held by the RCMP and CSIS that may reveal an organization's ties to terrorist groups.

1430. As part of the CRA, the Charities Directorate is subject to the Income Tax Act's stringent provisions on the confidentiality of taxpayer information. However, the ITA does permit the Directorate to share its information when such disclosures can reasonably be regarded as necessary to

enforce the ITA or the Charitable Registration (Security Information) Act[170]. The CRA can share information about a registered charity or an organization that has applied for such status with law enforcement and intelligence agencies where there are reasonable grounds to suspect that information held by the CRA might be relevant to the investigation of a terrorism offence under the Criminal Code or to threats to the security of Canada[171].

1431. The measures implemented by the CRSIA relate to the reliance on security information with regards to a decision whether to permit an entity to be registered or continue to be registered as a charity. There is no automatic trigger between the decision to issue a certificate under the CRSIA and the process leading to listing and/or freezing procedures. However, the measures implemented by CRSIA are supported by formal liaison agreements between the CRA and authorities responsible for conducting investigations which lead to the commencement of listing and/or freezing procedures (*i.e.* the RCMP and CSIS) and CRA information that is shared for purposes of CRSIA may be used to further investigations that could lead to commencing such procedures.

Access to information

1432. During the course of TF investigations, the RCMP will access the publicly available information as provided by the Canadian government registries and/or regulatory bodies and any additional information that can permissibly be obtained from the CRA. It may also seek information directly from the entity or individual under suspicion using existing law enforcement powers. The RCMP must abide by legislation that dictates the legal process, *i.e.* obtain search warrant or production order, under which information pertinent to a criminal investigation may be obtained. Through these methods, law enforcement is able to access all available information on the administration and management of an NPO in the course of an investigation.

1433. Under section 462.7 of the Criminal Code, and subject to section 241 of the Income Tax Act any person may make a disclosure to the Attorney General or a peace officer where a reasonable suspicion exists that property is the proceeds of crime or that the person has committed or is about to commit a designated offence. Section 241 of the Income Tax Act also provides an avenue for the law enforcement authorities to obtain information from the CRA where it is proven that a terrorism offence is being investigated is underway and that the information sought is likely to be of substantial value to the investigation.

Sharing of information

1434. Intelligence agencies have expertise and capability to examine NPOs that are suspected either being exploited by or actively supporting terrorist activity or terrorist organizations. CSIS investigates NPOs as part of their terrorist investigations and will disclose information to the police or other jurisdiction in the same manner as for any other investigations. Additionally, the CSIS Financial Analysis Unit works closely with the Charities Directorate of CRA in reviewing renewals and applications for charitable status. This unit, as the primary contact, conducts the research related to the requests and formulates the response on behalf of the CSIS.

1435. FINTRAC conducts analysis of the information it receives from reporting entities and other government departments and has made disclosures that have included information about the suspicious activities of NPOs. As of July 2005, FINTRAC had made over 120 case disclosures of suspected terrorist activity financing and other threats to the security of Canada. NPOs, both foreign and domestic, have figured in over one-third of the case disclosures related to suspected terrorist activity financing, with slightly more Canadian NPOs represented in these disclosures than foreign ones.

---

[170] To assist in the administration and enforcement of the CRSIA, an amendment has been made to the PCMLTFA to allow FINTRAC to disclose information to the CRA on suspected cases of terrorist financing involving charities.

[171] Amendments to section 241 of the Income Tax Act brought in force on February 10, 2007.

FINTRAC is however currently unable to make disclosures to the CRA and may only disclose a limited amount of information (see comments on "designated information" in Section 2.5 of the report).

1436. The CRA is constrained under section 241 of the Income Tax Act as regards the circumstances in which it can voluntarily share taxpayer information though there are a number of exceptions to the general rule that confidentiality must be maintained. One such exception is set out in s.241(3.2) which allows the disclosure to any person of certain information related to registered charities such as governing documents, names of directors, financial statements etc. Other information on registered charities or on other tax payers, including other NPOs, can be disclosed as part of criminal proceedings that have commenced (s.241(3)). Equally, defined classes of information relating to registered charities and any other NPO that has sought registration (though not all taxpayer information) can be shared with law enforcement, intelligence agencies and FINTRAC for purposes of investigating terrorism (including terrorist financing) in prescribed circumstances *i.e.* reasonable grounds to suspect the information would be relevant to an investigation of whether a terrorism (including TF) offence may have been committed (s.241(9)). In addition, under s.241(9.1) any information about a registered charity or an NPO that has applied for such status (other than individual Canadian donors information) which the CRA has provided to CSIS or the RCMP for purposes of administering or enforcing the CRSIA can also be used by those agencies for purposes of investigating terrorism. Finally, s.241 allows the release of all taxpayer information, without any restriction, pursuant to a court order or CSIS warrant.

1437. The assessment team believes that the CRA maintains an extensive information collection regime for all NPOs for taxation purposes. The team notes that a broader amount of information can be shared with respect to registered charities and NPOs that have sought registration than other types of taxpayers (including other NPOs). However, except in cases where it is acting under the authority of a court order or a CSIS warrant, the CRA can only share a broad class of tax payer information relating to all NPO with law enforcement when criminal proceedings have commenced, and a more limited class of information with FINTRAC when the requirements of s.241(9) are met. The requirements of s.241 thus impose some limitations on the type of information to be obtained, or the circumstances in which it can be obtained by FINTRAC or law enforcement, which may limit the investigative value of the information..

International requests

1438. Formal and informal mechanisms are used to provide and receive international information regarding the terrorist-support activity in the NPO sector. These are the same channels that are used by law enforcement, intelligence organizations and judicial authorities to share information on terrorist financing and money laundering activities (see Section 6.5 of the report).

Law Enforcement Cooperation

1439. Police forces in Canada regularly provide informal assistance to police forces from other countries. Generally, police are able to provide information or documentation that is publicly available or which may be obtained on a voluntary basis. This usually involves direct communication between police forces and may include transmission of information through Interpol.

Cooperation between Financial Intelligence Units

1440. For its part, FINTRAC also can exchange information relevant to the investigation or prosecution of a money laundering or terrorist financing offence involving non-profit organizations with international counterparts. To provide information, however, FINTRAC must have a memorandum of understanding with the counterpart FIU, which governs how the information will be used and protected. Further information about FINTRAC and its information sharing agreements are available in Sections 2.5 and 6.5.

Judicial Cooperation

1441. The International Assistance Group (IAG) of the Department of Justice is the focal point where all Mutual Legal Assistance Treaties (MLATs) requests are processed. The IAG has received MLAT requests for information related to NPOs suspected of terrorist financing or other forms of terrorist support. The IAG has applied the same process as for any other MLAT requests. The process is explained in Section 6.3 of the report.

5.3.2 Recommendations and Comments

1442. Canada has taken considerable steps to implement SR VIII in relation to registered charities, which it considers to be the sector most at risk, based on the risk assessment studies it has done. A large segment of the NPO population is not covered by the current measures using the risk based approach, but Canada should continue to monitor the risks in these other sectors. Canada should improve the existing co-ordination mechanisms between competent authorities, especially between the CRA and the parties responsible for listing and freezing applications. Again, Canada should review the capacity of CRA and FINTRAC to share information with law enforcement authorities related to the non-profit sector.

5.3.3 Compliance with Special Recommendation VIII

Rec.	Rating	Summary of factors underlying ratings
SR.VIII	LC	• The existing co-ordination mechanisms between competent authorities, especially between the CRA and the parties responsible for listing and freezing applications is insufficient to fully address the risk in some segments of the NPO sector.

6. NATIONAL AND INTERNATIONAL CO-OPERATION

6.1 National co-operation and coordination (R.31 & 32)

6.1.1 Description and Analysis

Recommendation 31

1443. The lead for policy and coordination in the AML/CFT area rests with the Department of Finance. The Department of Public Safety and Emergency Preparedness (PSEPC) takes a lead role in coordinating the Government of Canada's response and activities related to terrorist listings.

1444. Canada has developed several structures which are aimed at ensuring proper coordination in AML/CFT matters.

Department of Finance Committee Structures

1445. *Interdepartmental Assistant Deputy Minister (ADM) Steering Committee (ISC) and Working Group*. The ADM Steering Committee has representation from the key departments and agencies within the federal AML/CFT regime – FINTRAC, OSFI, PSEPC, RCMP, CSIS, CBSA, CRA, and the Department of Justice. The ISC meets a minimum of twice a year and serves as a forum for the discussion of policy and operational issues relative to the regime. This ADM Steering committee also serves as a forum for a high level assessment of the effectiveness of the regime and discussion of issues of strategic importance. In addition, there is a working level group that undertakes activities as directed by the committee through regular meetings (about 10 times annually), as required. This working level committee's work includes the development of new policy, legislative and regulatory proposals, the co-ordination of audits and evaluations of the effectiveness the regime, discussion of funding pressures and operational challenges among the partners and their potential impact on results.

1446. *Informal Group*. The Department of Finance originally established the Informal Group in 2002 to facilitate an integrated federal/provincial response to events in financial markets related to investor confidence. Some of the more recent issues that the Informal Group has dealt with include enforcement issues in capital markets, challenges posed by hedge funds and enhancements to Canada's AML/CFT regime.

1447. *Heads of Agencies*. The Governor of the Bank of Canada chairs the Heads of Agencies group, which meets three to four times each year. The group brings together regulators, such as OSFI and the chairs of the provincial securities commissions, as well as the Department of Finance, to exchange information regarding financial market regulatory developments.

1448. *Federal-Provincial-Territorial Financial Sector Policy Officials Meetings*. The Department of Finance chairs meetings of federal, provincial and territorial financial sector policy officials twice each year. The range of issues discussed is very broad and evolves with current developments. Although these meetings are generally focused on information sharing, they also serve to identify areas where coordinated intergovernmental action is required.

PSEPC Committee - Interdepartmental Coordinating Committee (ICC)

1449. The ICC is a working level group created in 2001, to address operational and administrative issues relating to the listing of terrorist entities pursuant to Security Council Resolutions 1267 and 1373, as well as under the Criminal Code. It is currently chaired by the Counter Terrorism Policy and Coordination Division within PSEPC and is attended by representatives of the Department of Finance, RCMP, CSIS, OSFI and DFAIT. The ICC meets on a monthly basis or as needed. The committee provides a forum for departments and agencies to assess operational challenges and requirements to implement the listing regime and the efficiency and effectiveness of that regime.

1450.

Department of Justice Prosecution Coordination Structure

1451. The new Public Prosecution Service of Canada (PPSC) assumes carriage and control of all prosecution functions previously undertaken by the Federal Prosecution Services and the PPSC is tasked with all of the consultation and coordination responsibilities previously undertaken by the Federal Prosecution Service. The PPSC continues the three times a year coordination meeting with the heads of prosecutions in the provinces. In the area of money laundering and proceeds of crime, there are two committees that have been created. The National Liaison Committee, comprised of money laundering prosecutors, meets yearly or more frequently to coordinate common issues relevant to money laundering prosecutions. The second committee is the Coordinating Committee of Senior Officials (CCSO) on Proceeds of Crime. It is also comprised of money laundering prosecutors and criminal law policy lawyers and reports to the Justice Deputy Ministers Committee (Federal, Provincial and Territorial). The PPSC is also a partner in a national memorandum of understanding with the RCMP for the IPOC.

Additional Co-ordination Initiatives

1452. *Canada Drug Strategy (CDS).* The CDS aims to strike a balanced, integrated approach to reducing both the demand for and the supply of drugs through integrated efforts of a number of federal organizations including the RCMP, Correctional Service of Canada, CBSA, Department of Justice, Drug Treatment Courts, Federal Prosecution Service, Foreign Affairs Canada. The programme of work includes law enforcement activities aimed at disrupting activities surrounding the production and supply of illicit substances, as well as substance abuse programs for Federal inmates.

1453. *First Nations Organized Crime Initiative (FNOC).* The First Nations Organized Crime Initiative assists First Nations police services in addressing organized crime and cross-border criminality. It enables sustained participation in multi-agency law enforcement activities. Furthermore, it provides training and opportunities for intelligence gathering and sharing.

1454. *Integrated Border Enforcement Teams (IBETs).* Established after September 11, 2001, the Integrated Border Enforcement Team (IBET) program is an intelligence-led cooperative that supports national security investigations associated to the Canada/US border and investigates cross-border illegal activities, between the Ports of Entry (POE). The RCMP and the Canadian Border Services Agency work with U.S. Customs and Border Protection, the US Bureau of Immigration and Customs Enforcement, and the US Coast Guard to share information and work together daily with other local, state and provincial enforcement agencies on issues relating to national security, organized crime and other criminality transiting the Canada/US border between the POE.

1455. Integrated Proceeds of Crime Initiative (IPOC). See description in Section 2.6 of the report.

1456. *National Coordinating Committee on Organized Crime (NCC).* The NCC, a body composed of federal, provincial and territorial (FPT) government senior officials, prosecutors, and representatives from the law enforcement community, identifies key issues for action and develops national strategies and initiatives to address them. The NCC has three main responsibilities: (1) to identify issues and policy priorities related to the problem of organized crime; (2) to advise FPT Deputy Ministers on the development, coordination and implementation of policies, legislation and programs aimed at combating organized crime; and (3) to encourage coordination of anti-organized crime activities among various players at the regional and local level.

1457. *Governance of Initiatives*. Initiatives such as FNOC, IBET, IMET, IPOC and NCC operate under a similar governance structure, with both a Partners Advisory Committee and a Senior Governance Committee. The Partners Advisory Committee is composed of representatives from each of the partner organizations at the Director and Senior Analyst levels. These committees meet several times a year or more frequently to address urgent issues. These working groups focus on a myriad of issues, including communications, research, evaluation and risk management and emerging issues, and have been established to support decision-making by the ADM Steering Committee.

Additional elements

1458. Finance is the primary lead in terms of consultations with stakeholders, and has a close working relationship with industry regulators and associations that represent the reporting entities. Finance also maintains a list of stakeholders to ensure that they are adequately consulted and informed of any new legislative and regulatory changes. A recent example is the release of Finance's consultation paper, "Enhancing Canada's Anti-Money Laundering and Anti-Terrorist Financing Regime" in June 2005, which led to over 50 written submissions and nine months of face-to-face consultations with stakeholders throughout the country. These consultations played a significant role in the drafting of the new legislation that was passed in December 2006, and the resulting changes to regulations and industry guidance. FINTRAC and OSFI, in particular, play an essential role with the Department of Finance, in liaising with the private sector to ensure their commitment to and compliance with the AML/CFT regime.

1459. Further, law enforcement maintains its own contacts with the private sector in order to ensure a supportive environment. There is an ongoing dialogue with the Canadian Bankers Association and with specific large banks.

1460. *AML/CFT Advisory Committee (AC).* One of the recommendations coming from domestic assessments of the Canadian regime was the creation of a new AML/CFT Advisory Committee. The AC had its first meeting in November 2007[172].

[172] With the aim of increasing outreach, cooperation and coordination, the new Advisory Committee comprises both public and private sector representatives. The AC consists of members of the key departments and agencies, in addition to representatives from each sector of the reporting entities. It is chaired by the Department of Finance and has high-level representation from approximately 30 members.

1461. Federal partners interact regularly with each other and with external stakeholders in relation to AML/CFT issues. The federal partners primarily use the interdepartmental working group led by the Department of Finance. The group meets regularly and, although no minutes of the meetings are kept, participants acknowledge that it provides an effective means of discussing common issues. However, at more operational level, the assessment team found signs of friction, especially between FINTRAC and the law enforcement authorities. Some signs of reluctance to share information remain which has an impact on the effectiveness of the implementation of the AML/CFT regime.

Recommendation 32

1462. Canada reviews quite extensively the effectiveness of the AML/CFT system on a regular basis and through different authorities and bodies.

1463. Canada's system of government has numerous means by which to ensure that its policies and programs are effectively meeting their intended goals, and Canada's anti-money laundering and counter-terrorist financing regime has been subjected to these checks and audits. This included an in-depth audit by the Office of the Auditor General[173], an independent government agency that ensures that government programs are effectively using public funds for their intended purpose. The AML/CFT regime has also been evaluated by a private research group[174] as a condition for a renewal of funds by the Treasury Board. Lastly, as stipulated under the PCMLTFA, the regime s recently underwent a five year review by a committee of the Senate[175] to review administrative and operational effectiveness and efficiency since the legislation was originally passed. Section 72(1) of the consolidated legislation mandates that such a review take place every five years by a committee of the House of Commons, of the Senate, or of both Houses.

1464. In the first review, the results of the 2004 OAG report were favourable. However, the auditors highlighted three areas for further consideration:

- The PCMLTFA limits the information that FINTRAC can disclose to law enforcement and security agencies as a result of Charter and privacy rights. This inhibits to some degree the usefulness of disclosures in generating new investigations.
- The partners involved in the initiative could enhance coordination through the introduction of an overarching advisory committee to discuss issues of common interest and develop approaches for dealing with emerging issues.
- Accountability mechanisms to monitor the impact and usefulness of the intelligence that FINTRAC provides law enforcement and security agencies could be enhanced.

1465. Overall, the AML/CFT system was viewed positively by EKOS that made the following key recommendations:

- Reporting entities require feedback from FINTRAC concerning the impact of their reports.
- Additional funding should be allocated to meet specific needs, such as IT renewal at FINTRAC and expansion of investigation capacities for the RCMP and CBSA.
- Information in FINTRAC disclosures could be expanded to increase the value to law enforcement and security agencies.

---

173 "Observations and Recommendations." Chapter 2 – Implementation of the National Initiative to Combat Money Laundering. 2004 Report of the Auditor General of Canada at: http://www.oag-bvg.gc.ca/domino/reports.nsf/html/20041102ce.html.

174 "Year Five Evaluation of the National Initiative to Combat Money Laundering and Interim Evaluation of Measures to Combat Terrorist Financing. Final Report" EKOS Research Associates Inc. November 30, 2004. p. iv.

175 "Stemming the Flow of Illicit Money: A Priority for Canada." Parliamentary Review of the Proceeds of Crime (Money Laundering) and Terrorist Financing Act. Standing Senate Committee on Banking, Trade and Commerce. October 2006. p. 27.

- Updating the logic model and evaluation framework should be undertaken, among other things, to ensure outcomes and cost effectiveness of the program.

