Financial Action Task Force

Groupe d'action financière

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

THE UNITED KINGDOM OF GREAT BRITAIN AND NORTHERN IRELAND

29 JUNE 2007

Table of Contents

PREFACE - information and methodology used for the evaluation of the United Kingdom 3

Executive Summary 4

1. General 13
1.1 General information on the United Kingdom 13
1.2 General Situation of Money Laundering and Financing of Terrorism 15
1.3 Overview of the financial sector and designated non-financial businesses and professions 16
1.4 Overview of commercial laws and mechanisms governing legal persons and arrangements 21
1.5 Overview of strategy to prevent money laundering and terrorist financing 23

2. Legal System and Related Institutional Measures 33
2.1 Criminalisation of Money Laundering (R.1 & 2) 33
2.2 Criminalisation of Terrorist Financing (SR.II) 41
2.3 Confiscation, freezing and seizing of proceeds of crime (R.3) 47
2.4 Freezing of funds used for terrorist financing (SR.III) 64
2.5 The Financial Intelligence Unit and its functions (R.26, 30 & 32) 78
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 & 32) 90
2.7 Cross Border Declaration or Disclosure (SR.IX) 102

3. Preventative Measures – Financial Institutions 106
3.1 Risk of money laundering or terrorist financing 111
3.2 Customer due diligence, including enhanced or reduced measures (R.5 to 8) 112
3.3 Third parties and introduced business (R.9) 128
3.4 Financial institution secrecy or confidentiality (R.4) 131
3.5 Record keeping and wire transfer rules (R.10 & SR.VII) 132
3.6 Monitoring of transactions and relationships (R.11 & 21) 139
3.7 Suspicious transaction and other reporting (R.13-14, 19, 25 & SR.IV) 143
3.8 Internal controls, compliance, audit and foreign branches (R.15 & 22) 149
3.9 Shell banks (R.18) 155
3.10 The supervisory and oversight system - competent authorities and SROs; Role, functions, duties and powers (including sanctions) (R.23, 29, 17 & 25) 157
3.11 Money or value transfer services (SR.VI) 200

4. Preventative Measures – Designated Non-Financial Businesses and Professions 203
4.1 Customer due diligence and record-keeping (R.12) 204
4.2 Monitoring transactions and other issues (R.16) 213
4.3 Regulation, supervision and monitoring (R. 24-25) 217
4.4 Other non-financial businesses and professions (R.20) 229

5. Legal Persons and Arrangements & Non-Profit Organisations 230
5.1 Legal Persons – Access to beneficial ownership and control information (R.33) 230
5.2 Legal Arrangements – Access to beneficial ownership and control information (R.34) 237
5.3 Non-profit organisations (SR.VIII) 240

6. National and International Co-Operation 245
6.1 National co-operation and coordination (R.31 & 32) 245
6.2 The Conventions and UN Special Resolutions (R.35 & SR.I) 250
6.3 Mutual Legal Assistance (R.36-38, SR.V, R.32) 252

6.4 Extradition (R.39, 37 & SR.V) 265
6.5 Other Forms of International Co-operation (R.40, SR.V & R.32) 274

7. OTHER ISSUES 282
7.1 Resources and statistics 282

TABLES....283
Table 1: Ratings of Compliance with FATF Recommendations....283
Table 2: Recommended Action Plan to Improve the AML/CFT System 289

ANNEXES....294
Annex 1: List of abbreviations and acronyms 294
Annex 2: Details of all bodies met on the on-site mission: Ministries, other government authorities or bodies, private sector representatives and others 295
Annex 3: List of laws, regulations and other guidance received....297
Annex 4: Copies of key laws, regulations and other measures 299

PREFACE - information and methodology used for the evaluation of the United Kingdom

1. The evaluation of the anti-money laundering (AML) and combating the financing of terrorism (CFT) regime of the United Kingdom was based on the Forty Recommendations 2003 and the Nine Special Recommendations on Terrorist Financing 2001 of the Financial Action Task Force (FATF), and was prepared using the AML/CFT Methodology 2004[1]. The evaluation was based on the laws, regulations and other materials supplied by the United Kingdom of Great Britain and Northern Ireland (UK), and information obtained by the evaluation team during its on-site visit to the UK from 27 November to 8 December 2006, and subsequently. During the on-site, the evaluation team met with officials and representatives of all relevant UK government agencies and the private sector. A list of the bodies met is set out in Annex 2 to the mutual evaluation report.

2. The evaluation was conducted by an assessment team, which consisted of members of the FATF Secretariat and FATF experts in criminal law, law enforcement and regulatory issues: Mr. Alain Damais, Executive Secretary of FATF and Mr. Kevin Vandergrift (FATF Secretariat); Ms. Elisabeth Florkowski, Expert, Integrated Supervision, Financial Market Authority, Austria (financial expert); Ms. Violaine Clerc, Head of the Legal Affairs Department, Commission Bancaire, France (financial expert); Mr. Pieter Smit, Head, Legal & Policy Division, Financial Intelligence Centre, South Africa (legal expert); Mr. Wayne Walsh, Deputy Principal Government Counsel, International Law Division, Department of Justice, Hong Kong,China (legal expert); and Mr. Alessio Nardi, Lieutenant Colonel, Guardia di Finanza, Italy (law enforcement expert). The experts 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. This report provides a summary of the AML/CFT measures in place in the United Kingdom as at the date of the on-site visit or immediately thereafter. It describes and analyses those measures, sets out the UK's levels of compliance with the FATF 40+9 Recommendations (see Table 1), and provides recommendations on how certain aspects of the system could be strengthened (see Table 2).

[1] As updated in June 2006.

Executive Summary

1. Background Information

1. This report provides a summary of the AML/CFT measures in place in the United Kingdom of Great Britain and Northern Ireland (UK) 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. It also sets out the UK's levels of compliance with the FATF 40+9 Recommendations (see the attached table on the Ratings of Compliance with the FATF Recommendations).

2. The UK has a comprehensive legal structure to combat money laundering and terrorist financing. The money laundering offence is broad, fully covering the elements of the Vienna and Palermo Conventions, and the number of prosecutions and convictions is increasing. The terrorist financing offence is also broad. The introduction of the Proceeds of Crime Act 2002 (POCA) has had a significant and positive impact on the UK's ability to restrain, confiscate and recover proceeds of crime. The UK has also established an effective terrorist asset freezing regime. Overall, the UK FIU appears to be a generally effective FIU. The UK has designated a number of competent authorities to investigate and prosecute money laundering offences. Measures for domestic and international co-operation are generally comprehensive as well.

3. The effectiveness of current preventative measures for financial institutions varies; the situation will be improved with the implementation of the 3rd EU Money Laundering Directive later in 2007. Currently, the main CDD deficiencies lie in the fact that certain requirements, such as beneficial ownership, are not laid out in law or regulation. Record-keeping and STR requirements are comprehensive and effective. The Financial Services Authority (FSA) has extensive powers to monitor and ensure compliance by the financial institutions it regulates. While the supervisory system is comprehensive for the larger firms, supervision of certain smaller firms (including some small banks, insurance companies, securities dealers, and investment managers) requires enhancement.

4. All designated non-financial businesses and professions (DNFBPs) as defined by the FATF are covered under the Money Laundering Regulations 2003. DNFBPs appear to be effectively complying with their STR obligations. There is generally comprehensive monitoring of casinos, and lawyers and certain accountants; the main deficiencies lie in the lack of monitoring for the real estate and company service provider sectors and certain unregulated accountants. These sectors will be supervised once the 3rd EU directive is implemented.

5. The UK is a political union made up of four constituent countries: England and Wales (which for legal purposes counts as a single jurisdiction) and Northern Ireland are common law jurisdictions, and Scotland, which operates a hybrid system based on both common law and civil law principles. The UK is a constitutional monarchy, with executive power exercised on behalf of Her Majesty Queen Elizabeth II by a democratically elected Prime Minister and other "Cabinet Ministers" who head the departments of state. Although the Parliament at Westminster remains the seat of Government for the UK, Scotland, Wales, and Northern Ireland have a degree of devolved government. Official estimates in 2004 indicated a population of 59,834,300. Based on market exchange rates, the UK is the fifth-largest economy in the world, the second largest in Europe, and the sixth-largest overall by purchasing power parity (PPP) exchange rates. The currency of the UK is pound sterling, represented by the symbol "£"[2].

6. The overall threat to the UK from serious organised crime, and contingent money laundering, is high. UK law enforcement estimates the economic and social costs of serious organised crime,

[2] At the time of the on-site visit, 1 £ = 1.48 EUR or 1.93 USD.

including the costs of combating it, at upwards of £20 billion a year. It is estimated that the total quantified *organised crime* market in the UK is worth about £15 billion per year as follows: drugs (50%); excise fraud (25%); fraud (12%); counterfeiting (7%); organised immigration crime (6%). Estimated total recoverable criminal assets per annum are £4.75 billion, of which it is estimated that GBP 2.75 billion is sent overseas. Cash remains the mainstay of most serious organised criminal activity in the UK. The following typologies are currently those of most concern to UK law enforcement: cash/value couriering; abuse of "gatekeepers"; abuse of money transmission agents (including Hawala and other alternative remittance systems); cash rich businesses & front companies; high value assets and property; abuse of bank accounts and other over-the-counter financial sector products.

7. The UK has substantial experience in responding to terrorist threats and the support networks that make terrorist acts possible; the principal current terrorist threat facing the UK is from extremists using a distorted and unrepresentative version of the Islamic faith to justify violence. This threat is genuinely international in nature. Attacks have been carried out in Britain by both British nationals and by outsiders. The domestic and international dimensions of the threat are therefore closely linked. The use of banks to move terrorist funds overseas is thought to have declined in response to the tightening of controls in that sector. Two areas of growing concern are: the abuse of charitable organisations to raise and distribute funds, and the abuse of the 'money service business' (MSB) sector (including alternative remittance services) to move funds.

8. All types of "financial institutions" as defined in the FATF methodology are active in the UK, and all are covered by the current Money Laundering Regulations 2003 (MLRs 2003). The UK is a major international centre for investment and private banking and has one of the largest commercial banking sectors in the world. The UK insurance industry is the largest in Europe and third largest in the world and is also one of the largest fund management markets in the world. It has a strong international orientation and attracts significant overseas funds (it is estimated that the UK fund management industry was managing over £2,960bn of funds at the end of 2004). This includes international private wealth management, hedge funds and private equity.

9. All types of "designated non-financial businesses & professions" (DNFBPs) as defined in the FATF methodology are active in the UK and all are within the scope of the MLRs 2003. The UK has a wide range of legal persons and arrangements. Legal forms include: Companies Act companies and other forms of companies (both public and private), partnerships, and societies. Trusts are a long-standing, popular, and integral part of the legal and economic landscape of the UK.

2. Legal Systems and Related Institutional Measures

10. The money laundering offences in the UK are comprehensive in their scope and appear to be used frequently. The introduction of POCA brought about a major improvement over the precursor legislation since it is no longer necessary for the authorities to distinguish between drug trafficking and other predicate offences upon the evidence at their disposal in order to prosecute money laundering offences. In England and Wales, the number of investigations, prosecution and convictions under POCA have each been increasing substantially each year since POCA first came into force in 2003.

11. The provisions criminalising terrorist financing have a generally broad coverage. The provisions specifically cover collecting or providing funds to be used for a terrorist act and providing funds to be used by a terrorist organisation or an individual terrorist; the provisions also appear sufficient to cover collection of funds for use by terrorist organisations and individual terrorists.