1466. The Senate Committee tabled a report, "Stemming the Flow of Illicit Money: A Priority for Canada", on October 5, 2006, which highlighted the need for the AML/CFT regime to meet domestic requirements, but also the importance of meeting international obligations in order to ensure that the world is "safer and more secure". The review was conducted with the understanding that there were proposed legislative changes underway stemming from a consultation paper released by the Department of Finance in June 2005. Recommendations and the Government's response included:

- Creating a registration system for money service businesses.
- Require dealers of precious metals and stones to report suspicious transactions and other prescribed reports to FINTRAC.
- Require customer identification in non-face-to-face transactions.
- Use a risk-based approach to determine the level of client-identification and record keeping for reporting entities.
- Oblige lawyers to follow client-identification, record keeping and reporting requirements, while still respecting solicitor-client privilege, the Canadian Charter of Rights and Freedoms, and the Quebec Charter of Human Rights and Freedoms.
- Enable FINTRAC to disclose to law enforcement and intelligence agencies the rationale for the disclosure and any other publicly available information.
- Determine the likelihood and extent of money laundering and terrorist financing activities that could be taking place with emerging modes of financial services delivery, like white label ATMs and Internet banking.
- Require feedback from law enforcement and security agencies to FINTRAC on the value of their disclosures. As well, FINTRAC should provide feedback to reporting entities on the usefulness of their reports in the fight against money laundering and terrorist financing.
- Require the reporting of suspicious attempted transactions.
- Examine whether the reporting threshold of CAD 10 000 is appropriate to activities in Canada and consistent with other countries.
- Ensure that FINTRAC is adequately funded to carry out its mandate under the PCMLTFA.
- Ensure that the RCMP has the required financial resources and expertise to investigate cases of money laundering and terrorist financing.
- Ensure appropriate oversight of FINTRAC.

1467. In response to these evaluations, the responsible government departments and agencies have been working to ensure that the recommendations made in each of these three evaluations were followed-up and that the appropriate changes to the regime were made.

1468. Canada's AML/CTF regime will be subject to a further third party evaluation in fiscal year 2009-2010 in order to secure continued funding. Similarly, Treasury Board also recommended, following the 2006 increase in funding for FINTRAC, the RCMP, CBSA and the Department of Justice in Budget 2006, that the evaluation framework be re-assessed to see if it is capturing the results of the regime appropriately. This new evaluation framework must be completed by October 2007. In addition, an assessment of the impacts of data collection and disclosures provided under Canada's AML/CFT regime on Canadians' privacy will be conducted.

6.1.2 Recommendations and Comments

1469. Canada has developed quite a large number of initiatives to improve co-operation mechanisms among the different stakeholders taking part in the fight against money laundering and terrorist financing. However, from the discussions that took place during the on-site visit, the assessment team believes that interagency cooperation between the FIU and law enforcement authorities is not fully effective and needs to be enhanced, in order to optimise Canada's capacity to investigate ML and TF

cases. Canada should consider encouraging more bilateral (ad-hoc and more formalised) contacts among agencies.

1470. The assessment team welcome the setting up of an AML/CFT Advisory Committee that allows private and public stakeholders to discuss emerging AML/CFT issues and support implementing the existing standards. It is important that private sector and provincial stakeholders are fully involved in the consultation process, including regional and provincial organisations that have important connections with practitioners in their respective sectors.

6.1.3 Compliance with Recommendation 31

Rec.	Rating	Summary of factors underlying ratings
Rec.31	LC	• Interagency cooperation between the FIU and law enforcement authorities is not fully effective and needs to be enhanced.

6.2 The Conventions and UN Special Resolutions (R.35 & SR.I)

6.2.1 Description and Analysis

Ratification and implementation of conventions

1471. Canada signed the Vienna Convention on December 20, 1988, and ratified the Convention on July 5, 1990. Canada signed the Palermo Convention on December 14, 2000 and ratified the Convention and its Protocols on May 13, 2002. Canada signed the United Nations International Convention for the Suppression of the Financing of Terrorism on February 10, 2000, and ratified the Convention on February 19, 2002.

1472. The provisions of the Palermo and Vienna Conventions relating to the ML offence have been almost entirely implemented; however there are two small deficiencies, the ML offence does not cover all designated categories of predicate offences/all indictable offences since Canada has a threshold approach to criminalising money laundering (including indictable offences such as offences under the Copyright Act which carry a penalty of up to 5 years imprisonment). Also, Section 462.31 ML offence contains a purposive element that is not broad enough to meet the requirements of the Conventions or Recommendation 1 (see conclusions in Section 2.1). Most of the provisions of the CFT Convention have also been fully implemented. However, Article 18(1)(b) of the Terrorist Financing Convention requires countries to implement efficient measures to identify customers in whose interest accounts are opened is insufficiently implemented. Canada's implementation of Recommendation 5 currently does not include adequate measures to ascertain the identity of beneficial owners through CDD procedures (see discussion in relation to Recommendation 5)[176].

Implementation of the U.N. Security Council Resolutions

1473. Canada implemented UNSCR 1267 (1999) by adopting the United Nations Afghanistan Regulations in November 1999. These regulations, which were renamed the United Nation Al - Qaida and Taliban Regulations in June 2006, incorporate by reference the list of individuals and entities maintained by the 1267 Committee for the purpose of freezing, seizing or confiscating the funds or assets owned or controlled by those listed individuals and entities. They also implement successor resolutions 1333, 1390, 1452, 1526 and 1617. Canada implemented UNSCR 1373 (2001) in October 2001, with the adoption of the Canadian UN Suppression of Terrorism Regulations, which in 2006 were renamed the Regulations Implementing the United Nations Resolutions on the Suppression of Terrorism.

[176] Canada indicated that shortfalls have been addressed in regulations enacted in June 2007 and coming into force on 23 June 2008. Such regulations have not been assessed by the assessors.

1474. Canada has fully implemented S/RES/1267(199) and its successor resolutions as well as UNSCR 1373(2001).

Additional elements

1475. Canada ratified the Inter-American Convention against Terrorism on December 2, 2002. It appears Canada has implemented the 2002 Inter-American Convention against Terrorism, with the possible exception of Article 4(b) of that Convention.

6.2.2 Recommendations and Comments

1476. Canada should ensure that the ML offence does cover all designated categories of predicate offences and Canada should consider removing the purpose element from Section 462.31 of the CC to be in line with the UN Conventions (see Section 2.1 of the report). Canada should enact stronger measures to customer identification so as to be more compliant with Article 18(1)(b) of the CFT Convention[177].

6.2.3 Compliance with Recommendation 35 and Special Recommendation I

Rec.	Rating	Summary of factors underlying ratings
Rec.35	LC	*Implementation of the Palermo and Vienna Conventions:* • Canada has ratified the Palermo and Vienna Conventions and implemented them with some omissions however (the ML offence does not cover all required categories of predicate offences and Section 462.31 ML offence contains a purposive element that is not broad enough to meet the requirements of the Conventions); *Implementation of the CFT Convention:* • Article 18(1)(b) of the Convention, which requires countries to implement efficient measures to identify customers in whose interest accounts are opened is insufficiently implemented. Canada's implementation of Recommendation 5 does not include adequate measures to ascertain the identity of beneficial owners.
SR.I	LC	*Implementation of the CFT Convention:* • Article 18(1)(b) of the Convention, which requires countries to implement efficient measures to identify customers in whose interest accounts are opened is insufficiently implemented. Canada's implementation of Recommendation 5 does not include adequate measures to ascertain the identity of beneficial owners.

6.3 Mutual Legal Assistance (R.36-38, SR.V, R.30 & 32)

6.3.1 Description and Analysis

Recommendation 36 & Special Recommendation V

Scope of assistance allowed

1477. Canada has extensive formal and limited informal means of providing mutual legal assistance (MLA) to requesting countries. Canadian police, directly or through Interpol, can provide assistance on the basis of a simple request but only where the evidence or information can be obtained without a court order. However, since 2006, the RCMP is more restricted in both the amount and type of informal information they can provide to foreign law enforcement partners without formal arrangements. Often, this forces the requesting law enforcement partners to resort to the much slower

[177] Canada indicated that shortfalls have been addressed in regulations enacted in June 2007 and coming into force on 23 June 2008. Such regulations have not been assessed by the assessors.

and more cumbersome formal legal assistance processes. This may over-burden the formal MLA process.

1478. Where the evidence can only be gathered pursuant to a court order, Canada's Mutual Legal Assistance in Criminal Matters Act ("MLACMA" or "the Act") is the domestic legislation that enables a Canadian court to issue orders compelling the production or authorizing the seizure of evidence at the request of a treaty partner. Canada is a party to 34 bilateral mutual legal assistance treaties, and as mentioned previously in Section 6.2.1 of the MER, Canada is also a party to multilateral treaties such as the Vienna, Palermo and Terrorist Financing Conventions.

1479. Under the MLACMA, the following mechanisms can be used to obtain evidence in compliance with Recommendation 36 (Criterion 36.1 (a) through (f)): search warrants; productions orders (typically used to compel production of evidence from disinterested third-parties such as banks, phone companies and other telecommunications service providers and to compel statements); any other warrant available under Canada's Criminal Code (such as a warrant for a number recorder on a telephone line); video or audio-link of a witness in Canada to proceedings in a foreign jurisdiction; an order for the lending of exhibits which have been tendered in Canadian court proceedings; an order for the examination of a place or site in Canada; the transfer of a sentenced prisoner (with his or her consent) to testify or assist in an investigation; service of documents; the enforcement of orders made by a court of criminal jurisdiction for the restraint, seizure or forfeiture of property situated in Canada; enforcement of foreign criminal fines; and enforcement of foreign criminal restraint and forfeiture orders.

1480. Canadian courts can also issue compulsory process for the evidence of witnesses and the production of documents in response to a request from a court in the foreign state via the letters rogatory process, but in such cases Canada cannot use the other compulsory means that are available to Treaty partners under the MLACMA.

1481. The tools most commonly used to obtain evidence on behalf of a requesting state are evidence gathering orders and search warrants. In order for a Canadian judge to issue a MLACMA search warrant or evidence gathering order, he or she must be satisfied that there are reasonable grounds to believe that "an offence under the foreign law has been committed" and that evidence of the commission of the offence will be found in Canada. The request for assistance must provide sufficient information to satisfy the judge on these two points. However, while treaty parties have access to the full slate of Canadian law enforcement tools to seek information and evidence, obtaining such orders appears, in practice, to be quite burdensome. To obtain simple production orders, in addition to the usual content required for executable MLA requests, the requesting state must provide Canada both a detailed explanation as to why it believes any evidence is located in Canada, and how such evidence will be relevant to proving elements of the foreign criminal case.

1482. Canada has a centrally-coordinated MLA regime involving: the Department of Justice which acts as a gatekeeper; Crown prosecutors who present the requests to Canadian Courts for execution; the Judiciary, and, on occasion, law enforcement agents who execute the Canadian court's compulsory orders. The MLACMA includes extensive judicial oversight of the process of collecting evidence for foreign governments. For example, no evidence that was obtained through compulsory orders obtained under MLACMA may be sent to a requesting state without judicial authorisation. The Department of Justice, while charged with guiding MLA requests through the MLA process, has very little control over the speed with which the MLA process is completed and has to rely upon the diligence of prosecutors, and the expectation that judges appreciate that timely responses to MLA requests are central to international criminal assistance. Undue delays in responding to MLA requests can hinder the ability of the requesting authorities to bring an accused to trial, given the short legal deadlines that often exist. This, in part, may explain the high number of abandoned requests in Canada's MLA regime.

1483. Canada can respond to a letters rogatory request from a foreign court addressed to a court in Canada. Assuming the letter rogatory contains sufficient information, counsel with the Department of Justice will bring an application before a Superior Court in Canada under the Canada Evidence Act for an order compelling the testimony of a witness or for the production of documents.

1484. Canada will also provide what assistance it can in response to a non-treaty letter of request. However, the scope of such assistance is limited to what can be provided without a court order since the evidence gathering powers in the MLACMA are available only to treaty partners and designated entities.

Conditions for refusal

1485. Where assistance is provided pursuant to a Treaty, the treaty itself restricts the use that can be made of the evidence concerning the matters set out in the letter of request. Where evidence has been gathered in Canada on behalf of a requesting state under the MLACMA, before the evidence can be sent to the requesting state, a judge must, by order, authorise the transmittal of the evidence. Affected parties may ask the judge to impose conditions on the sending of the evidence to the requesting state. In the majority of cases, sending orders are unconditional. In the few instances where a judge does impose conditions on the sending of the evidence, they are usually restricted to protecting the interests of those from whom evidence has been obtained. In this regard, a typical condition would be that the evidence be returned at the conclusion of all proceedings in the requesting state.

1486. Canada does not require that there be judicial proceedings underway in order to provide legal assistance. The exception is in cases where assistance is provided pursuant to a letters rogatory request and where a treaty request is made for the enforcement of foreign orders for restraint, seizure and forfeiture. In order for a letters rogatory request to be executed, there must be a matter pending before the court in the foreign jurisdiction, and therefore pre-trial investigatory assistance would not be available in the absence of a treaty. In the case of requests for the enforcement of foreign orders of restraint or seizure, the person must be charged with an offence which is also an indictable offence in Canada. In the case of requests for enforcement of a forfeiture order, the person must have been convicted of an offence which would be an indictable offence in Canada, if it had occurred in Canada. This latter situation is the only instance where Canada requires evidence of a conviction in order to provide assistance.

1487. Except in the case of requests for the enforcement of foreign orders of restraint, seizure and forfeiture, Canada does not require dual criminality in order to provide assistance and does not seek to include dual criminality as a requirement in the mutual legal assistance treaties that it negotiates. The analysis of whether dual criminality is established is conduct-based. That is, if the conduct is criminalized in both countries, it will be concluded that this criterion is satisfied, whether or not the denomination or the precise constituent elements of the respective offences are identical.

1488. Canada's MLATs typically contain a provision allowing for the refusal of a request for mutual assistance on the basis that it would be contrary to Canada's public interest to execute the request. Canada may use this provision to delay the execution of a request if execution would compromise a Canadian investigation.

1489. *Fiscal matters.* Canada does not impose a restriction on mutual legal assistance in criminal matters requests in Canada on the sole ground that the offence is also considered to involve fiscal matters. The MLACMA does not contain any reference to such limitations and it is not contained in Canada's bi-lateral treaties.

1490. *Secrecy.* According to the IAG, requests to Canada for mutual legal assistance will not be refused on the grounds of laws that impose secrecy or confidentiality requirements on financial institutions or DNFBP. Records of financial institutions are obtainable in Canada under the MLACMA and the PCMLTF does not contain any restrictions in that regard either.

1491. Where legal professional privilege, known in Canada as solicitor-client privilege, affects evidence sought in Canada and it is not waived, the evidence will not be ordered, produced or sent. The search of law offices in Canada is subject to many restrictions and close judicial oversight (see Lavallee, Rackel and Heintz v. Canada (Attorney General); White, Ottenheimer and Baker v. Canada (Attorney General; R. v. Fink [2002] S.C.C. 61).

Process for executing requests

1492. The Department of Justice is responsible for the implementation of mutual legal assistance agreements and the administration of the MLACMA. The IAG carries out the functions assigned to the Minister of Justice under the MLACMA and provides advice to the Minister regarding his or her responsibilities under the statute. The IAG is designated as Canada's Central Authority in mutual assistance agreements. It is located at the headquarters of the Department of Justice in Ottawa. The MLA process is thus a centrally coordinated process.

1493. The MLACMA establishes a two-phase process for the gathering of evidence, which is briefly summarized as follows. The first phase is performed by counsel at the IAG. As the Minister's delegates, counsel at the IAG receive, review, approve and arrange for the execution by competent Canadian authorities of mutual legal assistance requests made to Canada by treaty partners or designated entities in criminal matters. The IAG ensures that all mutual legal assistance requests comply with treaty provisions and any other international or domestic standards that may be applicable. Canada did not provide any statistics on how long this stage generally lasts.

1494. Once a request has been approved, the second or judicial phase is triggered. It is at this stage that an application must be made to court for an order compelling the production of evidence or authorizing its seizure. Canada is a federal state with prosecutorial authorities at both the federal and provincial level. An approved request from a foreign state will be sent to either the regional office of the federal Department of Justice or to the office of the relevant provincial Attorney General depending upon the nature of the offence under investigation or prosecution in the requesting state. If the offence relates to drug trafficking, immigration, tax evasion, or another matter that is prosecuted by federal officials in Canada, the request will be sent to a regional office of the Department of Justice. If the offence is one that would be prohibited by Canada's Criminal Code, the request will be sent to the office of the provincial Attorney General in the province where the evidence is believed to be located. After the evidence has been gathered or seized pursuant to orders obtained under MLACMA, a second application must be made to a superior court judge for an order authorizing the transmittal to the requesting state of the gathered evidence.

1495. The MLA work of the IAG is handled by six of the 16 IAG lawyers, with the other ten lawyers focusing on extradition. The 6 paralegals and support staff are divided into extradition and mutual legal assistance teams. The IAG works in close cooperation with federal and provincial investigative and prosecutorial officials in executing incoming requests and in the process of making requests to other countries. In the major urban centres of Vancouver, Toronto and Montreal, the regional offices of the federal Justice Department also maintain teams of lawyers dedicated to handling both extradition and mutual assistance requests. The British Columbia Regional Office of the Department of Justice in Vancouver executes all incoming requests for assistance which are to be executed in that province. In Ontario and Quebec, the provincial Attorneys General similarly maintain teams dedicated to the execution of incoming requests.

1496. Canada has posted two experienced Canadian criminal counsel abroad. Two liaison positions have been established in Europe: one in Brussels for the European Union, and the other in Paris dealing primarily with extradition and mutual assistance requests to and from France.

1497. Canada did not provide information (as requested) about the actual or average length of time it takes to respond to money laundering assistance requests. In the absence of such data, the effectiveness of the system cannot be assessed.

1498. Statistics provided reveal that in the last five years Canada received 167 MLA requests (143 requests for evidence in money laundering cases). 46 of the total MLA requests were withdrawn by the requesting state (41 of these were ML MLA requests), which is about 25% of the total. Information on the reasons for these withdrawals is unknown to the team and Canada. Canada executed and complied 90 of the remaining 121 total MLA requests, currently leaving 31 outstanding requests which are presumed to be more recent requests.