12. The UK has a comprehensive regime to confiscate criminal proceeds. The introduction of POCA has had a significant and positive impact on the UK's ability to restrain, confiscate and recover proceeds of crime. The provisions of the Act, particularly on the criminal confiscation side, appear to

be working reasonably well in practice. The UK also has sufficient provisional measures to freeze and seize property and instrumentalities.

13. The UK has established an effective terrorist asset freezing regime. As a member of the European Union, the UK is bound by the EU freezing mechanism. Domestic measures, the Al-Qaida and the Taliban (United Nations Measures) Order 2006 (previously 2002) and the Terrorism (United Nations Measures) Order 2006 (previously 2001), expand upon the coverage of the EU regulations. These measures include a domestic designation process that appears rapid and efficient; a total of 84 individuals and 58 entities had been designated under the 2006 UN Order at the time of the on-site visit. Failure to abide by an asset freeze under the Order is punishable by seven years imprisonment and an unlimited fine. The Bank of England, as Her Majesty's Treasury's (HMT's) agent on asset freezing, is responsible for issuing notices with respect to persons designated and maintains a consolidated sanctions list on its website. The UK has used the powers available under the orders on a number of occasions to take rapid asset freezing action against suspected terrorists.

14. Since March 2006, the UK FIU has been housed within the Serious Organised Crime Agency (SOCA) but operates with a high degree of independence. Overall, the UK FIU substantially meets the criteria of Recommendation 26 and appears to be a generally effective FIU; the private sector reported improved relations and co-operation since the transfer of the FIU responsibilities to SOCA in March 2006. However, the UK FIU has not released public reports on statistics, typologies and trends, as well as information regarding its activities, in a manner required by the FATF standards. The UK FIU could also conduct more proactive STRs analysis. The FIU now has 97 staff; however, the UK FIU should continue to increase its staff, especially its analytical staff, in line with the objective set out in the SARs ("Lander") review. UK officials should also continue to work to improve the current "consent" process (explained below), which appears to create an undue burden for the private sector and the FIU.

15. The UK has taken a pro-active approach to pursuing not only predicate offences but also the proceeds of crime and the financial aspects of terrorist cases. The UK has designated a number of competent authorities to investigate and prosecute money laundering offences. Investigation and prosecution agencies include, for the UK: SOCA and Her Majesty's Revenue and Customs (HMRC); for England and Wales: the Crown Prosecution Service (CPS) and the Revenue and Customs Prosecution Office (RCPO); for Northern Ireland the Public Prosecution Service of Northern Ireland (PPSNI); for Scotland, the Crown Office and Procurator Fiscal Services (COPFS) and the Scottish Crime and Drug Enforcement Agency (SCDEA). There are also 43 regional police forces in England and Wales, 8 in Scotland, and 1 in Northern Ireland. The National Terrorist Finance Investigation Unit (NTFIU) actively pursues terrorist financing issues in conjunction with all terrorism investigations. The various agencies appear adequately structured, funded, and resourced to effectively carry out their functions. Integrity standards, including standards of confidentiality, are high for investigators and prosecutors.

16. The system for disclosing cross-border movements of currency and bearer negotiable instruments appears generally effective; however, UK authorities do not have the authority to detain cash purely for a false disclosure, and there is no requirement to retain, at a minimum, the amount and identification the bearer in amount of disclosures where there is a false disclosure, although cash seizure provisions allow individual officers significant discretion to take action on the basis of a "reasonable grounds to suspect" test. Nor is there is a specific requirement to maintain this data in the event of a suspicion of ML/FT. The EU Council Regulation No 1889/2005 ("the Cash Controls Regulation") will also apply in the UK as of 15 June 2007. The regulation will apply a declaration system that will complement the existing disclosure system, although the declaration provisions will apply only to cross-border movements of currency and bearer negotiable instruments into and out of the EU.

3. Preventive Measures – Financial Institutions

17. The Money Laundering Regulations 2003 (MLRs), Proceeds of Crime Act 2002 and the Terrorism Act apply to all financial institutions carrying out financial activities as defined by the FATF. For FSA-regulated firms, additional obligations are laid out in the FSA Handbook, and include additional regulatory requirements as well as guidance. The Joint Money Laundering Steering Group (JMLSG) Guidance Notes provide further detail to the MLRs. These guidance notes as a whole cannot be considered as "other enforceable means" as defined by the FATF. However, parts of the guidance are linked to specific Rules, and when those Rules are read inclusively with the guidance, the content of the guidance on those particular points could be regarded as part of the enforceable means. Other parts of the guidance are not linked to specific Rules and are therefore only guidance.

18. The UK uses a risk-based approach to financial sector regulation. In general, the risk-based approach applies to two main areas: (1) the JMLSG Guidance Notes generally indicate that firms should apply the particular guidance to the extent that that is required, taking into account the firm's risk-based view on the need to do so in order to meet its more high level obligations under the MLRs and the FSA Handbook; and (2) the level of supervision that a financial institution receives by the FSA is also determined on a risk-based approach. To determine the level of supervision, the financial institutions are divided by the level of "impact" to the financial sector, based initially on the firm's total assets but can then be raised or lowered according to a number of factors, and ratings are determined for the level of risk.

19. MLRs contain basic customer identification requirements pursuant to the 2nd EU Money Laundering Directive. These include when establishing business relations, when conducting transactions over EUR 15,000, and when there is a suspicion of money laundering and terrorist financing. Overall, however, the CDD requirements contain a number of gaps. For example: there is no requirement in law or regulation to identify the beneficial owner or take reasonable measures to verify the identity of the beneficial owner, to determine who are the natural persons that ultimately own or control the customer, including those persons who exercise ultimate effective control over a legal person or arrangement or for on-going monitoring. Further, certain elements are not addressed in either law, regulation, or other enforceable means, such as an obligation to apply CDD to existing customers on the basis of materiality and risk, and measures for enhanced due diligence are not sufficient. Many of these issues will be addressed in the implementation of the 3rd ML Directive, scheduled for December 2007. Until that time, the JMLSG Guidance Notes provide comprehensive guidance to the private sector.

20. Other issues are currently encouraged on a risk-based approach in the guidance and are not directly mandatory, although there is evidence that the majority of firms address AML/CFT risk in line with the available guidance. UK authorities should make more direct obligations: to obtain information on the intended purpose and nature of the business relationship; to specify the procedures for on-going due diligence in compliance with the FATF Recommendations; to require that financial institutions maintain documents and other CDD data up-to-date and relevant by undertaking regular reviews. Regarding politically exposed persons (PEPs), the UK authorities should create enforceable obligations in this regard as soon as possible. While current language in the JMLSG Guidance on correspondent banking is generally comprehensive and appears to cover the main areas of Recommendation 7, it does not currently constitute an enforceable requirement.

21. Regarding introduced business, there is no current enforceable requirement that the financial institutions be satisfied that the introducer will make ID and other relevant documentation available upon request. Financial institutions are not required to satisfy themselves that the third party is regulated and supervised (in accordance with Recommendation 23, 24 and 29), and has measures in place to comply with, the CDD requirements.

22. There are no financial institution secrecy laws in the UK that inhibit the implementation of the FATF Recommendations, and record-keeping requirements are comprehensive. The new EU

Regulation No. 1781/2006, in force as of 1 January 2007, generally meets the technical requirements as set out in SR.VII. However, wire transfers within the EU are classified as domestic; the cross-border element in a non-domestic wire transfer is as an obstacle for timely access to the full originator information. In addition, sanctions for non-compliance will only be in place as of 15 December 2007.

23. There is no specific obligation to monitor all complex, unusual large transactions, to examine as far as possible the background and purpose of such transactions and to set forth findings in writing. However, there is generally comprehensive guidance in the JMLSG Guidance Notes, and the FSA-regulated institutions seem to follow the guidance effectively. The UK authorities should adopt more specific requirements to monitor transactions involving certain countries and to make out findings in writing.

24. The obligations on the regulated sector to submit suspicious activity reports (SARs) are comprehensive. There is no *de minimis* limit; and attempted transactions are also covered. However, there are some concerns regarding its current set up and implementation: the fact that, after a SAR has been filed, many banks now interpret the current legislation as requiring them to seek consent on every subsequent transaction over 250 pounds for that same customer. The legislation provides immunity from prosecution for those persons who report suspicions to the UK FIU in good faith. "Tipping off" is an offence, as is "prejudicing an investigation."

25. UK FIU has posted guidance on how to complete a SAR and when filing a SAR should be considered. General feedback and typologies provided to the reporting sectors appears generally comprehensive; private sector representatives across the board noted a welcomed increase of outreach and feedback from the UK FIU since it was transferred to SOCA in April 2006.

26. Overall, the system of internal controls is generally strong and complete. The FSA's supervisory approach, in its strong core area related to AML/CFT, focuses on the internal controls and compliance arrangements financial institutions have in place to prevent money laundering and terrorist financing as part of wider systems and controls issues. However, there should be a more direct requirement for firms to maintain an independent audit function. The UK should also adopt more specific rules relating to foreign branches and subsidiaries in relation to the requirements of Recommendation 22.

27. Shell banks are not permitted to be established or continue to operate in the UK. There is, however, no obligation for financial institutions not to enter into, or continue, correspondent banking relationships with shell banks or to require them to satisfy themselves that respondent financial institutions in a foreign country do not permit their accounts to be used by shell banks. However, the JMLSG Guidance Notes provide guidance in this area.

28. All types of financial institutions as defined in the FATF methodology are subject to the Money Laundering Regulations 2003. The Financial Services Authority (FSA) is the prudential and designated AML/CFT regulator for financial institutions carrying out activities under the Financial Services and Markets Act (FSMA). The FSA has extensive powers to monitor and ensure compliance by the financial institutions it regulates. The FSA has the authority to conduct on-site inspections to ensure compliance; such inspections can include the review of policies, procedures, books and records, and extends to sample testing. As a whole, the FSA seems adequately funded, staffed and has sufficient technical and other resources to fully and effectively perform its functions. The FSA is accountable to Treasury Ministers, and through them to Parliament. To fund its work, the FSA charges fees to all authorised financial institutions that carry out activities that it regulates.

29. There are a variety of criminal sanctions available in various pieces of AML/CFT legislation. The FSA also has a broad range of administrative sanctions available to it against financial institutions as well as managers and directors, including unlimited financial penalties, public censure, prohibition, variation or cancellation of permission to operate or carry out certain functions, injunction, and issuance of a formal caution.

30. On-going supervision of financial institutions is determined by a risk-based approach. This internal process is called "Advanced Risk Responsive Operating frameWork" (ARROW). The FSA measures the risk (the impact and probability before deciding on the nature of its supervisory relationship or the action (if any) that needs to be taken and by whom, to mitigate the risk. The FSA undertakes an "impact" assessment of each financial institution to measures the size of the firm and number of customers. For financial institutions whose impact is scored as medium-low or above (*i.e.* banking institutions with total assets over GBP 450 million, life insurance and securities firms with assets over £900 million, and investment management firms managing funds over £2 billion, although for private equity firms it is £500 million and for Hedge Funds it is £800 million), the FSA undertakes a separate institutional risk/probability assessment to judge the overall risk it presents. Firms below these thresholds are first scored as "low impact" (unless their score has been overridden by specific factors) and supervised as "small firms". Additionally, the impact of a risk is assessed using qualitative measures in the FSA's overarching Risk Dashboard to further target FSA supervision resources towards key areas of risk. Following the ARROW firm risk assessment, the FSA will send the ARROW letter, along with the risk mitigation program (RMP), which imposes requirements on firms to mitigate any deficiencies or risks identified.