Application of Recommendation 28 to request for mutual legal assistance

1499. The powers of competent Canadian authorities required under Recommendation 28 are available for use in response to requests for mutual legal assistance. Canada's mutual legal assistance measures apply equally to money laundering, terrorism and financing of terrorism offences. Where the request is made pursuant to a treaty, the offence must be one covered by the treaty. If there is no treaty, and the request is one by letter rogatory, then there are serious limitations. Under the MLACMA, there is the power to compel a witness to provide a statement other than at trial, which is not provided to Canadian police in domestic investigations, except for the investigation into a terrorism offence (see section 83.28 of the Criminal Code).

Mechanisms for determining the best venue for prosecution

1500. While there is no statute that applies to the determination of which country is best equipped to prosecute a matter, there is case law that sets forth the criteria that govern the exercise of discretion by Canadian prosecutorial authorities. The Supreme Court of Canada decision in *U.S.A. v. Cotroni* sets forth the test for when Canadian citizens should be prosecuted in Canada or abroad for their alleged criminal conduct. The determination of where a person may be prosecuted depends to a large extent on where the person is arrested. In cases where there has been a joint investigation involving Canadian police and their foreign counterparts, Canadian police do take part in consultations with their counterparts about the ultimate point of arrest. In cases where a person is arrested in Canada, who might simultaneously face the possibility of a Canadian and foreign prosecution based on the same conduct, there may be a request made to Canada for extradition[178]. There may be consultation between Canadian and foreign prosecution authorities on the appropriate territorial jurisdiction for the prosecution. Many of Canada's extradition treaties specifically provide for such consultation. Ultimately, the Courts in Canada leave the decision to prosecute or extradite in the hands of the Prosecution Service and the Department of Justice.

Additional elements

1501. As noted above, the powers to compel the production of evidence or authorise its seizure at the request of foreign authorities under the MLACMA are available only when the request is made pursuant to treaty or by a designated entity. Such requests must be made to Canada's central authority by the central authority of the requesting state or designated entity and if made directly police-to-police an MLACMA request is subsequently required to actually process the court order. Not all of the criminal investigatory tools are available for a judge who is considering a letter rogatory request, which limits the methods for obtaining evidence to the more limited production orders. Subsection 3(2) of the MLACMA specifically recognizes and maintains normal police to police contacts and arrangements. Where a foreign police agency provides evidence to its Canadian counterpart of the commission of an offence under Canadian law, Canadian police may choose to obtain an order under the Criminal Code or other domestic legislation to obtain the evidence for the Canadian investigation and may then be able to share that evidence with foreign authorities.

[178] Article 6 of the Canadian Charter of Rights and Freedoms protects the "right to remain in Canada for Canadian citizens", in cases where a Canadian citizen might either be prosecuted in Canada or extradited in relation to the same alleged conduct, the appropriate Attorney General within Canada (either federal or provincial) will perform an assessment based on factors identified under Canadian case law in order to determine whether prosecution in Canada is a "realistic" option in all of the circumstances.

1502. The discussions regarding Recommendation 36 (Criteria 36.1 – 36.6) also apply to mutual legal assistance requests related to terrorist acts and the financing of terrorism as they are offences in Canada.

Recommendation 37 & Special Recommendation V

1503. Except where direct enforcement of foreign orders for restraint or forfeiture of assets is requested, Canada does not require dual criminality for execution pursuant to the MLACMA.

1504. Canada does require dual criminality for extradition. However, because Canada uses a conduct oriented test, Canada will extradite where the conduct in issue would be a serious offence if it had been committed in Canada regardless of the fact that all of the elements of the foreign offence are non-congruent with all the elements of an offence in Canada (see section 3(2) of the Extradition Act).

1505. The discussions regarding Recommendation 37 (Criteria 37.1 – 37.2) also apply to mutual legal assistance requests related to terrorist acts and the financing of terrorism as they are offences in Canada.

Recommendation 38 & Special Recommendation V

1506. Under the MLACMA, Canada can directly enforce foreign orders for the restraint, seizure and forfeiture of assets on receipt of a request from a treaty partner or designated entity (see MLACMA sections 9.3 and 9.4). An order made by a court of criminal jurisdiction can be filed with the court in Canada and enforced as though it were an order of a Canadian court where the person has been charged in the requesting state or by the designated entity with an offence that would be an indictable offence were it to have been committed in Canada. This means, for example, that the owner or person in possession may challenge the order or apply to the Canadian court for the payment of legal, living and business expenses from the seized or restrained property. The property remains under the Canadian court's control while the foreign proceedings continue.

1507. With respect to foreign forfeiture orders, they may be filed and enforced as though they had been issued in Canada where the order has been issued by a court of criminal jurisdiction and the person has been convicted in the requesting state of an offence that would be an indictable offence were it to have been committed in Canada. The Minister of Justice must refuse a request for the enforcement of a foreign forfeiture order where the Minister has reasonable grounds to believe the request has been made for the purpose of punishing a person by reason of their race, sex, religion or other prohibited grounds. The Minister must also refuse where, in his or her opinion, giving effect to the order would prejudice an ongoing investigation, would impose an excessive burden on Canadian government resources, might prejudice Canada's security or where refusal of the request is in the public interest. Enforcing foreign restraint orders and forfeiture judgments can be cumbersome since the enforcement of such orders depends more upon the sufficiency of the foreign requests than would be the case in requests for legal assistance seeking evidence. The requesting state has to provide very detailed information regarding the grounds for the restraint, almost to a level of detail ordinarily reserved for obtaining domestic restraint in the first instance, even though under MLACMA the Canadian courts are not supposed to look behind the foreign order, but simply enforce same as if it were an order issued by a Canadian court. See MLACMA Section 9.3(4). Enforcing forfeiture orders has been done successfully, but it seems that the number of successful requests is not numerous: only four times in five years. Canada was unable to demonstrate to the assessors the effectiveness of the assistance it provides to foreign governments in confiscation matters.

1508. Although Canada initially provided statistics on the number of MLA requests it handled in a 5-year period, and then later provided some information on the success rate of those requests, it did not provide information about the average time in which MLA requests were executed in general or with regards to the relatively few forfeiture matters it handled nor explained any of the results Only 40% of forfeiture requests over the last five years were executed. In the absence of more compelling

MLA and extradition statistical data, the assessment of the MLA system's effectiveness is based on other information that was made available to the assessors. Canada on average has shared a little under CAD 100 000 in forfeited funds a year with its foreign partners. Considering that Canada forfeits about CAD 33 million in assets per annum, this international sharing figure seems low.

1509. Canada's MLA provisions for confiscation seem to encourage duplicative and potentially conflicting litigation in Canada. Presumably, Canada would not enforce forfeiture orders from foreign states that did not permit affected innocent owners the opportunity to challenge a confiscation order in the requesting state as the MLACMA gives the Minister relatively broad discretion to refuse to execute MLA requests if they are not in the interest of Justice. Nonetheless, Canada's MLA provisions, via MLACMA Section 9.4(9), incorporates Sections 462.41(3) and 462.42 of the Criminal Code, which permit any person, other than the accused, who is affected by a foreign restraint, seizure or forfeiture order to fully challenge the validity of the same in Canada and raise the "innocent owner" defence in Canada. There is no presumption of validity of the foreign order under Canadian law nor does MLACMA recognize that third-party property rights may have already been adequately protected by similar procedures in the foreign jurisdiction. This lack of comity results in the potential duplication of legal decisions made abroad, superimposes Canada's version of forfeiture onto foreign forfeiture regimes and proceedings, and creates the possibility of conflicts with the laws of requesting state and previous legal decisions made in the requesting state. A foreign judge handling a foreign forfeiture case would always be in better position to determine who is or is not an innocent owner, but Canada reserves the right to possibly hear or rehear that issue in Canada. Similarly, a Canadian judge can reduce a foreign forfeiture order of offence related property based upon "the proportionality" of the forfeiture to the offence giving rise to forfeiture and that claim can be brought by the accused. See MLACMA Section 9.4(9) incorporating Section 490.41(3) of the Criminal Code. This issue would normally be litigated in the requesting state.

1510. This duplication of the opportunity to make challenges in international confiscation matters increases the chances that defendants can bring lengthy legal battles in Canada. Proceeds of crime restrained for foreign governments may be released by a Canadian court to pay for legal fees and living expenses of the foreign criminal defendant under Canadian law prior to property being forfeited under the foreign law even if that would not be permitted under the applicable foreign law. This has the potential of undermining the criminal or forfeiture processes taking place abroad. The statement that the Section 462.34 financial hardship provisions apply to foreign forfeitures is odd given the fact that the innocent owner and proportionality provisions of the Criminal Code are expressly incorporated into the MLACMA, but the Criminal Code provisions that permit the release of frozen proceeds to pay for attorney fees or business and living expenses provisions are not as there is no specific reference to Section 462.34 of the Criminal Code in the MLACMA. Compare Section 9.3(4) with Section 9.4 (6) and (9).

1511. Canada can enforce foreign criminal orders for restraint, seizure or forfeiture, as described above, as long as they relate to the proceeds of crime or offence-related property. MLACMA does not provide for the enforcement of orders against property that is the equivalent value of forfeitable property, but has the power to enforce an order for "the payment of a fine" imposed in respect of an offence by a "court of criminal jurisdiction". Canada treats value based forfeiture judgements as fines. This means generally that Canada cannot enforce preliminary orders from legal systems that allow Courts to issue restraining orders in anticipation of an equivalent value forfeiture judgment until after the requesting state has actually obtained a final forfeiture judgement. The problem with this approach is that some jurisdictions, including Canada, do not have restraint mechanisms that can be used to place pre-judgement holds on non-tainted assets in anticipation of obtaining a fine or a value-based forfeiture judgement. Moreover, while the MLACMA has provisions that authorize Canadian courts to enforce foreign pre-judgment orders that seize or restrain proceeds or offence related property in anticipation of a forfeiture judgement against such identified proceeds or offence related property, the MLACMA does not provide similar authority for the enforcement of pre-judgment restraint or seizure orders obtained for anticipated fines or value-based forfeiture judgments.

1512. The IAG as Canada's central authority works closely with other central authorities and with investigative agencies. The timing of the execution of searches and seizures may be coordinated if Canada is provided with sufficient notice of the impending action in the requesting state. In situations where Canadian police are in a position to apply for orders under the Criminal Code for seizure, they may coordinate their actions with foreign counterparts. However, Canada has no formal arrangements or mechanisms were the confiscation experts in one country regularly meet with their Canadian counter parts. Confiscation coordination is ad hoc at best, and has been problematic with at least one major treaty partner. Canada does not seem to involve specialized confiscation points of contact, but, instead, seems to rely upon a central authority competence in confiscation law that rarely is present in most central authorities throughout the world.

1513. At the Federal level, Canada has not established an asset forfeiture fund that allows dedicated use of forfeited assets in a systematic way. Canada advised the assessment team that it had considered an asset forfeiture fund at a federal level to promote law enforcement, health education or other appropriate purposes, and decided against it, although Canada did not detail the process of their consideration. Forfeited funds can be shared with domestic and foreign law enforcement partners and the recipients themselves determine how those funds may be used or spent. There are riders on forfeited funds that the Federal government shares with the provinces requiring that the shared funds be used law enforcement, criminal justice and drug education purposes. Forfeited funds that are not shared eventually go into the general treasury and are spent by the Canadian Parliament as it sees fit.

1514. The Seized Property Management Act, which outlines Canada's proceeds of crime and offence related property asset management regime, includes authority to share anything forfeited to Canada in section 9(d) of that Act. Essentially, this provision allows Canada to share the "proceeds of disposition" (*i.e.* the money realised from the sale of forfeited assets). The Seized Property Management Act also specifically recognizes international sharing in section 11of the Act. Sharing must occur in accordance with the Act and the applicable Regulations.

1515. The Canadian Sharing Regulations allow Canada to share with a foreign government that participated in an investigation or prosecution that resulted in the forfeiture or provided information relevant thereto. There also must be a reciprocal forfeiture agreement with Canada for such sharing to be authorised. Canada has entered into many asset sharing arrangements with foreign states and is negotiating a number of additional agreements. Canada shares net proceeds after the forfeited items are liquidated, and cannot share an item in specie, that is, give the item to the other government to place into official use.

Additional elements

1516. As mentioned above, foreign orders for forfeiture must have been made by a "court of criminal jurisdiction" in order to be eligible to be enforced under the MLACMA. As most non-conviction based confiscation systems are "civil" in nature Canada cannot enforce such orders, even though many foreign Courts issuing such judgment are enforcing criminal laws and may in fact be acting under their criminal jurisdiction. This inability to enforce foreign *in rem* judgments does not apply in several Canadian provinces which have enacted comprehensive civil forfeiture legislative regimes. Canada indicated that constitutional issues eliminated this as a federal option, as only provinces have the competence to run civil court systems.

1517. The discussions regarding Recommendation 38 (Criteria 38.1 – 38.3) also apply to mutual legal assistance requests related to terrorist acts and the financing of terrorism as they are offences in Canada.

Statistics

1518. Inadequate statistics are maintained by the Department of Justice on some matters relevant to the effectiveness and efficiency of Canada's extradition and mutual legal assistance activities in

combating money laundering and terrorist financing. The IAG electronically records the receipt of a request, the requesting country, the nature of the request and when the file is closed. Special note is made of mutual assistance requests related to terrorism, money laundering and proceeds of crime.

1519. Canada responds to requesting countries immediately to confirm receipt of requests. The IAG is in regular contact with its counterparts to provide timely information regarding the execution of requests for assistance. Information was sought on the average time within which a request for assistance is executed but the data was not provided.

1520. The following table indicates the mutual legal assistance requests received and made by Canada for all offences from 2001-2006:

	Requests incoming	**Requests outgoing**	**Total**
2001-2002	387	140	**527**
2002-2003	406	104	**510**
2003-2004	311	84	**395**
2004-2005	318	77	**395**
2005-2006	350	84	**434**

1521. The following table indicates the mutual legal assistance requests received and made by Canada relating to money laundering, terrorism and financing of terrorism from 2001-2006:

	Requests involving money laundering – incoming	**Requests involving money laundering – outgoing**	**Requests involving terrorism – incoming**	**Requests involving terrorism – outgoing**	**Requests involving financing of terrorism – incoming**	**Requests involving financing of terrorism – outgoing**
2001-2002	22	38	5	5	2	0
2002-2003	32	15	8	2	3	0
2003-2004	28	14	6	4	1	0
2004-2005	23	32	4	1	2	0
2005-2006	38	14	4	4	1	0

1522. Canada indicated that the total number of mutual legal assistance requests received in all categories for the period between 2001 and 2006 is 167 and as follows:

MONEY LAUNDERING

Requests receive	143
Requests executed	78
Requests withdrawn/abandoned	41
Requests still active	24

RESTRAINT/FORFEITURE

Requests received	10
Requests executed	4
Requests withdrawn/abandoned	3
Requests refused	1
Requests still active	2

TERRORIST FINANCING

Requests receive	14
Requests execute	8
Requests withdrawn	2
Requests still active	4

1523. The following table indicates the value of the forfeited goods shared with other states:

Year	Value of forfeited goods
2002	CAD 153 000 (shared with Foreign States)
2003	CAD 18 500 (shared with Foreign States)
2004	CAD 270 000 (shared with Foreign States)
2005	CAD 54 000 (shared with Foreign States)
2006	N/A

6.3.2 Comments and Recommendations

1524. Canada has some problems with providing efficient MLA assistance. Canada should keep better MLA statistics than were provided to the assessors. Canada should consider options for streamlining judicial assistance such as streamlining processes to get financial and business records for foreign criminal investigations and consider devising a system that requires less judicial oversight of such matters. Not all involuntary production of business records or testimony should require judicial inquiries or oversight. For example, only if a party raises a valid legal objection to a production order should there be a need for judicial intervention.

1525. Canada should consider ways to give foreign confiscation requests more weight and become less subject to Court interference with the foreign criminal process. For example, Canada could make forfeiture assistance contingent upon the requesting state having a process that permits affected third-parties to challenge the forfeiture and that the proceedings in the foreign state otherwise comport with the Canadian concepts of due process, and then let the AG make that initial determination and place the burden upon the party challenging the foreign request to show that the requesting state's process for challenging a forfeiture falls below Canadian Constitutional standards. Canada should consider devising a way of executing foreign value based forfeiture judgments and related freeze, seizure or restraint orders to the same extent it can encumber proceeds and offence related assets before a foreign forfeiture judgment is obtained. Or, in the alternative, within the parameters of Canada's Constitutional framework, provide for pre-conviction restraint of an accused's assets for the payment of any potential fine, thereby protecting those assets from dissipation before the foreign court issues the fine, or value based forfeiture judgment.. Canada should create an informal process for the coordination of international confiscation cases jointly with the RCMP, the IAG and the prosecution service entities that execute MLA requests and their counter-parts in foreign governments so that these case can be handled more expeditiously and by persons who are experts in forfeiture law.

1526. Canada should allocate more resources to the authorities in charge of processing MLA requests.

6.3.3 Compliance with Recommendations 36 to 38 and Special Recommendation V

Rec.	Rating	Summary of factors underlying ratings
Rec.36	LC	• There are concerns about the ability of Canada to handle MLA requests in a timely and effective manner and effectiveness of the current regime cannot be demonstrated due to the lack of adequate data.
Rec.37	C	• The Recommendation is fully met.
Rec.38	LC	• There are doubts about the effectiveness of the measures in place under Recommendation 38: there is limited evidence of effective confiscation assistance as only four cases have been successful in last 5 years and international sharing statistics indicate that while asset sharing with foreign states is possible, it rarely occurs. Canada executes requests to enforce corresponding value judgments as fines, which has limitations and cannot be enforced against property held by third parties.
SR.V	LC	**Regarding compliance with Recommendation 38** • All elements missing in R. 38 are missing for SR.V; • There are concerns about the ability of Canada to handle MLA requests in a timely and effective manner and effectiveness of the current regime cannot be demonstrated due to the lack of adequate data.

6.4 Extradition (R.39, 37 & SR.V)

6.4.1 Description and Analysis

Recommendation 39 & Special Recommendation V

1527. *ML as an extraditable offence*. The money laundering offence is an extraditable offence under Canada's Extradition Act. Money laundering is a criminal offence under the Criminal Code and thus the dual criminality aspect of extradition can usually be met.