31. For the largest financial institutions (39 complex major retail groups, which account for about 80% of retail business in the UK, and 43 major wholesale groups), where the potential impact of failure on consumers and the wider economy is high (*i.e.* "high impact"), the FSA adopts "close and continuous" supervision, with more intense supervision and regular risk assessments (typically every 12-24 months). Small firms (as are all firms) are subject to baseline (off-site) monitoring and to "Thematic Work," which aim to assess score and mitigate the risks of a particular issue. The normal output from this work tends to be in the form of a communication to the regulated sector or individual institutions, discussion papers, or guidance on the FSA website.

32. While the supervisory system is generally comprehensive for the larger ("high impact" firms), there is less adequate supervision for certain smaller firms (including some small banks, insurance companies, securities dealers, and investment managers) – the risk assessment and resulting level of supervision can rely too heavily on the size of the financial institutions and does not always adequately take AML/CFT risk into account. There also appears to be an over reliance on interview-based visits without sample testing. In addition, there are activities that come under the FATF definition which are neither supervised nor obliged to comply with FSA rules and industry guidance (consumer credit, financial leasing, guarantees and commitments, brokers, factoring, safe-keeping and administration). UK authorities plan to cover these areas when implementing the 3rd EU Money Laundering Directive.

33. Since 30 November 2001, the FSA's Enforcement Division has dealt with one hundred and sixty seven cases relating to a form of financial crime (including market abuse matters); of these cases, eighteen have related specifically to anti-money laundering compliance. Of these, three have resulted in a private warning, eight resulted in a fine, two resulted in a variation of the firm's permissions and one resulted in a prohibition (for a total of 14 enforcement actions). Having regard to the size of the UK's financial sector, the number of FSA disciplinary sanctions (since 2001) seems relatively low.

34. The JMLSG Guidance is the key document that provides practical interpretation to financial institutions in complying with AML/CFT legislation, FSA AML rules and good generic industry practice guidance. These are extensive, comprehensive documents, and are extremely useful for the industry. The FSA has also established a number of mechanisms to help financial institutions to comply with their regulatory requirements.

35. Her Majesty's Revenue and Customs (HMRC) supervises "money service businesses" (MSBs), including money exchangers and money/value transfer offices. HMRC also has adequate powers to obtain access to all records, document or information relevant to monitoring compliance. HMRC may issue a warning letter and impose financial penalties up to GBP 5,000. There are not adequate

sanctions that can be used against directors and senior managers. The evaluation team also had some minor concerns about the effectiveness of the sector's supervision due to the large size of this sector particularly exposed to ML and FT risks.

4 Preventive Measures – Designated Non-Financial Businesses and Professions

36. All designated non-financial businesses and professions (DNFBPs) as defined by the FATF are covered under the Money Laundering Regulations 2003. The JMLSG Guidance notes do not apply, although all the DNFBP sectors have issued guidance to supplement the MLRs. While the MLRs impose certain CDD measures, recordkeeping, and other preventative measures, the deficiencies are the same as indicated above for financial institutions.

37. DNFBPs have comprehensive obligations to report SARs, and appear to be adequately complying with these obligations. However, as with financial institutions, the UK authorities should adopt stronger obligations to monitor transactions (Recommendations 11 and 21). The UK should also require that the estate agents identify the buyer of real estate.

38. The supervisory framework for casinos is currently in transition. A regime was established under the Gaming Act 1968, which gave the "Gaming Board" authority to license, supervise, and sanction casinos for provisions of the Act and AML compliance. Under the new Gambling Act 2005, the previous authorities of the Board, with new strengthened supervisory capabilities, have passed to the "Gambling Commission." The Gambling Commission has already been established; other provisions of the Act are due to come into effect in September 2007. In general, legal or regulatory measures 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. Current sanctions available to the Commission include those that go against the licensing requirements and collusion of staff in illegal activities. Possible sanctions for AML/CFT breaches generally include the authority to issue warnings and revoke a license; the range of sanctions should be expanded. (The range of sanctions will be expanded once the new Gambling Act 2005 comes into force later in 2007.)

39. Legal professionals are subject to a generally adequate system of AML/CFT monitoring conducted by the various self-regulatory organisations for England, Wales, Northern Ireland, and Scotland. Accountants that are members of professional bodies also receive adequate AML monitoring; however, there is a concern about the numerous accountants that are not members of professional bodies. In addition, real estate agents, and trust and company service providers that are not lawyers or accountants are not yet supervised for AML/CFT. The UK authorities plan to address these areas when implementing the 3rd EU Money Laundering Directive later in 2007. High value dealers (which include dealers in precious metals and stones) are subject to the same system of monitoring that HMRC applies to MSBs.

5. Legal Persons and Arrangements & Non-Profit Organisations

40. The UK has a wide range of legal persons and arrangements. Legal forms include: Companies Act companies and other forms of companies (11,500 public and over 2 million private companies), partnerships, and societies. The UK has a registration system for most of these legal persons; all companies formed under the Companies Act are required to have a registered office in the UK and are required to keep an up-to-date register of the names and addresses of its members. Trusts are a long-standing, popular, and integral part of the legal and economic landscape of the UK.

41. The UK's approach to preventing the unlawful use of legal persons and legal arrangements for ML and FT relies on the investigative and other powers of law enforcement, regulatory, supervisory, and other competent authorities to obtain or get access to information. While the investigative powers are generally sound, there are not adequate measures in place to ensure that there is adequate, accurate and timely information on the beneficial ownership and control of legal persons that can be obtained or accessed in a timely fashion by competent authorities. Information on the companies registrar

pertains only to legal ownership/control (as opposed to beneficial ownership), is not verified, and is not necessarily reliable. Directors and shareholders can be nominees and other legal persons, which can slow down the investigative trail. It is recommended that the UK authorities review the current system to determine ways in which adequate and accurate information on beneficial ownership may be available on a timely basis to law enforcement authorities.