1528. The Minister of Justice is responsible for the implementation of extradition agreements, the administration of the 1999 Extradition Act ("Act"), including the processing of requests for extradition or provisional arrest under the Act or an applicable agreement. The Act provides that if certain preconditions are met a person may be extradited: 1) for the purpose of prosecution, 2) for the purpose of imposing a sentence on the person, or 3) for the purpose of enforcing a sentence already imposed on the person. Canada is party to 50 bilateral extradition treaties and has designated a number of countries as extradition partners.

1529. Canada's assistance under the Act may be engaged on the basis of 1) an extradition treaty between Canada and the state or entity making the request, 2) a multilateral agreement to which both Canada and the requesting party are signatories and which contains a provision on extradition, 3) a specific agreement entered into between Canada and the requesting state or entity with respect to a person or persons in a particular case, and 4) a general designation of the requesting state or entity as an "extradition partner" under the Act thereby allowing the extradition partner full coverage under the provisions of the Act notwithstanding the absence of an extradition treaty. In addition to a number of members of the Commonwealth, Canada has designated as extradition partners, two non-commonwealth countries, Costa Rica and Japan, as well as the International Criminal Court, and International Criminal Tribunals concerned with the prosecution of persons responsible for violations of international law in Rwanda and in the Former Yugoslavia.

1530. A request for provisional arrest may precede a formal request for extradition. Provisional arrest refers to a request for the apprehension of an individual, generally in circumstances of urgency or a similar ground of public interest, prior to the preparation of the documentary material upon which the formal extradition will be requested. A provisional arrest request may be made through Interpol.

1531. The Minister of Justice has the discretion to approve an application for a provisional arrest warrant if satisfied that a) the offence in question is subject to certain minimum penalty requirements set out in the Act, and 2) the extradition partner will make a formal request for the extradition of the person within a given time-period (specified by the treaty, other agreement or the Act) subsequent to the person's provisional arrest. Once a formal extradition request is received, the Minister of Justice may issue an authority to proceed. An authority to proceed authorises an extradition hearing to be held in order to consider whether the person should be committed for extradition.

1532. Once approved, the IAG forwards the request and all supporting material to the regional office of the Department of Justice in the jurisdiction where the person sought is believed to be located. That regional office will assign legal counsel to initiate and assume conduct proceedings before a judge to seek an order for the committal for extradition of the person. Regional counsel will also represent the extradition partner and the Minister of Justice throughout any appeal or judicial review proceedings.

1533. The person whose extradition is sought appears at the extradition hearing and participates through his legal counsel or directly. The Canadian offence that corresponds to the conduct supported by the foreign request will be identified by IAG counsel and named in a document called an Authority to Proceed ("ATP"), which is filed with the Canadian court before judicial proceedings begin. In the case of a person sought for the purpose of prosecution, the judge will determine if the evidence provided by the extradition partner is such that the person would be committed for trial in Canada if

the conduct had occurred in Canada and the corresponding offence had been charged in Canada. In the case of a person sought for the imposition or enforcement of a sentence the judge will determine if the person has been convicted with respect to conduct that corresponds to the Canadian offence listed in the ATP. Where the person sought for extradition has been convicted in the foreign State in absentia, the matter will be treated in Canada has though it were a request for prosecution rather than imposition or enforcement of a sentence.

1534. The Extradition Act allows evidence to be presented at the extradition hearing in a variety of ways: 1) in the usual manner applicable to Canadian domestic proceedings such as through the testimony of witnesses, or 2) in reliance on the provisions for the introduction of evidence set out in an applicable extradition arrangement, or 3) by means of a "record of the case". Evidence gathered in Canada must satisfy the rules of evidence under Canadian law in order to be admitted.

1535. The Extradition Act renders admissible at the extradition hearing a document called the Record of the Case, which summarizes the evidence available to the extradition partner for use in the prosecution, notwithstanding the fact that this document contains evidence otherwise inadmissible in Canadian domestic proceedings, as long as certain safeguards are respected. This includes having a judicial or prosecuting authority of the extradition partner certify that the evidence summarized is available for trial and is either sufficient to justify prosecution or gathered in accordance with their law. If the presiding judge is satisfied with the evidence, he or she will order the person detained pending the Minister of Justice's decision whether to surrender the person. Otherwise, the person will be discharged and released.

1536. The judicial phase of the extradition process is a determination only that the evidence is sufficient to warrant that the person be extradited. The ultimate decision with respect to whether the person will in fact be surrendered to the extradition partner is that of the Minister of Justice. At this phase of the process the Minister of Justice will consider any representations from the person or the person's counsel with respect to why the person should not be extradited or concerning any conditions to which the surrender order should be subject. In reaching a decision on surrender the Minister of Justice will be obliged to weigh the submissions of the person against Canada's international obligations with respect to extradition. The Minister of Justice in reaching his or her decision must respect the rights of the person sought as guaranteed by the Canadian Charter of Rights and Freedoms.

1537. If the person sought for extradition is serving a sentence in Canada, the Minister of Justice may order temporary surrender so that the person can face prosecution or appeal proceedings in the courts of the extradition partner and then be returned to Canada to serve the remainder of his or her outstanding sentence here. While the Minister of Justice relies upon advice from the IAG, he or she decides personally in each case. When the Minister of Justice agrees to surrender the person, the IAG helps coordinate arrangements for the actual transfer of the person to authorised agents of the requesting state or entity.

1538. *Extradition of nationals*. Canada can extradite its own nationals subject to the discretionary ground of refusal set out in section 47 of the Extradition Act or the relevant extradition agreement. Any actions taken by Canadian authorities in relation to a foreign request for extradition will be governed by the Canadian Charter of Rights and Freedoms. The Charter is a part of Canada's Constitution, which is the supreme law of Canada. The Charter guarantees certain rights and freedoms. For example, Section 6 of the Charter gives Canadian citizens "the right to remain in Canada." This means that where the person sought for extradition is a Canadian citizen and the offence for which extradition is requested is one that is capable of being prosecuted in Canada, the relevant Canadian Attorney General (either federal or provincial) must perform an assessment of whether prosecution in Canada is a "realistic" option. The assessment, known as a "Cotroni assessment", is based on factors that were enumerated in a decision from the Supreme Court of Canada called U.S.A. v. Cotroni [1989] 1 S.C.R. 1469. Historically, the result of most of these assessments has been to favour extradition.

1539. *Delays to process extradition requests*. The Extradition Act sets out time lines for specific steps to ensure minimal delays. For example, it is expected that extradition cases are to take priority at courts. The Extradition Act contains provisions calling for early dates to be set in extradition matters. The Department of Justice Canada has also created specialized teams throughout the country to help deal more swiftly and efficiently with requests for extradition and mutual legal assistance.

1540. The Extradition Act sets out time lines for specific steps in the extradition process to ensure minimal delay. Extradition cases are to take priority in accordance with section 21(3) of the Extradition Act: "The judge shall set an early date for the extradition hearing, whether that date is in or out of the prescribed sessions of the court." Extradition appeal cases are to take priority in accordance with section 51 of the Extradition Act: "An appeal under this Act shall be scheduled for hearing by the court of appeal at an early date whether that date is in or out of the prescribed sessions of that court."

1541. The use of the diplomatic channel is not mandatory in Canada as the Department of Justice is designated by Statute as the Central Authority for the implementation of extradition agreements, the administration of the Extradition Act and requests for extradition made under them. A few of Canada's more recent extradition treaties reflect this by providing for direct transmission of extradition requests between Canada's Department of Justice and Canada's treaty partner's appropriate authority. However, per international convention and the great majority of Canada's extradition agreements, extradition requests generally continue to be conveyed through diplomatic channels.

1542. *Statistics*. Canada provided the number of formal extradition requests it has received in a five year period from 2001 to 2006 and data showing the number of completed and abandoned incoming MLA requests, but did not provide any data on how long those requests were pending, or explain why requests were abandoned or denied. Only 24 of 106 persons requested for extradition over the last five years (less than 25%) have been returned to the requesting state.

1543. The following table indicates the number of extradition requests received and made by Canada for all offences from 2001-2005:

	Incoming requests	Outgoing requests	Total
2001	148	52	**200**
2002	187	37	**224**
2003	200	41	**241**
2004	178	36	**214**
2005	183	31	**214**

1544. The following table indicates the number of extradition requests received and made by Canada relating to money laundering, terrorism and financing of terrorism from 2001-2005:

	Requests involving money laundering – incoming	Requests involving money laundering – outgoing	Requests involving terrorism – incoming	Requests involving terrorism – outgoing	Requests involving financing of terrorism – incoming	Requests involving financing of terrorism – outgoing
2001	9	4	4	0	2	0
2002	5	2	3	0	0	0
2003	9	1	1	0	2	0
2004	17	2	1	0	0	0
2005	14	1	3	0	0	0

1545. There were 58 incoming requests relating to money-laundering and TF, but there were 106 persons sought for extradition as follows:

Money Laundering: Total of 103 persons sought for extradition[179]

- 23 individuals were returned to the Requesting State.
- The requests for 28 individuals were abandoned or withdrawn.
- For 52 individuals, the cases are still pending (that is, either the person has still not been located or the case is still at some stage of the extradition process, including the judicial, ministerial and appellate stages).

Terrorist Financing: Total of 3 persons sought for extradition

- 1 returned.
- 1 request withdrawn.
- 1 still ongoing.

1546. Recommendation 39 (Criteria 39.1 – 39.4) also applies to extradition proceedings related to terrorist acts and the financing of terrorism as they are offences in Canada.

Additional elements

1547. Persons cannot be extradited based only on warrants of arrests or judgements. There must be an assessment of the evidence, which takes place in the course of the judicial phase, which is followed by the Ministerial phase of the extradition proceedings.

1548. The simplified procedure of extradition of consenting persons who waive formal extradition proceedings will speed up the process and is set out in sections 70 -71 (consent) and section72 (waiver of extradition) of the Extradition Act For purposes of waiver, a description of the evidence (record of the case) is sufficient and certain ministerial acts are waived. Some of the cumbersome Ministerial approvals are dispensed with as well.

Recommendation 37 (dual criminality relating to extradition) and Special Recommendation IV

1549. With respect to extradition, dual criminality is required. Dual criminality requires that the conduct constitute an offence in both countries and that it be punishable by a prescribed period of incarceration. By default, as provided in the Extradition Act, in most cases, for the offence to be extraditable, it must carry a maximum penalty of at least two years of imprisonment. However, particular treaties may fix a lower sentence as a minimum, as does the Canada-U.S. treaty, for example. Canada uses a conduct test and will only extradite where the conduct in issue constitutes an offence that carries the relevant sentence minimum. However, it is not necessary that the offence under Canadian law have the same name or precise constituent elements as the foreign offence.

6.4.2 Recommendations and Comments

1550. Canada should maintain better extradition request data and should consider doing a critical evaluation of the extradition process.

[179] Of the 52 matters on 24 May 2007, there were only 32 requests still pending.

6.4.3 Compliance with Recommendations 37 & 39 and Special Recommendation V

Rec.	Rating	Summary of factors underlying ratings
Rec.37	C	• The Recommendation is fully met.
Rec.39	LC	• Insufficient statistical data was provided to make a thorough assessment, particularly the assessment of the delay element, but even the limited data provided indicates that obtaining extradition from Canada quickly may be difficult.
SR.V	LC	**Regarding compliance with Recommendation 39** • No meaningful statistical data provided to assess delay element (effectiveness issue).

6.5 Other Forms of International Co-operation (R.40, SR.V & R.32)

6.5.1 Description and Analysis

Obligation to provide the widest range of international co-operation

Law enforcement authorities

1551. Law enforcement authorities in Canada regularly provide informal assistance to police forces from other countries, in accordance with the laws of Canada. Generally, Canadian police are able to provide information or documentation that is publicly available or those that can be obtained on a voluntary basis. This usually involves direct communication between the police forces and may include transmission of information through Interpol.

1552. The RCMP is able to provide international cooperation to their foreign counterparts under Interpol, the international Liaison Officer (LO) program, MLAT and Extradition requests. The RCMP has formal arrangements that it can enter into with foreign counterparts for exchange of information, such as, Memoranda of Understanding (MOU) or Letters of Agreement (LOA). When sensitive information in the national interest is shared with or released to other governments, departments or organizations not covered by the Security Policy and Standards of the Government of Canada, the RCMP must ensure, through written agreements, *e.g.* MOU, that appropriate safeguards are established for the safekeeping of the information.

1553. The RCMP, in accordance with the Privacy Act, will share information related to domestic national security information with appropriate international agencies depending on that agency's "need and right to know" and in considering how such information would help further a criminal investigation. The RCMP includes with all outgoing written correspondence, messages and documents shared with other foreign agencies the required caveats that concern the ownership and the classification of the shared information. The RCMP may, with the Minister of PSEPC's prior approval, enter into a written or oral arrangement, or otherwise cooperate, with foreign security and intelligence organizations. This does not apply to foreign law enforcement agencies or organizations. National Security Investigations Section (NSIS) of the RCMP will be the point of contact for all foreign intelligence agencies in matters of national security.

1554. The RCMP Liaison Officer program was established to train and deploy highly skilled and multi-lingual regular members to strategic locations throughout the world. Partnering with international law enforcement agencies, foreign governments and Canadian embassies, the role of a LO is to maintain a link between Canadian law enforcement and the law enforcement agency of a host country to prevent and detect criminal offences against Canadian federal laws. Currently there are 35 RCMP liaison officers in 25 different locations in three geographic regions: Asia-Pacific/South Africa; Europe-Middle East-Africa; and Western Hemisphere.

1555. Mutual Legal Assistance Treaty (MLAT) requests and Extradition requests from participating countries are other mechanisms in which information is exchanged between international law enforcement agencies. A review of the money laundering investigational files indicate that through the

use of MLATs, Canada Law Enforcement provided the evidence/support for the restraint and eventual forfeiture of assets in the United States, Cuba, Antigua, the Cayman Islands, Switzerland and Luxembourg.

1556. The RCMP receives numerous requests to provide additional training internationally. Training has been provided to representatives from many countries including Columbia, Dominican Republic, Jamaica, Cuba, Austria, Czech Republic, Russian Federation, Peru, Venezuela, Hong Kong, Kenya, Panama, Bogotá, Pakistan, Bahrain, and Guatemala.

FINTRAC as an FIU

1557. FINTRAC is authorised to share information about suspected money laundering or terrorist financing with a foreign financial intelligence unit or similar foreign entity if a Memorandum of Understanding is signed between the two organisations. FINTRAC is authorised to receive information from these similar foreign entities when no MOU is signed between the two organizations. According to the PCMLTFA, the Minister of Finance or FINTRAC, with approval of the Minister may enter into a written agreement with a similar foreign entity for the exchange of information that there are reasonable grounds to suspect would be relevant to investigating or prosecuting a money laundering offence or a terrorist activity financing offence, or an offence that is substantially similar to either offence.

1558. When deciding to pursue an MOU with a similar foreign entity (hereafter FIU), FINTRAC considers a number of factors, including the following: Canadian foreign policy; FINTRAC's operational priorities; the FIU's enabling legislation; other jurisdictional legislation relating to curbing money laundering or terrorist financing; the privacy/access laws that exist in the jurisdiction (physical, IT and others); the jurisdictions participation in the FATF or FATF Regional-Style Bodies; the FIUs standing in the Egmont Group and adherence to the Egmont Principles of Information Exchange; and the measures that the FIU has in place to protect information. FINTRAC's signed MOUs are consistent with the Egmont Group Model MOU Template.

1559. Requests for information from MOU partners are normally received through the Egmont Secure Website (ESW) a secure communication channel used by most Egmont-member FIUs. Once an FIU query (FIUQ) is received FINTRAC sends an acknowledgment of receipt email via ESW. A copy of the FIUQ is made and immediately assigned to an analyst in order to determine if FINTRAC has transaction information related to the FIUQ. If so, analysts use all information available to them to build a case in response to the query. If FINTRAC does not have financial transaction information relating to the query received, a negative response is provided to the querying FIU. As a matter of practice, the assessment team was told that all queries are dealt with at least on a preliminary basis within 30 days or sooner for an urgent request. Negative responses are generally provided within five days of receipt of the query.

1560. The threshold for disclosing to foreign counterparts is the same as for domestic police forces, and once the analysts are of the view that the threshold has been met, the disclosure is worked through the same approval process described earlier with respect to domestic disclosures. Similarly, in its disclosures to foreign FIUs, FINTRAC provides the same designated information as it does domestically (see Section 2.5).

1561. If FINTRAC is in a position to disclose designated information in response to a FIUQ it is sent via ESW (provided the FIU has a current security certificate, to ensure the information that is being sent is encrypted). One of the stipulations of the MOU between FINTRAC and its foreign counterparts is that any information provided to the foreign agency may only be used for its intended purpose (investigation or prosecution of a money laundering or terrorist financing offence), and the information may not be further disseminated to any third party without the explicit prior consent of FINTRAC. FINTRAC also adheres to these stipulations regarding the information received from foreign FIUs.

1562. FINTRAC currently has 44 MOUs in place and continues to actively negotiate additional MOUs.

International Fora

1563. Canada has responded to the challenges of international cooperation by posting experienced Canadian criminal counsel abroad. Two liaison positions have been established in Europe: one in Brussels for the European Union, and the other in Paris, to coordinate Federal Prosecution Service (FPS)[180] (see Section 6.3 of the report).

Supervisors co-operation

1564. *FINTRAC.* Until the new provisions were enacted in December 2006, the PCMLTFA did not allow FINTRAC to exchange compliance-related information with its foreign counterparts. PCMLTFA now allows FINTRAC to enter into information sharing arrangements or agreements under new section 65(2) with any agency in a foreign state that has responsibility for verifying AML/CFT or with an overseas organization with respect to compliance information relating to any reporting entity under the Act as well as the assessment of risk relating to the institution's level of compliance.

1565. FINTRAC advised the examiners that at this time the organisation had not entered into any arrangements or agreements of this nature. In addition, FINTRAC has MOUs with most of the Canadian financial sector supervisors both at a federal and provincial level to receive compliance information from these agencies. Given the fact that FINTRAC is the supervisory agency as regards AML/CFT compliance issues and the wide range of institutions under AML/CFT obligations in Canada, to a large extent, FINTRAC would rely on the information received from federal and provincial regulatory agencies to meet requests for information from supervisory counterparts. However, the actual mechanisms for sharing are still in discussion.