42. England, Wales, and Scotland have well-established systems for the regulation of charities with adequate provision for the registration, transparency, supervision and investigation of charities. The Charity Commission has extensive legal powers to allow it sanction wrongdoing or mismanagement in charities or anything purporting to be a charity in England and Wales. The Charity Commission conducts 400 targeted "Review Visits" each year to review compliance with the Charities Act 2003. These are normally based on information submitted in the annual returns. However, a supervisory regime does not yet apply to Northern Ireland (although legislation was being drafted at the time of the on-site visit). Authorities should therefore develop appropriate procedures for registration, transparency, supervision and investigation of charities in Northern Ireland as soon as possible.

6. National and International Co-operation

43. Internal co-operation and co-ordination between UK policy makers, the FIU, law enforcement and supervisors and other competent authorities appears effective both at the policy and operational levels. The system benefits from an effective network of interdepartmental and interagency contact and co-operation both for policy and for operational matters. These include: the Money Laundering Advisory Committee" (MLAC), which develops AML policy, and the Terrorist Finance Action Group (TFAG), which forms part of the wider Whitehall framework on counter-terrorism, and the Asset Freezing Working Group (AFWG), which is chaired by HMT and agrees the handling of individual asset freezing cases as well as the architecture of the UK's asset freezing regime. In addition, the UK has regularly reviewed the effectiveness of its AML/CFT systems; results and recommendations of the reviews have been endorsed by ministers and are now being implemented. The UK authorities should continue to implement the recommendations of the various AML/CFT reviews.

44. The UK has ratified and implemented the provisions of the Vienna, Palermo and CFT Conventions and the provisions of S/RES/1267(1999) and S/RES/1373(2001). The UK has broad legal provisions to facilitate requests for mutual legal assistance. Standard evidence gathering mechanisms have recently been reviewed and updated in the Crime (International Co-operation) Act 2003, and new provisions have been introduced to allow for the restraint and confiscation of instrumentalities of crime at the request of foreign jurisdictions. New legislation has also been introduced under POCA to give effect to foreign restraint, confiscation and forfeiture orders in both the criminal and civil context.

45. There are no unduly restrictive measures placed on the provision of assistance, and dual criminality is only required for certain coercive measures such as search warrants. In these cases, the UK appears to have no legal or practical impediment to rendering assistance where both countries criminalise the conduct underlying the offence. The UK is able to share confiscated or forfeited assets with other jurisdictions, and internally is able to use funds confiscated to incentivise law enforcement and prosecution agencies in their work. However, there are concerns about the ability of the UK authorities (excluding Scotland) to handle routine or non-urgent mutual legal assistance requests in a timely and effective manner.

46. Money laundering and terrorist financing are extraditable offences; there are no restrictive conditions or impediments existing in law for extradition. The UK can extradite its own nationals. Extradition law and procedure in the UK was significantly altered by the introduction of the Extradition Act 2003. This was necessary to implement obligations in relation to the EU Framework Decision concerning the European Arrest Warrant (EAW) scheme ("Part 1" in the Extradition Act 2003). However, procedures for all other jurisdictions ("Part 2") were also changed with a view to expediting the process of extradition. Overall, the UK has systems in place for adequate administrative co-operation, equally for the FIU, law enforcement, and financial supervisors.

7. Resources and Statistics

47. Competent authorities, including law enforcement and the FSA, appear adequately structured and resourced to effectively perform their functions. However, in order to more effectively perform its tasks, HMRC should deploy a broader allocation of resources at all levels of ML/FT risk for the MSB sector. The FIU, while its numbers have already increased, should also increase resources in order to meet commitments made under recent government reviews.

48. In general, the various UK authorities maintain a wide range of statistics on the full range of AML/CFT matters. However, with regard to MLA requests, there are no statistics on the breakdown of the offences concerned in each case (*i.e.* ML, predicate offences, or FT), nor on the number granted and refused, or the time required to respond. Information technology provisions for MLA requests are currently under review by the UK Central Authority. Nor are there comprehensive statistics for the number of SARs analysed and disseminated by the FIU.

1. General

1.1 General information on the United Kingdom

1. The United Kingdom of Great Britain and Northern Ireland (often shortened to "The United Kingdom", or the "UK") is a political union made up of four constituent countries: England, Scotland, and Wales on the island of Great Britain, and Northern Ireland. Official estimates in 2004 indicated a population of 59,834,300. UK's overall population density is one of the highest in the world. About a quarter of the population lives in England's prosperous southeast and is predominantly urban and suburban, with about 7.2 million in the capital, London.

Economy

2. Based on market exchange rates, the UK is the fifth-largest economy in the world, the second largest in Europe after Germany, and the sixth-largest overall by purchasing power parity (PPP) exchange rates. The currency of the UK is pound sterling, represented by the symbol "£"[3]. The Bank of England is the central bank and is responsible for issuing currency, although banks in Scotland and Northern Ireland retain the right to issue their own notes, subject to retaining enough Bank of England notes in reserve to cover the issue. Since 1997, the Bank of England has exercised control of interest rates and other monetary policy, independent of Government. Government intervention in the economy is exercised at a macroeconomic level, primarily through HM Treasury, the UK's economics and finance ministry.

System of government

3. The UK is a constitutional monarchy, with executive power exercised on behalf of Her Majesty Queen Elizabeth II by a democratically elected Prime Minister and other "Cabinet Ministers" who head the departments of state. The UK does not have a codified constitution, relying instead on traditional customs and separate pieces of constitutional law. While the Queen is Head of State and theoretically holds all executive power, the Prime Minister is the Head of Government. The Parliament, the legislative body, is traditionally considered to be "supreme" (that is, able to legislate on any matter and not bound by decisions of its predecessors). Parliament consists of one entirely elected chamber, the House of Commons, and one part-hereditary part-appointed chamber, the House of Lords. An Act of Parliament does not become law until it has been signed by the monarch ("royal assent"). The party that commands a majority in the House of Commons further to a General Election (held once every 4-5 years) is normally appointed as Her Majesty's Government - or, if there is no majority party, the largest coalition.