1566. *OSFI*. Under the OSFI and Bank Act, the Superintendent of Financial Institutions is empowered to share information relating to banks with other agencies that are involved in the regulation of financial institutions provided that the Superintendent is satisfied that the information will be held by those agencies on a confidential basis.

1567. Although not required by law, OSFI generally shares information with overseas regulators via MOU. OSFI MOUs refer specifically to sharing information relating to terrorism and financial crimes. Financial crimes are specifically defined as money laundering, unauthorised banking, investment or insurance business and all other violations of law on financial markets. The crime of financing terrorism would not seem to be included as "…violations of law on financial markets".

1568. OSFI demonstrates effectiveness based on its co-operation in conducting cross border examinations in a number of countries in which its licensees have subsidiaries. Assistance has been rendered to OSFI in the absence of formal MOUs. However cross border examinations of institutions in Canada would be subject to a formal MOU requirement.

1569. *Provincial regulators*. Four provincial Securities Regulators (Ontario, Quebec, Alberta and British Columbia) are signatories under IOSCO's Multilateral Memorandum of Understanding Concerning Consultation and Co-operation and the Exchange of Information. However, the MOU examined did not refer to the exchange of information relating to AML/CFT. The definition of "laws

[180] The Federal Prosecution Service, through the National Security Group, is responsible for developing operational policy related to the prosecution of terrorism offences, providing legal advice to investigative bodies (*e.g.* Royal Canadian Mounted Police, Canada Border Services Agency (CBSA), etc.) in relation to the investigation of terrorism offences, and conducting prosecutions of terrorism offences involving the national interest and supporting prosecutions conducted by the provincial Attorneys General.

and regulations" under the MOU is expressly limited to issues relating to securities. However, this does not preclude securities regulators to exchange AML/CFT compliance information should their securities legislation permit it.

1570. The Ontario Securities Commission has its Office of Domestic and International Affairs that deals with overseas governments and regulators. Its governing statute at section 153 does also specifically refer to wide powers of the Commission to share information internationally with foreign regulators, stock exchanges, SRO and law enforcement authorities. This may permit the OSC to share information even in the absence of a MOU. The IDA has broad powers to share information with other regulatory and police agencies whether or not a formal information sharing agreement is in place. In Québec, section 297 and following of the *Securities Act* refer to broad powers of the *Autorité des marchés financiers* for sharing information with foreign and national authorities, including securities regulators, police forces, the Minister of Revenue or any other department, body or organization with whom the *Autorité des marchés financiers* may enter into an agreement to facilitate the administration or enforcement of securities and fiscal legislation as well as penal or criminal legislation.

1571. In the case of Credit Unions, there are several supervisors. In the case of the Deposit Insurance Corporation of Ontario, the Credit Union and *Caisses Populaires* Act does not provide DICO with the express power to share information (whether AML/CFT related or otherwise) cross border. In the case of the Financial Services Commission of Ontario the governing statute also seems to have this shortfall (there is no statutory authority for the Superintendent to share information under his general powers and duties in Section 5 of the Financial Services Commission of Ontario Act, 1997). Desjardins Group also plays a supervisory role in the case of its group of credit unions. Whilst Desjardins has demonstrated outreach to other jurisdictions to assist in development of Co-operative movement, the assessors did not see any basis for or evidence of the sharing of information with other supervisory counterparts on a cross border basis. Canada indicated that all credit union supervisors can exchange compliance information with international counterparts although there is no legal framework that explicitly authorises the exchange of such data.

1572. The assessors take the view that the main avenue for the cross-border sharing of supervisory information relating to AML/CFT compliance issues would be through FINTRAC, the main AML/CFT supervisory authority although there is no barriers to OSFI, the OSC, the IDA or the AMF sharing AML/CFT supervisory information with foreign counterparts. This mechanism of directing AML/CFT information through FINTRAC appears necessary given in particular the absence of legal framework for certain provincial regulators that explicitly authorises them to exchange AML/CFT compliance information with foreign counterparts.

Gateways and channels for prompt and constructive exchanges of information

Law enforcement authorities

1573. Canada became a member of International Criminal Police Organization in 1949, and the RCMP was delegated the responsibility for administering and operating the National Central Bureau (Interpol Ottawa). Interpol Ottawa is located at RCMP National Headquarters and forms part of the International Liaison Program. Interpol Ottawa works closely with the Canadian Central Authority and serves as the link between official Canadian and international law enforcement agencies. Interpol Ottawa is the central coordination point for the Canadian law enforcement community in pursuing criminal investigations abroad, establishing rapid contact with foreign police agencies and liaison officers, transmitting requests for information required in investigations to NCBs in other countries and assisting on judicial proceedings. Interpol Ottawa provides information on various organized crime groups and their activities, criminal activity with international ramifications, and provides money laundering information for use in countering international money laundering.

FINTRAC as an FIU

1574. FINTRAC has developed and implemented a process to obtain feedback from its partner FIUs about the query process and disclosures. The assessment team was told that FINTRAC has generally received positive feedback and is currently considering how best to respond to comments and to further strengthen these relationships.

Supervisors co-operation

1575. While FINTRAC as AML/CFT compliance supervisor now has legislative authority to share supervisory information, it must do so via agreement or arrangements with its international supervisory counterparts. FINTRAC has not entered yet into arrangements or agreements of this nature (although Canada indicated that FINTRAC is currently negotiating with several counterparts abroad) and therefore a serious issue arises as to the effectiveness of the system and the perceived inability at this point for an international supervisory counterpart to receive supervisory information relating to AML/CFT in sectors outside of those supervised by OSFI, IDA, the OSC and the AMF.

1576. Whilst OSFI is able to share AML/CFT compliance information on its FRFIs under the MOU that it executes with supervisory counterparts (and even possibly in the absence of such a MOU under the OSFI Law), the IOSCO MOU is restricted in terms of the information that can be shared and in several cases (not including the Ontario Securities Commission and the AMF in Québec the regulators themselves do not appear to have an inherent jurisdiction to share information on a cross border basis. The same situation appears to exist in the case of other provincial regulators.

Spontaneous exchanges of information or upon request

Law Enforcement authorities

1577. As described earlier in this Section, the RCMP is able to assist foreign counterparts with both spontaneous and more formally administered requests for information. These exchanges are subject to the RCMP information sharing protocols (see comments latter in this Section on controls and safeguards).

FINTRAC as an FIU

1578. As stipulated in the PCMLTFA, FINTRAC is authorised to exchange information, either spontaneously or upon request, in relation to money laundering offences, terrorist activity financing offences and offences that are substantially similar. Although FINTRAC can receive information about money laundering and the underlying predicate offence, FINTRAC can only provide information relevant to the money laundering offence (not about the underlying predicate offence). Since June, 30 2007, FINTRAC is able to share a larger amount of designated information, including "*the grounds on which a person or entity made a report under section 7* (i.e. *a suspicious transaction report) about the transaction or attempted transaction and that the Centre considers relevant in the circumstances*". An MOU between FINTRAC and the foreign agency must be in place to govern this exchange.

Supervisors co-operation

1579. FINTRAC's powers to share supervisory information will be dependent on the terms of the agreements or arrangements that would be established between FINTRAC and its supervisory counterpart. As these have not yet been established it is not clear whether information will be provided on a spontaneous basis as well as upon request.

1580. Information exchange will occur with OSFI in practice within the context of an MOU. However provided that the requirements of the Bank and OSFI laws are met, there would be no bar to

spontaneous information exchange. The MOU provides that for the most part, information requests must be made in writing but that in cases where expedition is required, then the request should be followed up in writing. The assessors also consider that the OSFI laws are framed widely enough for OSFI to share information even in the absence of a MOU.

1581. Similarly under the Securities Act of Ontario, the OSC can receive and provide information broadly with regulators and law enforcement. There is no legal limitation as to whether the information must be the subject to a request or whether it may be shared on a spontaneous basis. Canada indicated that the same holds true for the Autorité des marches financiers in Québec.

1582. The IDA has broad powers to share information with other regulatory and police agencies whether or not a formal information sharing agreement is in place.

1583. The assessors noted limitations as regards other provincial securities regulators whose information sharing is based on the IOSCO MOU. In addition there was no express power of provincial credit union supervisors to share AML/CFT information internationally.

Authorisation to conduct inquiries on behalf of foreign counterparts

Law Enforcement authorities

1584. The RCMP can use a number of criminal intelligence and police databases to conduct inquiries on behalf of foreign counterparts. The information contained in those systems is governed by different sharing protocols that aim at protecting the right to privacy of the individuals mentioned in the different databases.

FINTRAC

1585. FINTRAC is able to conduct inquiries on behalf of foreign counterparts in relation to with which it has an MOU. In such cases, FINTRAC is able to access its databases of all report types. FINTRAC is also able to access federal and provincial databases maintained for purposes related to law enforcement information or national security, and in respect of which there is an existing agreements, and to publicly available information, including commercially available databases, in developing the case. The threshold and limitations on designated information for disclosing the results of inquiries conducted on behalf of foreign counterparts is the same as previously discussed for domestic disclosures.

Supervisors co-operation

1586. Provided that there is an agreement or arrangement in place, FINTRAC may make queries relating to AML/CFT supervisory information on behalf of international counterparts and relate their findings to the requesting authority. FINTRAC has overarching powers to carry out inspections and otherwise obtain information from of financial institutions that are covered by the PCMLTFA. Additionally, it may rely on information received from domestic supervisors to respond to queries from these overseas counterparts.

1587. Both OSFI and the Ontario Securities Commission can make enquiries on behalf of international partners as regards AML/CFT issues and communicate these findings to the counterpart supervisor. In the case of other securities regulators, such exchanges may not be possible in the absence of express power to share AML/CFT information internationally.

1588. OSFI is not an investigatory body per se, and would be limited by its governing law to conducting investigations which relate to obligations under their own governing statutes.

Exchanges of information without disproportionate or unduly restrictive conditions

Law Enforcement authorities

1589. The RCMP is committed to exchanging information with foreign counterparts in circumstances that help to effectively combat money laundering and terrorist financing. The RCMP handles requests in accordance with all Canadian laws and its own internal procedures and protocols for information sharing. These procedures and protocols provide clear guidelines for proportionate classification of material along with the necessary conditions that must be enforced on protected, classified material.

1590. The RCMP also uses Interpol and the RCMP International Liaison Officer Program to help facilitate the flow of information between international policing agencies.

FINTRAC as an FIU

1591. FINTRAC's legislation requires that an MOU be signed and that a legal threshold be met to exchange information related to suspected money laundering and terrorist financing with an MOU partner. It is important to note that disclosures to MOU partners are similar to disclosures to domestic law enforcement and national security agencies.

Supervisors co-operation

1592. The exchange of supervisory information is not made subject to disproportionate or unduly restrictive conditions. FINTRAC's main criteria with regards to supervisory information is that there is an appropriate agreement or arrangement in place and that the compliance information will be kept confidential and used only for the purposes of ensuring compliance and measuring risks. In OSFI's case, the criteria are that the recipient agency is a supervisory agency and that the agency will keep the information confidential. In the case of the OSC the powers are broader. Other provincial regulators would have to rely on FINTRAC acting as a conduit for the exchange of information internationally.

Cases involving fiscal matters

1593. Under the PCMLTFA, FINTRAC may disclose designated information to an MOU partner when it has reasonable grounds to suspect that this information would be relevant to investigating or prosecuting a money laundering or a terrorist activity financing offence, or that is substantially similar to either offence. Whether or not the query involves fiscal matters, FINTRAC will consider disclosing information as long as the query also involves money laundering and/or terrorist financing activity matters.

1594. For OSFI, once an MOU is in place with another regulator, information is shared as permitted under the MOU subject to the conditions contained therein.

Existence of secrecy or confidentiality requirements

Supervisors co-operation

1595. The supervisory authorities in Canada including FINTRAC, OSFI, the provincial supervisors and SROs all have very clear and broad power to access information from their supervised entities, which may then be passed on to overseas counterparts through the appropriate channels provided that the statutory or administrative preconditions are met (*e.g.* the execution of an information sharing agreement or arrangement). In the case of supervisory authorities that do not have the appropriate power to share directly, such information exchange would be likely to occur through FINTRAC. The assessors did not consider that secrecy or confidentiality laws would have affected the ability of the relevant supervisors to co-operate with their counterparts, through the abovementioned avenues.

Controls and safeguards

Law Enforcement authorities

1596. The RCMP supports the concept of integrated policing through the exchange of criminal intelligence and information with external partners. The RCMP also recognizes this exchange and sharing process is governed by federal legislation, Ministerial Treasury Board Directives, Ministerial directives, and RCMP policies, and various specific caveats and conditions. There are fundamental protocols and Best Practices the RCMP uses to ensure that criminal intelligence and information that is shared with foreign partners and agencies is used only in an authorised manner. The RCMP have policies that help guide it to appropriate decisions for handling requests and sharing or exchanging criminal intelligence and information with foreign partners and agencies. The large majority of RCMP information is subject to security classification. The security level of the information in question will govern many aspects of information sharing or exchange process with external partners.

1597. RCMP documents containing police information or criminal intelligence also include standard caveats that provide further direction on how, and with whom, the document can be shared. These caveats generally outline conditions that are binding on the recipient, regarding the use and disclosure of the information contained in the document.

FINTRAC as an FIU

1598. Consistent with Canada's privacy legislation, FINTRAC undertakes strict safeguards to protect the confidentiality of the information collected through the PCMLTFA. This principle of protecting information is also applied to information received from other competent authorities. A confidentiality clause in FINTRAC's MOU template stipulates that all information exchanged will be subject to strict controls and safeguards to ensure that the information is used only in an authorised manner and treated in a confidential manner and will be protected by FINTRAC and the foreign authority by the same confidentiality as provided by the legislation of the country of the receiving Authority for similar information received from domestic sources.

Supervisory authorities

1599. FINTRAC as AML/CFT supervisor is subject to the safeguards indicated above. In OSFI's case, the criterion is that the recipient agency is a supervisory agency and that the agency will keep the information confidential. In the case of the OSC the powers appear to be broader.

Additional elements

1600. The RCMP may, with the Minister of PSEPC's prior approval, enter into a written or oral arrangement, or otherwise cooperate, with foreign security and intelligence organizations. As such, there are working arrangements and understandings between the RCMP and those intelligence agencies in respect to the sharing of information. Information received from any of these agencies will be treated to the standard care maintained by the agency which generated the document and any other conditions they wish to impose.

1601. Other arrangements with foreign agencies are established and maintained as long as they remain compatible with Canada's foreign policy towards the country or international organization in question.

1602. OSFI does not have authority to deal with non-counterparts in respect of confidential information on supervised financial institutions. However, OSFI can and does assist both domestic and foreign regulators where non-confidential information is involved. For examples, OSFI has an active program of tracking alleged unauthorised banking and insurance activity in Canada and elsewhere. Information received as part of this activity is freely and regularly exchanged with law enforcement,

other regulators, prosecutors (domestic and foreign), supervised financial institutions, and others. Where appropriate OSFI also posts this information to its web site.

Statistics

1603. *FIU*. FINTRAC keeps adequate statistics concerning the number of formal request for assistance made to or received by the FIU from foreign counterparts, including the number of spontaneous referrals. No statistics are kept on the number of requests granted or refused and the time requested to respond.

1604. *Supervisory authorities*. OSFI keeps statistics on the number of formal requests for assistance made or received.

Data on other forms of international co-operation

1605. The following tables provide summary information about FINTRAC exchange of information with foreign FIUs (up to date as of October 17, 2006). The number of disclosures made by FINTRAC to foreign FIUs continues to increase.

	2002-2003	2003-2004	2004-2005	2005-2006	2006-2007[1]	**Totals**
Spontaneous Disclosures	2	3	0	4	9	**18**
Disclosures in response to a Query	8	19	22	27	13	**89**

[1] Fiscal year 06-07 statistics include data up to October 17, 2006.

1606. At the time of the on-site visit, FINTRAC had received 264 requests from foreign FIUs and sent 46 requests to its counterparts (in Australia, Barbados, Bahamas, Belgium, Denmark, Japan, UK and USA).

1607. The number of queries from FINTRAC (46 since 2000-2001) to foreign FIUs is relatively low, taking into account that the majority of these queries were sent to one neighbouring country. FINTRAC has signed up to now 44 MOUs with foreign FIUs. Nevertheless, a wide range of these MOUs has been signed in 2005 (9) and 2006 (16). This could partly explain the low number of requests until now.

1608. The following tables provide an overview of requests received and made by OSFI to foreign counterparts.

Regulator's Country receiving request	**Reason**
Jamaica	Review of Canadian bank's subsidiary operations conducted by OSFI
Mexico	Review of Canadian bank's subsidiary operations conducted by OSFI
Cayman Islands	Review of Canadian banks' subsidiary operations conducted by OSFI
Jersey	Review of Canadian bank's subsidiary operations conducted by OSFI
Guernsey	Review of Canadian bank's subsidiary operations conducted by OSFI
Regulator's Country making request	
UK	Status of Canadian Banks' AML/CFT programs
Germany	Provide Results of OSFI's AML Review of German Bank's Canadian operations
USA	Provide Results of OSFI's AML Review of US Bank's Canadian operations

1609. No information exchanges (in either direction) have been refused. No statistics are kept by OSFI on the time requested to respond to a request initiated by its counterparts.

6.5.2 Recommendations and Comments

1610. *FINTRAC as a supervisory authority*. FINTRAC, if it is to act as a conduit for overseas supervisors to obtain information relating to AML/CFT compliance within the Canadian system, should rapidly enter into agreements with key supervisory counterparts in order to allow proper information sharing. This is necessary in order for FINTRAC to be in a position to render assistance to supervisory counterparts. This requirement is even more critical as a number of Canadian regulatory bodies (not including OSFI, the OSC, the IDA and the AMF) have not been given the explicit power to share AML/CFT information with overseas regulatory counterparts.

1611. Canadian Authorities may wish to consider removing the requirement in the PCMLTFA for formal arrangements or agreements between FINTRAC and foreign supervisory counterparts in order to provide international assistance on a more prompt and effective basis.

1612. Canadian Authorities should ensure that the MOUs established between FINTRAC and Canadian regulatory authorities make appropriate reference to the use of the information received in international requests. If there are requirements for the governing laws of the regulators to be changed to allow for international exchange of information, then this should be implemented.

6.5.3 Compliance with Recommendation 40 and Special Recommendation V

Rec.	Rating	Summary of factors underlying ratings
Rec.40	LC	*FINTRAC as a supervisory authority* • FINTRAC has the legal capacity to exchange information with foreign counterparts but has not yet put the arrangements and agreements in place.
SR.V	LC	**Regarding compliance with Recommendation 40** *FINTRAC as a supervisory authority* • FINTRAC has the legal capacity to exchange information with foreign counterparts but has not yet put the arrangements and agreements in place.

7. RESOURCES AND STATISTICS

7.1 Resources and Statistics (R. 30 & 32)

1613. The text of the description, analysis and recommendations for improvement that relate to Recommendations 30 and 32 is contained in all the relevant sections of the report *i.e.* all of Section 2, parts of sections 3 and 4, and in section 6. There is a single rating for each of these Recommendations, even though the Recommendations are addressed in several sections. Section 7.1 of the report contains only the box showing the rating and the factors underlying the rating.

Rec.	Rating	Summary of factors underlying ratings
Rec.30	PC	*In relation to the FIU*: • The number of staff dedicated to the analysis of ML/TF cases is too low, especially considering the amount of reports coming in. *In relation to law enforcement agencies:* • The RCMP lacks resources to properly undertake ML/TF investigations. *In relation to the Department of Justice* • There seems to be very little if any coordinated or sophisticated training efforts in the forfeiture area. • The authorities in charge of processing MLA requests lack resources. *In relation to prosecution agencies:* • Insufficient training is provided for combating ML and TF. *In relation to supervisors:* • FINTRAC current internal organisation and resources dedicated to supervision are insufficient to allow it to perform its compliance function effectively.
Rec.32	LC	• Incomplete statistics are kept in relation to ML investigations. • Incomplete statistics are kept in relation to ML sentencing. • Statistics on confiscation are incomplete. • There is no data available on the time requested to respond to extradition and MLA requests. • No statistics are kept by OSFI on the time to respond to a request initiated by its counterparts.

7.2 Other relevant AML/CFT measures or issues

N/A

7.3 General framework for AML/CFT system

N/A

TABLES

Table 1. Ratings of Compliance with FATF Recommendations

The rating of compliance vis-à-vis the FATF Recommendations should be made according to the four levels of compliance mentioned in the 2004 Methodology (Compliant (C), Largely Compliant (LC), Partially Compliant (PC), Non-Compliant (NC), or could, in exceptional cases, be marked as not applicable (NA).

Forty Recommendations	Rating	Summary of factors underlying rating
Legal systems		
1. ML offence	LC	▪ The ML offence does not cover all designated categories of predicate offences (copyright related offences). ▪ Section 462.31 ML offence contains a purposive element that is not broad enough to meet the requirements of the Conventions or R.1. ▪ The number of convictions for Section 462.31 ML is very low, as is the percentage of convictions in comparison to charges laid.
2. ML offence – mental element and corporate liability	LC	▪ The number of convictions for Section 462.31 ML is very low. ▪ Due to the lack of data on ML sentencing, is not possible to assess whether natural and legal persons are subject to effective, proportionate and dissuasive sanctions for ML.
3. Confiscation and provisional measures	LC	▪ The fine in lieu forfeiture provision does not fully and effectively meets the requirement for equivalent value provisions and does not apply to property held by third parties. ▪ Based on the limited quantitative and qualitative information available, it does not seem that the confiscation and seizure regime is fully effective, particularly with respect to value based confiscation.
Preventive measures		
4. Secrecy laws consistent with the Recommendations	C	▪ The Recommendation is fully met.
5. Customer due diligence	NC	*Scope issue* ▪ the requirement to conduct CDD does not extend to all financial institutions as defined by the FATF (notably financial leasing, factoring and finance companies). *Numbered accounts* ▪ Although numbered accounts are permissible and used, there is no direct requirement to maintain them in such a way that full compliance can be achieved with the FATF Recommendations. *When CDD is required* ▪ There is no requirement to carry out CDD measures when there is a suspicion of ML or TF and when financial institutions have doubts about the veracity or adequacy of previously obtained CDD data. ▪ Customer identification for occasional transactions that are cross-border wire transfers takes place for transactions above CAD 3 000. This threshold is currently too high and no equivalent requirement is in place for domestic wire transfers. *Required CDD measures* ▪ The current customer identification measures for natural persons are insufficient, especially in relation to non face-

Forty Recommendations	Rating	Summary of factors underlying rating
		to-face business relationships. *Identification of persons acting on behalf of the customer* ▪ The requirement to identify up to three persons who are allowed to give instructions in respect of an account is too limitative. *Third party determination and identification of beneficial owners* ▪ Except for IDA supervised entities, financial institutions are neither required to understand the ownership and control structure of the customer nor obliged to determine who are the natural persons that ultimately own or control the customer. *Purpose & intended nature of the business relationship* ▪ There are currently no requirements (except for securities dealers) to obtain information on the purpose and intended nature of the business relationship. *Ongoing Due Diligence* ▪ Except for securities dealers, there are currently no requirements to conduct ongoing due diligence on the business relationship although the need to identify customers for large cash transactions and electronic fund transfers provide certain automatic trigger points. ▪ Except for securities dealers financial institutions are not required to ensure that documents, data and information collected under the CDD process is kept up-to-date and relevant. *ML/FT risks – enhanced due diligence* ▪ There is no requirement to perform enhanced due diligence for higher risk categories of customer, business relationship or transaction. *ML/FT risks – reduced or simplified due diligence* ▪ The current exemptions mean that, rather than reduced or simplified CDD measures, no CDD apply, which is not in line with the FATF standards. ▪ Exemptions from CDD and third party determination bring in very far reaching exceptions that introduce potential gaps in the customer identification process (especially the exemptions apply to financial entities that operate in FATF countries based on presumption of conformity only). ▪ There is no explicit provisions that set out that CDD or third party determination exemptions are not acceptable where there is a suspicion of ML or FT or specific higher risk scenarios apply. ▪ Financial institutions, in certain circumstances, are given the permission to exempt from CDD requirements or third party determination obligations certain customers resident in another country. However, Canada has not carried out a systematic country risk analysis to ensure that third countries in which customers of Canadian financial institutions are resident are in compliance with and have effectively implemented the FATF Recommendations. *Timing of verification* ▪ PCMLTF Regulations sets out unreasonable verification timelines to be carried out by certain financial sectors and/or in relation to certain customers. *Failure to satisfactorily complete CDD* ▪ Financial institutions (except securities dealers in some circumstances) are not prevented from opening an account or commencing business relationship or

Forty Recommendations	Rating	Summary of factors underlying rating
		performing a transaction and they are not required to make a suspicious transaction report. ▪ In situations where the financial institution has already commenced a business relationship but is unable to perform adequate CDD and establish beneficial ownership, there is no requirement to terminate the business relationship and to consider making a suspicious transaction report.
6. Politically exposed persons	NC	▪ There were no mandatory legislative or other enforceable requirements in relation to PEPs at the time of the on-site visit.
7. Correspondent banking	PC	▪ Financial entities are not required to assess the respondent institution's AML/CFT controls and to ascertain that these controls are adequate and effective. ▪ Financial institutions are not required to determine the reputation of the foreign financial entity (other than take reasonable measures to ascertain whether there are any civil or criminal penalties that have been imposed on the foreign financial institution in respect of AML/CFT requirements) and the quality of supervision of that entity. ▪ In the context of payable through accounts, the respondent entity is not required to perform all the normal CDD obligations set out in Recommendation 5 on its customers that have direct access to the accounts of the correspondent institution in line with the FATF standards. ▪ The effectiveness of the measures in place cannot yet be assessed.
8. New technologies & non face-to-face business	NC	▪ There are no specific legislative or other enforceable obligations addressing the risks posed by the application of new technological developments. ▪ Financial institutions are not required to have policies and procedures in place to address any specific risk associated with non face-to-face business relationships or transactions. ▪ No effective CDD procedures for non face-to-face customers are in place.
9. Third parties and introducers	NC	▪ In the only two scenarios where reliance on a third party or introduced business is legally allowed without an agreement or arrangement, the measures in place are insufficient to meet the FATF requirements. ▪ In addition to the two reliance on third parties/introduced business scenarios contemplated by the Regulations, the financial sector uses introduced business mechanisms as a business practice. However, no specific requirements as set out in Recommendation 9 apply to these scenarios.
10. Record keeping	LC	*Scope issue* ▪ The record keeping requirement does not extend to all financial institutions as defined by the FATF (notably financial leasing, factoring and finance companies). ▪ Financial institutions must ensure that all records required to be kept under the PCMLTFA can be provided within 30 days which does not meet the requirement to make CDD records available on a *timely* basis to competent authorities, especially in normal business circumstances.
11. Unusual transactions	PC	▪ There is no explicit nor enforceable requirement for financial institutions to examine all complex, unusual large transactions under the current legislation (except for IDA members). Except for IDA members, the monitoring obligation is implied and indirect (it flows from reporting suspicious transactions, large international electronic funds transfer and large cash transactions) and it does not cover the full range of monitoring situations as stipulated in Recommendation 11.

Forty Recommendations	Rating	Summary of factors underlying rating
		▪ There is no explicit requirement to examine the background and purpose of these unusual transactions (except for IDA members). ▪ There is no requirement to keep record of financial institutions' findings in relation to complex, unusual large or unusual patterns of transactions.
12. DNFBP – R.5, 6, 8-11	NC	*Scope issue* ▪ Lawyers, Quebec Notaries, BC Notaries, dealers in precious metals and stones, Internet casinos, ship based casinos and TCSPs are not captured by the PCMLTFA and therefore are not subject to the requirements under Recommendations 5, 6 and 8-11. *Application of Recommendation 5 to casinos* ▪ The requirements applicable to casinos are insufficient in relation to: (1) when CDD is required; (2) required CDD measures; (3) identification of persons acting on behalf of the customer; (4) third party determination and identification of beneficial owners ; (5) purpose & intended nature of the business relationship ; (6) ongoing Due Diligence; (7) ML/FT risks and (8) failure to satisfactorily complete CDD. *Application of Recommendation 5 to real estate brokers and sales representatives and accountants* ▪ The circumstances in which real estate agents and sales representatives and accountants have to carry out customer identification are too limitative. ▪ The CDD requirements that real estate agents and sales representatives and accountants are subject to are substantially very basic and extremely limited. *Application of Recommendation 6 to casinos, real estate brokers and sales representatives and accountants* ▪ Canada has not implemented any specific AML/CFT measures concerning PEPs that are applicable to DNFBPs. *Application of Recommendation 8 to casinos, real estate brokers and sales representatives, accountants* ▪ There are no specific legislative or other enforceable obligations for DNFBPs to take measures to prevent the misuse of technological developments in ML/TF schemes. ▪ The DNFBPs are not required to have policies and procedures in place to address any specific risk associated with non face-to-face business relationships or transactions. *Application of Recommendation 9 to casinos, real estate brokers and sales representatives and accountants* ▪ There are currently no provisions for DNFBPs that address the issue of relying on intermediaries or third parties to perform elements of the CDD process outside the outsourcing type of scenario. *Application of Recommendation 10 to casinos, real estate brokers and sales representatives and accountants* ▪ The circumstances in which real estate agents and sales representatives and accountants have to keep records are too limitative. ▪ Real estate agents and sales representatives, casinos and accountants institutions must ensure that all records required to be kept under the PCMLTFA can be provided within 30 days which is not in line with the FATF requirement to make CDD records available on a timely basis to competent authorities.

Forty Recommendations	Rating	Summary of factors underlying rating
		Application of Recommendation 11 to casinos, real estate brokers and sales representatives and accountants ▪ There is currently no explicit provision requiring that DNFBPs pay special attention to all complex, unusual large transactions that have no apparent or visible economic or lawful purpose (the monitoring obligation is implied and indirect (it flows from reporting suspicious transactions, large international electronic funds transfer and large cash transactions) and it does not cover the full range of monitoring situations as stipulated in Recommendation 11). The other requirements under Recommendation 11 are not met either.
13. Suspicious transaction reporting	LC	▪ Some financial institutions as defined by the FATF (especially financial leasing, finance companies, providers of e-money) are not covered by the obligation to report. ▪ There is no requirement to report attempted transactions. ▪ The low numbers of STRs sent by certain financial sectors raise concerns in relation to the effectiveness of the reporting system.
14. Protection & no tipping-off	C	▪ The Recommendation is fully met.
15. Internal controls, compliance & audit	LC	▪ The requirement for internal controls does not extend to all financial institutions as defined by the FATF (notably financial leasing, factoring and finance companies). ▪ There is no mandatory explicit requirement to maintain up to date internal procedures, policies and controls and such policies do not include the detection of unusual and suspicious transactions. ▪ There is no explicit requirement to ensure that the AML/CFT compliance officer has a timely access to customer identification data and other CDD information, transactions records and other relevant information. ▪ There is no mandatory requirement for an independent audit function to test AML/CFT regime compliance for small financial institutions (including some MSBs) for which a simple self-assessment is admitted. ▪ There is no general requirement concerning screening procedures when hiring employees.
16. DNFBP – R.13-15 & 21	NC	*Scope issue* ▪ Lawyers, Quebec Notaries, BC Notaries, dealers in precious metals and stones, Internet casinos, ship based casinos and TCSPs are not captured by the PCMLTFA and therefore are not subject to the suspicious transactions reporting requirements. *Application of Recommendation 13 to casinos, real estate brokers and sales representatives and accountants/accountant firms* ▪ The circumstances in which real estate agents and sales representatives and accountants have to report suspicious transactions under the PCMLTFA are too limited. ▪ Attempted transactions are not yet covered by the Suspicious Transaction Reporting requirement. ▪ The relatively low numbers of STRs sent by real estate agents/sales representatives and accountants raise significant concerns in relation to the effectiveness of the reporting system in these sectors. *Application of Recommendation 15 to casinos, real estate brokers and sales representatives and accountants/accountant firms* ▪ There is no explicit requirement to: (1) keep up to date internal procedures, (2) have policies to monitor for and detect unusual and suspicious transactions and (3) ensure that the AML/CFT compliance officer has timely access to

Forty Recommendations	Rating	Summary of factors underlying rating
		customer identification data and other CDD information, transactions records and other relevant information. ▪ There is no mandatory requirement for an independent audit function to test AML/CFT regime compliance. ▪ Except for casinos, there are no requirements concerning screening procedures when hiring employees. *Application of Recommendation 21 to casinos, real estate brokers and sales representatives and accountants/accountant firms* ▪ There is no general enforceable requirement for DNFBPs to give special attention to transactions or business relationships connected with persons from or in countries which do not or insufficiently apply the FATF Recommendations but only through general guidance or advisories sent on a case by case basis. ▪ There are no effective measures in place whereby DNFBPs are advised of other countries that have specific weaknesses in their AML/CFT systems. ▪ There is no requirement to examine the background and purpose of these transactions and to document the related findings.
17. Sanctions	PC	▪ With the exceptions of OSFI and IDA regulated institutions, only criminal sanctions are available to FINTRAC under the PCMLTFA for all other types of financial institutions and these are only applicable for the most serious failures, and need to be proved to the criminal standard. ▪ OSFI only uses a limited range of actions/sanctions in the AML/CFT context (namely supervisory letters and in a limited number of cases, staging). ▪ The lack of effective sanctions applied in cases of major deficiencies raises real concern in terms of effectiveness of the sanction regime, particularly taking into account that only one criminal sanction and a very limited number of administrative sanctions have been applied.
18. Shell banks	LC	▪ Financial entities are not required to terminate business relationships with shell banks, nor with any foreign financial institution that has, directly or indirectly, correspondent banking relationships with shell banks. ▪ The effectiveness of the measures in place cannot yet be assessed.
19. Other forms of reporting	C	▪ The Recommendation is fully met.
20. Other NFBP & secure transaction techniques	C	▪ The Recommendation is fully met.
21. Special attention for higher risk countries	PC	▪ There is no general enforceable requirement for financial institutions to give special attention to transactions or business relationships connected with persons from or in countries which do not or insufficiently apply the FATF Recommendations. ▪ There are no effective measures in place whereby financial institutions are advised of other countries that have specific weaknesses in their AML/CFT systems. ▪ There is no requirement to examine the background and purpose of these transactions and to document the related findings.
22. Foreign branches & subsidiaries	NC	▪ Currently, the PCMLTFA and PCMLTF Regulations contain no explicit enforceable provision requiring financial institutions to ensure that their foreign branches and subsidiaries observe AML/CFT measures consistent with home country requirements although foreign branches of Canadian financial institutions are Canadian entities under the Bank Act and the Insurance Companies Act that are subject to Canadian laws.