Legal system and hierarchy of laws

4. Although the Parliament at Westminster remains the seat of Government for the UK, Scotland, Wales, and Northern Ireland have a degree of devolved government. This is exercised through, respectively: the Scottish Parliament, the National Assembly for Wales, and the Northern Ireland Assembly. Several areas of law-making remain reserved for the UK Parliament: this includes all law on money laundering and terrorist financing.

5. The Scottish Parliament of 129 members is elected every four years. It operates broadly on the Westminster model, electing a First Minister who heads the "Scottish Executive." The National Assembly for Wales has 60 members. It does not have the power to make primary legislation, but enjoys extensive executive powers and may make secondary legislation (such as orders and regulations fixing the detail of implementation of primary legislation). The Northern Ireland

[3] At the time of the on-site visit, 1 £ = 1.48 EUR or 1.93 USD.

Assembly consists of 108 members with a similar range of legislative and executive powers to the Scottish Parliament, although at the time of the on-site visit this body was suspended.

6. The United Kingdom has three distinct jurisdictions: Scotland, Northern Ireland, and England and Wales which for legal purposes counts as a single jurisdiction. England and Wales and Northern Ireland are common law jurisdictions, whereas Scotland operates a hybrid system based on both common law and civil law principles. The Act of Union 1707 guarantees the continued existence of a separate law system for Scotland. Unlike many countries, there is no single criminal or penal code, but rather an emphasis on the independence of prosecuting authorities and the judiciary. In all three countries, many areas of law developed over the centuries as courts made decisions and these decisions became a body of laws, established principles, and procedures.

7. Cases coming to court fall into one of two categories: civil or criminal. Civil cases are concerned mostly with disputes between individuals or corporate bodies. Cases must be proved on the balance of probabilities (more than a 50 per cent probability that the defendant is liable) rather than the "beyond reasonable doubt" standard applied in criminal cases. In both criminal and civil cases, the courts make decisions on an adversarial rather than an inquisitorial basis.

8. The House of Lords is the highest court in the land for all criminal and civil cases in England, Wales, and Northern Ireland, and for all civil cases in Scots law. Recent constitutional changes will see the powers of the House of Lords transfer to a new Supreme Court of the United Kingdom. In England and Wales, the court system is headed by the Supreme Court of Judicature of England and Wales, consisting of the Court of Appeal, the High Court of Justice (for civil cases) and the Crown Court (for criminal cases). Offences that are not (or potentially not) serious enough to be tried at Crown Court ("summary offences" and "triable either way offences") are tried at Magistrates' Courts, presided over by one or more Justice of the Peace (who can be a voluntary "lay magistrate"). Trial at Crown Court is before a jury, whereas Magistrate's Courts do not make use of juries. The system in Northern Ireland is nearly identical, headed by the Supreme Court of Judicature which incorporates the Northern Ireland Court of Appeal, High Court, and Crown Court. In Scotland, the chief courts are the Court of Session, for civil cases, and the High Court of Justice, for criminal cases, while the Sheriff Court is broadly the Scottish equivalent of the Magistrate's Court.

9. Statutory Instruments (SIs) (also known as secondary legislation, delegated legislation, or regulations) are the most common form of subordinate legislation. They are made by or under powers conferred by or under statute on Her Majesty in Council or on a Minister, the National Assembly for Wales or other body or person, and provide the detailed regulations which implement Acts of Parliament. They must always be within the scope of the enabling power in the parent Act.

Transparency, good governance, ethics and measures against corruption

10. The UK is not considered to have a significant problem with domestic corruption. The Transparency International 2005 "Corruption Perceptions Index" ranked the UK at 11th out of 158 (where 158 is most corrupt). Similarly, the findings of the Transparency International "Global Corruption Barometer" 2005 reflected the complete absence of bribe-paying from the social and economic landscape of the UK. Government Ministers, Members of Parliament, and public officials are all subject to strict, written rules in relation to their professional conduct, enforced through a framework of oversight committees and regulatory bodies. As a key international financial centre, the UK is at risk of being abused as a destination or channel for the proceeds of corruption perpetrated by foreign public figures overseas, as indicated by for example the high-profile case of the late Nigerian general Sani Abacha who moved stolen funds through the UK financial system in the 1990s. On an annual basis, the UK FIU routinely receives a significant volume of suspicious activity reports from the financial sector concerning suspected laundering of corrupt funds. Earlier in 2006, the Government launched a new police "international corruption taskforce" to specialise in the investigation of bribery overseas by UK entities and the laundering of corrupt funds from overseas in the UK.

11. The UK ratified the UN Convention Against Corruption on 14 February 2006. The UK is also a signatory to the Council of Europe Criminal Law Convention on Corruption, and has ratified the Convention on Combating Bribery of Foreign Public Officials in International Business Transactions ("the OECD Convention"). The OECD's report on the UK's compliance with this Convention approved in March 2005 (the "Phase 2 report") noted that in general "there had been no significant progress in implementation of the conclusions under the Phase 1bis examination", which raised concerns about the level of implementation of the OECD Convention by the UK authorities.

12. An OECD news release of January 2007 indicated that the OECD Working Group on Bribery had discussed the recent discontinuation by the United Kingdom of a major foreign bribery investigation concerning BAE SYSTEMS plc and the Al Yamamah defence contract with the government of Saudi Arabia. The Working Group had "serious concerns as to whether the decision was consistent with the OECD Anti-Bribery Convention and [would] discuss further the issue in March 2007, in the context of the United Kingdom written report on its implementation of recommendations set out in the 2005 Phase 2 examination report on its enforcement and application in practice of the OECD Convention." On 12-14 March 2007, the OECD Working Group on Bribery discussed the implementation by UK of the recommendations set out in the 2005 Phase 2 report and further discussed the BAE matter. Continuing concerns led the Group to agree to conduct a follow-up "Phase 2bis" review, including an on-site visit, to take place within a year.