Forty Recommendations	Rating	Summary of factors underlying rating
		▪ There is no requirement that particular attention be paid to branches and subsidiaries in countries which do not or insufficiently apply the FATF Recommendations. ▪ There is no legal obligation in the PCMLTFA and PCMLTF Regulations that, where the minimum AML/CFT requirements of the home and host countries differ, branches and subsidiaries in host countries are required to apply the higher standard, to the extent that local (*i.e.* host country) laws and regulations permit. ▪ There is no requirement that financial institutions be required to inform their home country supervisor when a foreign branch or subsidiary is unable to observe appropriate AML/CFT measures because this is prohibited by local (*i.e.* host country) laws, regulations or other measures.
23. Regulation, supervision and monitoring	PC	▪ Exclusion from the AML/CFT regime of certain financial sectors (such as financial leasing, factoring, finance companies, etc.) without proper risk assessments. ▪ For the financial institutions subject to the PCMLTFA, there is a very unequal level of supervision of AML/CFT compliance, with certain categories of financial institution appearing to be insufficiently controlled (MSBs, certain credit unions/*caisses populaires*, life insurance intermediaries…). This is due to the limited staff resources of FINTRAC dedicated to on-site assessments compared to the high number of reporting entities, which has not always been compensated by the involvement of the primary prudential regulators in AML/CFT issues. ▪ "Fit and proper" requirements are not comprehensive. ▪ At the time of the on-site visit, there was no specific obligation for FRFIs to implement screening procedures for persons who are hired, or appointed to the Board, after the initial incorporation or authorisation procedures are concluded. ▪ There is currently no registration regime for MSBs.
24. DNFBP - regulation, supervision and monitoring	NC	*Scope issue* ▪ Lawyers, Quebec Notaries, BC Notaries, dealers in precious metals and stones, Internet casinos, ship based casinos and TCSPs are not captured by the PCMLTFA and not subject to FINTRAC supervision. *Supervision of casinos* ▪ The sanction regime available to FINTRAC is currently inadequate (see conclusions in relation to Rec. 17). Provincial regulators may have administrative sanctions at their disposal but there is no evidence that these are dissuasive, effective and proportionate, since no data or statistics regarding sanctions taken by these regulators on the grounds of AML/CFT non-compliance issues have been made available to the assessment team. *Supervision of other DNFBPs* ▪ Limited staff resources deprives FINTRAC from closely and efficiently monitoring DNFBPs' compliance with the PCMLTFA requirements especially in sectors/provinces where the primary regulators or SROs are not or insufficiently involved in AML/CFT compliance supervision. ▪ The sanction regime available to FINTRAC is currently inadequate (see conclusions in relation to Rec. 17). Provincial regulators may have administrative sanctions at their disposal but there is no evidence that these are dissuasive, effective and proportionate, since no data or statistics regarding sanctions taken by these regulators on the ground of AML/CFT non-compliance issues have been

Forty Recommendations	Rating	Summary of factors underlying rating
		made available to the assessment team.
25. Guidelines & Feedback	LC	▪ There is a lack of specific guidelines intended for sectors such as life insurance companies and intermediaries. ▪ There is not enough general feedback given outside the large financial institutions sector.
Institutional and other measures		
26. The FIU	PC	▪ FINTRAC has insufficient access to intelligence information from administrative and other authorities (especially from CRA , CSIS and Customs). ▪ FINTRAC is not allowed by the PCMLTFA to gather additional financial information from reporting entities. ▪ Effectiveness: (1) the number of staff dedicated to the analysis of potential ML/FT cases is low especially in comparison with the amount of reports coming in, which may have an impact on the number of cases that FINTRAC generate; (2) feedback from law enforcement authorities outlines the relatively limited added value of FINTRAC disclosures in law enforcement investigations; (3) the timeliness of FINTRAC disclosures to law enforcement authorities was raised as an issue at the time of the on-site visit; (4) 80% of the disclosures made by FINTRAC result from voluntary information from law enforcement; only 20% result from STRs which raises serious concerns with respect to the capability of FINTRAC to generate ML/TF cases on the basis of STRs or other reports it receives from the private sector; (5) so far, very few if any convictions for ML or TF have resulted from a FINTRAC disclosure which is an additional factor to consider when looking at FINTRAC's ability to produce intelligence to be used in criminal investigations and prosecutions.
27. Law enforcement authorities	LC	▪ The RCMP lacks the resources that would allow it to focus on a larger spectrum of ML/TF investigations.
28. Powers of competent authorities	C	▪ The Recommendation is fully met.
29. Supervisors	LC	▪ FINTRAC has no power to impose administrative sanctions.
30. Resources, integrity and training	PC	*In relation to the FIU*: ▪ The number of staff dedicated to the analysis of ML/TF cases is too low, especially considering the amount of reports coming in. *In relation to law enforcement agencies:* ▪ The RCMP lacks resources to properly undertake ML/TF investigations. *In relation to the Department of Justice* ▪ There seems to be very little if any coordinated or sophisticated training efforts in the forfeiture area. ▪ The authorities in charge of processing MLA requests lack resources. *In relation to prosecution agencies:* ▪ Insufficient training is provided for combating ML and TF. *In relation to supervisors:3* ▪ FINTRAC current internal organisation and resources dedicated to supervision are insufficient to allow it to perform its compliance function effectively.
31. National co-operation	LC	▪ Interagency cooperation between the FIU and law enforcement authorities is not fully effective and needs to be enhanced.
32. Statistics	LC	▪ Incomplete statistics are kept in relation to ML investigations. ▪ Incomplete statistics are kept in relation to ML sentencing.

Forty Recommendations	Rating	Summary of factors underlying rating
		▪ Statistics on confiscation are incomplete. ▪ There is no data available on the time requested to respond to extradition and MLA requests. ▪ No statistics are kept by OSFI on the time to respond to a request initiated by its counterparts.
33. Legal persons – beneficial owners	NC	▪ There is no requirement to ensure adequate transparency, for instance there is no obligation that information on the beneficial ownership of shares in legal persons is required to be collected by either the corporate registry, within corporate records held by legal persons or by lawyers, accountants or TCSPs. ▪ While law enforcement and other authorities have sufficient powers, those powers are not adequate to ensure the existence of adequate, accurate and timely information on the beneficial ownership of legal persons, which can be accessed or obtained in a timely fashion by competent authorities. ▪ There are no measures to ensure that bearer shares are not misused for ML, particularly for private corporations.
34. Legal arrangements – beneficial owners	PC	▪ There are limited and indirect legal requirements to obtain, verify, or retain information on the beneficial ownership and control of trusts and fiducie in Québec. ▪ While the investigative powers are generally sound and widely used, there is minimal information that is adequate, accurate and timely concerning the beneficial owners of trusts and fiducie in Québec that can be obtained or accessed by the competent authorities in a timely fashion. Where some information is held, such as by CRA, there are limits on the circumstances in which information on trusts can be shared.
International Co-operation		
35. Conventions	LC	*Implementation of the Palermo and Vienna Conventions:* ▪ Canada has ratified the Palermo and Vienna Conventions and implemented them with some omissions however (the ML offence does not cover all required categories of predicate offences and Section 462.31 ML offence contains a purposive element that is not broad enough to meet the requirements of the Conventions). *Implementation of the CFT Convention:* ▪ Article 18(1)(b) of the Convention, which requires countries to implement efficient measures to identify customers in whose interest accounts are opened is insufficiently implemented. Canada's implementation of Recommendation 5 does not include adequate measures to ascertain the identity of beneficial owners.
36. Mutual legal assistance (MLA)	LC	▪ There are concerns about the ability of Canada to handle MLA requests in a timely and effective manner and effectiveness of the current regime cannot be demonstrated due to the lack of adequate data.
37. Dual criminality	C	▪ The Recommendation is fully met.
38. MLA on confiscation and freezing	LC	▪ There are doubts about the effectiveness of the measures in place under Recommendation 38: there is limited evidence of effective confiscation assistance as only four cases have been successful in last 5 years and international sharing statistics indicate that while asset sharing with foreign states is possible, it rarely occurs. Canada executes requests to enforce corresponding value judgments as fines, which has limitations and cannot be enforced against property held by third parties.
39. Extradition	LC	▪ Insufficient statistical data was provided to make a thorough assessment, particularly the assessment of the delay element, but even the limited data provided indicates that obtaining extradition from Canada quickly may be

Forty Recommendations	Rating	Summary of factors underlying rating
		difficult.
40. Other forms of co-operation	LC	*FINTRAC as a supervisory authority* ▪ FINTRAC has the legal capacity to exchange information with foreign counterparts but has not yet put the arrangements and agreements in place.
Nine Special Recommendations	**Rating**	**Summary of factors underlying rating**
SR.I Implement UN instruments	LC	*Implementation of the CFT Convention:* ▪ Article 18(1)(b) of the Convention, which requires countries to implement efficient measures to identify customers in whose interest accounts are opened is insufficiently implemented. Canada's implementation of Recommendation 5 does not include adequate measures to ascertain the identity of beneficial owners.
SR.II Criminalise terrorist financing	LC	▪ The lack of any TF convictions and the very limited number of prosecutions shows that the offence has not yet been fully and effectively used.
SR.III Freeze and confiscate terrorist assets	LC	▪ The actions taken to communicate the names of listed persons or entities do not cover all types of financial institutions and the lists are not effectively communicated to other types of asset holders. ▪ With the exception of guidance given to federally regulated financial institutions (and copied to provincial regulators/SROs), Canada has issued insufficient guidance to other financial institutions and DNFBPs that may be holding funds of other assets concerning their obligations in taking action under freezing mechanisms. This may have an impact on Canada's ability to freeze terrorist funds or other assets for such entities without delay. ▪ The existing measures to effectively monitor the compliance with the legislation governing the obligations under SRIII are insufficient (except for federally regulated financial institutions supervised by OSFI).
SR.IV Suspicious transaction reporting	LC	▪ Some financial institutions as defined by the FATF (especially financial leasing, finance companies, providers of e-money) are not covered by the obligation to report. ▪ There is no requirement to report attempted transactions.
SR.V International co-operation	LC	**Regarding compliance with Recommendation 38** ▪ All elements missing in R. 38 are missing for SR.V. ▪ There are concerns about the ability of Canada to handle MLA requests in a timely and effective manner and effectiveness of the current regime cannot be demonstrated due to the lack of adequate data. **Regarding compliance with Recommendation 39** ▪ No meaningful statistical data provided to assess delay element (effectiveness issue). **Regarding compliance with Recommendation 40** *FINTRAC as a supervisory authority* ▪ FINTRAC has the legal capacity to exchange information with foreign counterparts but has not yet put the arrangements and agreements in place.
SR VI AML requirements for money/value transfer services	NC	▪ There is no registration regime for MSBs as contemplated by SR VI. ▪ Overall, requirements and implementation of Recommendations 4-11, 21-23 and SR. VII is inadequate which has a significant negative impact on the effectiveness of AML/CFT measures for money transmission services. ▪ MSBs are not required to maintain a list of their agents.

Forty Recommendations	Rating	Summary of factors underlying rating
		▪ The sanction regime available to FINTRAC and applicable to MSBs is not effective, proportionate and dissuasive.
SR VII Wire transfer rules	NC	▪ Canada has not implemented SRVII.
SR.VIII Non-profit organisations	LC	▪ The existing co-ordination mechanisms between competent authorities, especially between the CRA and the parties responsible for listing and freezing applications is insufficient to fully address the risk in some segments of the NPO sector.
SR.IX Cross Border Declaration & Disclosure	C	▪ The Recommendation is fully met.

Table 2: Recommended Action Plan to Improve the AML/CFT System

AML/CFT System	Recommended Action (listed in order of priority)
1. General	
2. Legal System and Related Institutional Measures	
Criminalisation of Money Laundering (R.1 &, 2)	▪ Canada should cover all designated categories of predicate offences. ▪ Canada should amend Section 462.31 ML offence (in relation to the intent mental element) in order to fully met the requirements of the Conventions or Recommendation 1. ▪ Canada should ensure that the statutes available for countering ML are effectively used. ▪ Canada should develop a more proactive approach to prosecuting the specific money laundering charge under s.462.31.
Criminalisation of Terrorist Financing (SR.II)	▪ Canada should pay attention to the overall effectiveness of the TF offence and regime and ensure that the TF offence is effectively used.
Confiscation, freezing and seizing of proceeds of crime (R.3)	▪ Canada should review the fine in lieu forfeiture provision to be in line with the FATF requirements. ▪ Canada should ensure that the confiscation and seizure regime is fully effective, particularly with respect to value based confiscation.
Freezing of funds used for terrorist financing (SR.III)	▪ There needs to be more communication on listed persons provided to certain categories of financial institutions and other potential asset holders as well more clear and practical guidance to reporting entities (including DNFBPs and MSBs) that may be holding targeted funds or other assets concerning their obligations in taking action under freezing mechanisms. ▪ Canada should enhance the existing measures to monitor the compliance with the legislation governing the obligations under SRIII (except for federally regulated financial institutions supervised by OSFI).
The Financial Intelligence Unit and its functions (R.26 & 30)	▪ FINTRAC should be able to obtain additional financial information from the reporting entities, especially during the analytical process. ▪ FINTRAC should be authorised to have access to more intelligence data from CSIS, CRA and the Canadian Customs Agency to reinforce its analytical work. ▪ Canada should examine FINTRAC effectiveness in disclosing ML/TF cases to law enforcement authorities. ▪ Canada should ensure that FINTRAC has sufficient analysts that are in charge of developing ML/TF cases and processing disclosures to law enforcement authorities for further investigations.
Law enforcement, prosecution and other competent authorities (R.27 & 28)	▪ Canada should ensure that the RCMP gets sufficient resources that would allow it to focus on a larger spectrum of ML/TF investigations.
Cross Border declaration or disclosure (SR.IX)	▪ There are no recommendations for this section.
3. Preventive Measures – Financial Institutions	
Risk of money laundering or terrorist financing	▪ Canada should rely on a more comprehensive, thorough and formal risk assessment process. The underlying principle should be that the financial activities referred to in the FATF standards should be covered unless there is a proven low risk of ML/TF.
Customer due diligence, including enhanced or reduced measures (R.5 to 8)	*In relation to Recommendation 5:* ▪ With regard to numbered or confidential accounts, Canada should consider adopting detailed rules or guidance on the use of such accounts by financial institutions. Such rules should clearly set out the obligation for compliance officers to have access to CDD information.

AML/CFT System	Recommended Action (listed in order of priority)
	▪ New provisions will come into force in 2008 with regard to the circumstances where financial institutions have to perform customer identification. Canada should ensure that the new provisions are fully in line with the FATF requirements. ▪ With regard to the identification measures for natural persons, Canada should ensure that only reliable CDD documentation is acceptable, especially in non face-to-face situations. Canada should consider introducing additional requirements for identifying foreign customers. ▪ New provisions will come into force in June 2008 with regard to identification of beneficial owners. Canada should ensure that the new provisions are fully in line with the FATF requirements and are properly implemented by all financial institutions. ▪ The requirement to identify up to three persons who are authorised to give instructions in respect of an account should be extended to any person purporting to act on behalf of the customer. ▪ The PCMLTF Regulations, enacted in June 2007 and coming into force in June 2008 require financial entities to keep a record of the intended use of the account. Canada should ensure that such requirement is implemented by all financial institutions in line with the FATF standards. ▪ Based on the provisions adopted in June 2007 and coming into force in 2008, Canada should ensure that financial institutions fully implement the obligation to conduct ongoing due diligence on the business relationship and ensure all documents, data and information collected under the CDD process in line with the FATF standards (as it is already the case for securities dealers) are kept up-to-date and relevant. ▪ In relation to ML/FT risks, Canada should ensure that financial institutions perform enhanced due diligence for higher risk categories of customer, business relationship or transaction once the new regulations enter into force in June 2008. This should be done in line with the FATF standards. Current scenarios of full exemptions from CDD and third party determination should be subject to simplified or reduced CDD. Where financial institutions are permitted to apply simplified or reduced CDD measures to customers resident in another country, this should be limited to countries that Canada is satisfied are in compliance with and have effectively implemented the FATF recommendations (*i.e.* Canada should not rely on presumption of conformity of FATF countries for instance). Canada should adopt explicit provisions that set out that such exemptions are not acceptable where there is a suspicion of ML or FT or specific higher risk scenarios apply. Canada should consider developing guidelines for financial institutions that are permitted to determine the extent of the CDD measures on a risk sensitive basis. ▪ With regard to the timing of customer's identity verification, new regulations that will enter into force in June 2008 should be implemented in line with the FATF standards and Canada should consider adopting shorten timelines in the insurance, foreign exchange, MSBs and securities sectors for corporations' or entities' identification, especially in normal business circumstances. *In relation to Recommendation 6*: ▪ Canada should ensure that the new provisions enacted in June 2007 are fully in line with the FATF requirements and ensure that reporting entities implement measures that meet the FATF standards. *In relation to Recommendation 7:* ▪ Canada should require financial entities to assess the respondent institution's AML/CFT controls and to ascertain

AML/CFT System	Recommended Action (listed in order of priority)
	that these controls are adequate and effective. ▪ Institutions should also be required to determine the reputation of the foreign financial entity (other than take reasonable measures to ascertain whether there are any civil or criminal penalties that have been imposed on the foreign financial institution in respect of AML/CFT requirements) and the quality of supervision of that entity. ▪ In the context of payable through accounts, the respondent entity should be required to perform all customer identification in line with the FATF standards. ▪ Canada should ensure that reporting entities implement measures that meet the FATF standards. *In relation to Recommendation 8:* ▪ Canada should ensure that the new provisions enacted in June 2007 are fully in line with the FATF requirements and ensure that reporting entities implement measures that meet the FATF standards.
Third parties and introduced business (R.9)	▪ Since introduced business arrangements exist in Canada in other circumstances than those captured by Sections 56(2) and 57(5) of the PCMLTF Regulations, Canada should adopt provisions that address all aspects of Recommendation 9 and ensure that financial institutions implement them.
Financial institution secrecy or confidentiality (R.4)	▪ There are no recommendations for this section.
Record keeping and wire transfer rules (R.10 & SR.VII)	*In relation with Recommendation 10:* ▪ Canada should ensure that all types of transactions (including business correspondence) carried out by financial institutions (except for IDA members) are subject to proper record keeping requirements that permit their reconstruction so as to provide, if necessary, evidence for prosecution of criminal activity. ▪ Canada should ensure that all customer and transactions records and information are available on a timely basis to domestic competent authorities. *In relation with SRVII:* ▪ Canada should ensure that the new provisions enacted in December 2006 and coming into force in June 2008 are fully in line with the FATF requirements and ensure that reporting entities implement measures that meet the FATF standards. ▪ Canada should ensure that the wire transfers operated by casinos outside the banking network are subject to equivalent requirements.
Monitoring of transactions and relationships (R.11 & 21)	*In relation with Recommendation 11:* ▪ Canada should ensure that the new provisions enacted in June 2007 are fully in line with the FATF requirements and ensure that reporting entities implement measures that meet the FATF standards. *In relation with Recommendation 21:* ▪ The requirement to give special attention to business relationships or transactions with persons from or in countries which do not or insufficiently apply the FATF Recommendations should be included in an enforceable legal instrument applicable to all financial institutions. ▪ Effective measures should be put in place whereby financial institutions are advised of other countries that have specific weaknesses in their AML/CFT systems. This should be completed by a provision requiring that the background and purpose of such transactions having no apparent economic or visible lawful purpose be examined and the findings documented.

AML/CFT System	Recommended Action (listed in order of priority)
Suspicious transaction reports and other reporting (R.13-14, 19, 25 & SR.IV)	*In relation with Recommendation 13 & SRIV* ▪ All financial institutions covered by the definition of the FATF should be subject to the suspicious transactions reporting requirement unless a proven low risk of ML and FT is established in the sectors that are currently exempted. ▪ Canada should ensure that the different categories of financial institutions contribute more equally to the total number of STRs received by FINTRAC. *In relation with Recommendation 14* ▪ There are no recommendations for this section. *In relation with Recommendation 19* ▪ There are no recommendations for this section. *In relation with Recommendation 25* ▪ FINTRAC should develop more general feedback for smaller reporting entities.
Internal controls, compliance, audit and foreign branches (R.15 & 22)	*In relation to Recommendation 15* ▪ The current requirements should be expanded, made more explicit and enforceable, in particular (1) written policies and procedures should be explicitly required, and should be kept up to date, and their minimum mandatory content should include the detection of unusual and suspicious transactions; (2) there should be an explicit requirement to ensure that the AML/CFT compliance officer has a timely access to customer identification data and other CDD information, transactions records and other relevant information; (3) the requirement for an independent audit function (internal or external) to test on a regular basis the compliance of the AML regime should be strengthened for MSBs and small financial institutions, and made more explicit generally; (4) Canada should impose screening procedures when hiring employees for financial institutions. *In relation to Recommendation 22* ▪ Canada should ensure that the provisions in relation to Recommendation 22 that will enter into force in June 2008 are in line with the FATF requirements and are properly implemented by all financial institutions.
Shell banks (R.18)	▪ Canada should adopt a requirement for financial entities to terminate business relationships with shell banks as well as with any foreign financial institution that has, directly or indirectly, correspondent banking relationships with shell banks. ▪ Canada should ensure that the measures adopted in relation to shell banks are fully implemented by financial institutions.
The supervisory and oversight system - competent authorities and SROs Role, functions, duties and powers (including sanctions) (R.23, 30, 29, 17 & 25)	*In relation to Recommendation 17, 23 & 29* ▪ Canada should ensure a proper and effective implementation of the regime of administrative and monetary penalties and ensure that competent authorities put in place effective, proportionate and dissuasive sanctions. ▪ Canada should implement a more equal level of supervision of AML/CFT compliance vis-à-vis certain categories of financial institution (MSBs, certain credit unions/*caisses populaires*, life insurance intermediaries…). ▪ Canada should ensure that "fit and proper" requirements are in place. ▪ Canada should adopt screening procedures for persons who are hired, or appointed to the Board, after the initial incorporation or authorisation procedures are concluded. ▪ Canada should implement the registration regime for MSBs. *In relation to Recommendation 25* ▪ Canada should provide more specific guidelines for sectors such as life insurance companies and intermediaries.

AML/CFT System	Recommended Action (listed in order of priority)
Money value transfer services (SR.VI)	▪ Canada should ensure effective implementation of the registration system for MSBs in force in June 2008 and ensure that the requirements applicable to MSBs fully meet the FATF requirements.
4. Preventive Measures –Non-Financial Businesses and Professions	
Customer due diligence and record-keeping (R.12)	▪ All DNFBPs as defined by the FATF should be subject to the AML/CFT regime. ▪ The circumstances in which real estate agents and sales representatives and accountants have to carry out customer identification and keep records should be extended to be in line with the types of activities targeted under Recommendation 12. *In relation to Recommendation 5:* ▪ Canada should ensure that the entire set of requirements under Recommendation 5 apply to all non-financial professions. *In relation to Recommendations 6, 8, 9 and 11:* ▪ Canada should require the non-financial professions to implement requirements in relation to Recommendations 6, 8, 9 and 11. *In relation to Recommendation 10:* ▪ Canada should ensure that all types of transactions carried out by the non-financial professions are subject to proper record keeping requirement that permits their reconstruction so as to provide, if necessary, evidence for prosecution of criminal activity. ▪ Canada should ensure that all customer and transactions records and information collected by the non-financial professions are available on a timely basis to domestic competent authorities.
Suspicious transaction reporting (R.16)	*In relation to Recommendation 13:* ▪ All DNFBPs as defined by the FATF should be subject in Canada to the suspicious transactions reporting requirement in all circumstances defined in Recommendation 16. *In relation to Recommendation 15:* ▪ The current requirements should be expanded, specified and enforced, especially: (1) the policies and procedures should be required to be written and their minimum mandatory content should include the detection of unusual and suspicious transactions for all DNFBPs; (2) there should be a requirement to ensure that the AML/CFT compliance officer has a timely access to customer identification data and other CDD information, transactions records and other relevant information; (3) the requirement for an independent audit function (internal or external) to test on a regular basis the compliance of the AML regime should be strengthened; (4) Canada should impose screening procedures when hiring employees to DNFBPs. *In relation to Recommendation 21*: ▪ The requirement to give special attention to business relationships or transactions with persons from or in countries which do not or insufficiently apply the FATF Recommendations should be included in an enforceable legal instrument applicable to DNFBPs. ▪ Effective measures should be put in place whereby DNFBPs are advised of other countries that have specific weaknesses in their AML/CFT systems. ▪ Finally a provision should be introduced requiring that the background and purpose of such transactions having no apparent economic or visible lawful purpose be examined and the findings documented.

AML/CFT System	Recommended Action (listed in order of priority)
Regulation, supervision and monitoring (R.24-25)	▪ All DNFBPs as defined by the FATF should be subject to the AML/CFT regime. ▪ Canada should ensure that supervisory action (especially on-site examinations) vis-à-vis casinos, but more importantly with respect to all other DNFBPs is strongly reinforced. ▪ The role, functions and monitoring powers of other regulators and SROs in ensuring compliance of DNFBPs with the AML/CFT requirements should be clarified. ▪ Canada should consider revisiting the supervision issue as a whole and give further consideration on whether FINTRAC should be the only authority in charge of ensuring compliance with the AML/CFT requirements. ▪ The sanction regimes applicable to DNFBPs, including casinos, should be reinforced and Canada should ensure that the sanctions available for failures to apply AML/CFT requirements are effective, proportionate and dissuasive.
Other designated non-financial businesses and professions (R.20)	▪ There are no recommendations for this section.
5. Legal Persons and Arrangements & Non-Profit Organisations	
Legal Persons – Access to beneficial ownership and control information (R.33)	▪ Canada should adopt further requirements to prevent the unlawful use of legal persons in relation to ML and TF. ▪ Canada should ensure that competent authorities have access to accurate and current information on the ultimate beneficial owners and controllers of all legal persons on a timely basis. ▪ Canada should adopt measures to ensure that bearer shares are not misused for ML, particularly for private corporations.
Legal Arrangements – Access to beneficial ownership and control information (R.34)	▪ Canada should ensure that competent authorities have access to accurate and current information on the ultimate beneficial owners and controllers of all legal arrangements on a timely basis. ▪ Canada should implement measures to ensure that adequate, accurate and timely information is available to law enforcement authorities concerning the beneficial ownership and control of trusts and fiducie in Québec.
Non-profit organisations (SR.VIII)	▪ Canada should improve the existing co-ordination mechanisms between competent authorities, especially between the CRA and the parties responsible for listing and freezing applications.
6. National and International Co-operation	
National co-operation and coordination (R.31)	▪ Canada should enhance interagency cooperation between the FIU and law enforcement authorities.
The Conventions and UN Special Resolutions (R.35 & SR.I)	▪ Canada should ensure that the ML offence does cover all designated categories of predicate offences and Canada should consider removing the purpose element from Section 462.31 of the CC to be in line with the UN Conventions. ▪ Canada should enact stronger measures to customer identification so as to be more compliant with Article 18(1)(b) of the CFT Convention.
Mutual Legal Assistance (R.36-38, SR.V)	▪ Canada should ensure that MLA requests are handled in a timely and effective manner. ▪ Canada should consider ways to improve the mechanisms to respond to foreign confiscation requests.
Extradition (R.39, 37, SR.V)	▪ Canada should ensure that extradition requests are handled in a timely and effective manner.
Other Forms of Co-operation (R.40, SR.V)	▪ FINTRAC should rapidly enter into agreements with key supervisory counterparts in order to allow proper information sharing.
7. Resources and Statistics	
Resources of Competent Authorities (R.30)	*In relation to the FIU*: ▪ FINTRAC should increase the number of staff dedicated to the

AML/CFT System	Recommended Action (listed in order of priority)
	analysis of ML/TF cases. *In relation to law enforcement agencies:* ▪ Canada should increase the resources of the RCMP in relation to ML/TF investigations. *In relation to the Department of Justice* ▪ Canada should put in place more sophisticated training efforts in the forfeiture area. ▪ The authorities in charge of processing MLA requests should be given more resources. *In relation to prosecution agencies:* ▪ More training should be provided for combating ML and TF. *In relation to supervisors:* ▪ Resources of FINTRAC to carry out its supervision duties should increase.
Statistics (R.32)	▪ Canada should collect more statistics in relation to ML investigations. ▪ Canada should collect more statistics in relation to ML sentencing. ▪ Canada should collect more statistics on confiscation. ▪ Canada should collect more data on the time requested to respond to extradition and MLA requests. ▪ OSFI should collect more statistics on the time to respond to a request initiated by its counterparts.

Table 3: Authorities' Response to the Evaluation

Relevant sections and paragraphs	Country Comments
General	Legislative amendments to the PCMLTFA passed in December 2006 and associated regulations enacted in June 2007 and December 2007 will address a substantial number of deficiencies identified in this report. Please see Annex 1 for a detailed list of legislative and regulatory amendments to Canada's AML/CFT regime that came into force after June 2007 and have not been considered in this evaluation. Canada's regulations allow a period of time between enactment and coming into force to provide an opportunity for businesses and sectors to modify systems.
Section 2.5	Recommendation 26 Canada believes that a partially compliant rating does not adequately reflect Canada's legal reality and FINTRAC's sophisticated organisation. First, it should be noted that, in order to safeguard Canadians' rights under the *Canadian Charter of Rights and Freedoms,* FINTRAC has no investigative powers. FINTRAC is not able to request further information directly from reporting entities for analysis purposes as this activity corresponds to investigative powers. There is therefore a clear constitutional impediment to requesting additional information and this should have been properly reflected in the analysis. Second, FINTRAC is effective in receiving, analysing and disclosing information to competent authorities: • FINTRAC has one of the most sophisticated FIU information technology systems in the world. Its unique technology-driven approach to analysis permits effective analysis of large volumes of transactions by its 36 tactical financial analysts. As the report notes in para 371, total staff at FINTRAC is "more than adequate". • The report notes in para 388 that FINTRAC disclosures provide added value to recipients in terms of identifying new leads and contributing to investigations. • The timeliness of disclosures is an issue that has been addressed by FINTRAC, as indicated in feedback received since 2006 and has also been improving, as noted in para 391. • Disclosures related to voluntary information (VIRs) demonstrate FINTRAC's responsiveness to the investigative priorities identified by law enforcement. • Like many FIUs, FINTRAC is not responsible for investigation or prosecution of cases. As such, it is not appropriate that its effectiveness be measured on the basis of convictions for ML/TF.
Section 2.5	Recommendation 30 Canada believes that a partially compliant rating does not adequately reflect the situation of resources in Canadian authorities, in particular those of FINTRAC. FINTRAC has one of the world's most sophisticated FIU IT systems, which supports the analysis of STRs and other transactions. 35 analysts conduct the analysis of financial transactions to develop FINTRAC disclosures. The work of these analysts is supported by FINTRAC's 80 information technology staff through, for example, the electronic filing of all report data, matching software that links incoming reports to current/former cases and other reports in the system based on a variety of data elements (*e.g.* name, account number, address, etc.), and tools that permit efficient database searches and case compilation. FINTRAC designed its compliance program based on a sophisticated risk-based model and has staffed the appropriate number of compliance officers to carry out the supervisory activities required to discharge its mandate of ensuring compliance with the PCMLTFA. As the report notes in para 371, total staff at FINTRAC is "more than adequate".
Sections 3.1-3.2	Recommendation 5 Canada believes that a non compliant rating clearly fails to recognize the broad-based record-keeping and client identification measures that have been in place in Canada since 2002. In addition, OSFI, the IDA and FINTRAC have issued and enforced guidance on implementation. Regulatory amendments enacted in June 2007 introduce enhanced customer due diligence provisions that come fully into force in June 2008. These provisions will further reinforce compliance with this recommendation and address most deficiencies identified.

Relevant sections and paragraphs	Country Comments
Section 3.2	Recommendation 6 Regulatory provisions enacted in June 2007 which come into force in June 2008 address the deficiencies identified.
Section 3.2	Recommendation 8 Rregulatory provisions enacted in June 2007 which come into force in June 2008 address the deficiencies identified.
Section 3.3	Recommendation 9 Canada believes that the report fails to recognize that there are only two specific situations where no written agreements are necessary for Canadian financial institutions to rely on another entity to identify their customers. When reliance is done through written agreements, Canada believes that these relationships fall outside the scope of Recommendation 9. In addition, a clarifying provision in the regulations enacted in June 2007 which come into force in June 2008 will address deficiencies identified.
Section 3.5	Special Recommendation VII Legislative and regulatory provisions enacted in June 2007 which come into force in June 2008 address deficiencies identified.
Section 3.6	Recommendation 11 Regulatory provisions enacted in June 2007 which come into force in June 2008 address the deficiencies identified.
Section 3.6	Recommendation 21 Regulatory provisions enacted in June 2007 which come into force in June 2008 address the deficiencies identified.
Section 3.8	Recommendation 22 Canada believes that the report fails to recognize that the Bank Act currently applies to bank branches outside Canada. As the PCMLTFA applies to banks, it also *de facto* applies to foreign bank branches. Legislative amendments enacted in December 2006 and coming into force in June 2008 will make it explicit that the PCMLTFA applies to foreign branches and subsidiaries.
Section 3.10	Recommendation 23 Canada believes that a partially compliant rating does not adequately reflect the supervisory situation in Canada. OSFI and FINTRAC have been effectively enforcing AML/CFT requirements for years. FINTRAC designed its compliance program based on a sophisticated risk-based model and has staffed the appropriate number of compliance officers to carry out the supervisory activities required to discharge its mandate of ensuring compliance with the PCMLTFA.
Section 3.10	Recommendation 17 Legislative amendments enacted in December 2006 and regulatory provisions implementing an administrative monetary penalty regime enacted in December 2007 which come into force in December 2008 address the gaps in compliance with this recommendation.
Section 3.11	Special Recommendation VI MSBs have been subject to broad-based reporting, CDD, and record keeping requirements since 2001. These obligations are being further expanded in regulations enacted in June 2007 which come into force in June 2008. There has been effective compliance monitoring of the sector by FINTRAC. Legislative amendments enacted in December 2006 and regulatory provisions enacted in June 2007 will establish an MSB registration regime as of June 2008.
Section 4.1	Recommendation 12 Casinos, accountants and real estate agents have been subject to some CDD and record-keeping requirements since 2001. Regulations enacted in June 2007 which come into force in June 2008 will expand requirements for these sectors. New regulations enacted in December 2007 and coming into force in December 2008 cover additional DNFBP sectors, thereby further addressing deficiencies identified. Regarding Internet and cruise ship casinos, it should be noted that Internet casinos

Relevant sections and paragraphs	Country Comments
	are illegal under the Criminal Code and enforcement action has been taken. There are no Canadian flagged ships operating casinos and shipboard casinos are subject to restrictions to limit access and abuse.
Section 4.2	Recommendation 16 Casinos, accountants and real estate agents have been subject to suspicious transaction reporting requirements since 2001. Regulations enacted in December 2007 which come into force in December 2008 will expand these requirements to cover additional DNFBP sectors, thereby further addressing deficiencies identified.
Section 4.3	Recommendation 24 Supervision mechanisms have been in place since 2001 for the casino, real estate and accounting sectors. Legislative amendments enacted in December 2006 and regulatory provisions enacted in December 2007 which come into force in December 2008 will further address deficiencies.

ANNEX 1

Legislative and regulatory Changes to the Canadian AML/CFT regime

Amendment	Legislation Enacted	Regulations Enacted	Measure Fully In Force
Extending record retention time period for FINTRAC	Dec 14, 2006	n/a	Feb 10, 2007
Enhanced information sharing on non-profit organisations	Dec 14, 2006	n/a	June 30, 2007
Enhanced FINTRAC disclosure information	Dec 14, 2006	June 27, 2007	June 30, 2007
Prohibition against correspondent relationships with shell banks	Dec 14, 2006	June 27, 2007	June 30, 2007
Correspondent banking due diligence requirements	Dec 14, 2006	June 27, 2007	June 30, 2007
Explicit prohibition on opening accounts for unidentified customers	Dec 14, 2006	n/a	June 23, 2008
Application to foreign branches or subsidiaries	Dec 14, 2006	n/a	June 23, 2008
Non-face-to-face CDD measures	n/a	June 27, 2007	June 23, 2008
Use of an agent or mandatary for customer identification (clarifying provision)	n/a	June 27, 2007	June 23, 2008
Beneficial owner requirements	n/a	June 27, 2007	June 23, 2008
Enhancing CDD and Record Keeping	Dec 14, 2006	June 27, 2007	June 23, 2008
PEPs requirement for financial institutions	Dec 14, 2006	June 27, 2007	June 23, 2008
Special attention to complex and unusual transactions (*i.e.* risk assessment)	Dec 14, 2006	June 27, 2007	June 23, 2008
Reporting suspicious attempted transactions	Dec 14, 2006	June 27, 2007	June 23, 2008
Special attention to business from countries of risk (*i.e.* risk assessment)	Dec 14, 2006	June 27, 2007	June 23, 2008
MSB registration	Dec 14, 2006	June 27, 2007	June 23, 2008
Wire transfers travel rule	Dec 14, 2006	June 27, 2007	June 23, 2008
Enhancing measures for casinos, accountants and real estate, including: • Enhanced CDD and record-keeping. • Non face to face measures. • Use of agent and mandatary. • Special attention to transactions.	Dec 14, 2006	June 27, 2007	June 23, 2008
Inclusion of Lawyers, BC Notaries and Jewellers, including measures on: • CDD and record-keeping. • Non face to face measures. • Use of agent and mandatary. • Special attention to transactions. • Triggers for STR reporting (except lawyers). • Coverage by FINTRAC to ensure compliance.	Dec 14, 2006	Dec 2007	Dec 2008
Administrative Monetary Penalties provisions	Dec 14, 2006	Dec 2007	Dec 2008
Application to businesses and professions at risk (real estate developers)	n/a	Feb 2008	Feb 2009