1.2 General Situation of Money Laundering and Financing of Terrorism

Money laundering

13. The overall threat to the UK from serious organised crime, and contingent money laundering, is high. UK law enforcement estimates the economic and social costs of serious organised crime, including the costs of combating it, at upwards of £20 billion a year. It is estimated that the total quantified *organised crime* market in the UK is worth about £15 billion per year as follows[4]: drugs (50%); excise fraud (25%); fraud (12%); counterfeiting (7%); organised immigration crime (6%). Estimated total recoverable criminal assets per annum are £4.75 billion, of which it is estimated that £2.75 billion is sent overseas.

14. Cash remains the mainstay of most serious organised criminal activity in the UK. It leaves no audit trail and is the most reliable form of payment as well as the most flexible. "Cash couriers" play a significant role. A considerable amount of cash is physically smuggled and exchanged for local currency abroad. By analysing pound sterling (£) cash repatriated to the UK it is clear that cash smuggling is still a major method of money laundering utilised by organised crime gangs. In the view of the evaluation team, a potential vulnerability in this regard is that real estate may be purchased in cash, which could facilitate the laundering of cash smuggled into the UK.

15. Drug trafficking continues to attract the highest level of involvement from organised crime. The social and economic harm from serious crime connected to drug trafficking is considered by law enforcement to be the greatest criminal threat to the UK at this time. Law enforcement experience also suggests that organised crime gangs see immigration crime as lucrative and relatively low risk. Financial and other losses suffered by government, by companies, and by individuals, as a result of frauds are substantial, and fraud therefore constitutes a major threat. Between 2000 and 2004 the face value of counterfeit Sterling recovered in the UK rose from £5 million to £11 million

16. Organised crime groups generate substantial income through excise fraud. This includes: VAT Fraud, tobacco smuggling (including counterfeit goods); alcohol smuggling and diversion;

[4] *: these figures are currently being updated, and may be subject to change*

hydrocarbon oils smuggling and using rebated fuels for general use. VAT fraud exploits the EU VAT system and is by far the most serious type of fraud encountered by the UK's tax and customs authority, estimated to be worth up to £6 billion per year to organised crime groups (OGCs). Excise fraud is another substantial source of illegally obtained funds. There are three main types: tobacco smuggling, alcohol duty fraud, and hydrocarbon oil smuggling. The total amount lost to the economy through excise fraud is estimated at £4.74 billion in 2002/2003 rising to £5.03 billion in 2003/2004.

17. The following typologies are currently those of most concern to UK Law Enforcement, based on intelligence and investigative experience, but are not ranked in order: Cash / value couriering; abuse of "gatekeepers"; abuse of money transmission agents (including Hawala and other alternative remittance systems); cash rich businesses & front companies; high value assets & property; abuse of bank accounts and other over the counter financial sector products.

18. Demand for money laundering opportunities is generated by all acquisitive criminal enterprises active in the UK; however the majority of demand appears to come from organised gangs running drugs and / or immigration crime rackets. UK experience is that there is no one sector used to launder money, but that all parts of the regulated sector can be vulnerable to money laundering.

19. According to law enforcement observations, more cash is being taken abroad for laundering as controls in the UK have tightened; and generally, displacement of criminal property usually occurs when controls are tightened in a particular area.

20. UK law enforcement agencies all contribute to an annual threat assessment exercise to identify and gauge the scale of the threats posed to the UK by serious and organised crime. The threat from money laundering activity is explicitly covered. UK threat assessment 2006-2007 is available online at: http://www.soca.gov.uk/assessPublications/downloads/threat_assess_unclass_250706.pdf.

Terrorist financing

21. The UK has substantial experience in responding to terrorist threats and the support networks that make terrorist acts possible: for many years terrorism arising from the political situation in Northern Ireland constituted a significant threat to security in the UK. The principal current terrorist threat however is from extremists using a distorted and unrepresentative version of the Islamic faith to justify violence. This threat is genuinely international in nature. Attacks have been carried out by individuals from the UK and overseas. The domestic and international dimensions of the threat are therefore closely linked. The UK Government's assessment is that the threat from Islamist terrorism is serious and sustained, is potentially still increasing, and may not diminish to any significant extent for some years. The recent successful convictions of five men for plotting to make and deploy a fertiliser-based bomb is just one of numerous terrorist actions that UK authorities have averted since 2001.

22. The intelligence picture on the methods employed by terrorists to raise, move, store, and deploy funds is constantly evolving. The use of banks to move terrorist funds overseas is thought to have declined in response to the tightening of controls in that sector. Two areas of growing concern are: the abuse of charitable organisations to raise and distribute funds, and the abuse of the 'money service business' (MSB) sector (including alternative remittance services) to move funds. Both of these issues have been subject to formal review by the central government to identify where controls need to be tightened.

1.3 Overview of the financial sector and designated non-financial businesses and professions

a. Overview of the financial sector

23. All types of "financial institution" as defined in the FATF methodology are active in the UK, and all are covered by the current Money Laundering Regulations 2003 (MLRs 2003). The financial sector is of crucial importance to the UK economy, accounting for 6.8% of GDP in 2004, with professional service firms closely connected to the financial sector (accounting, legal and management consultancy) contributing a further 3-4%. It is also the largest contributor to the UK balance of payments.

24. Over 1.1 million people are employed in financial services. While London is core to the UK's international position (London has the largest share of many international financial markets) other cities such as Birmingham, Bristol, Edinburgh, Glasgow, Manchester, and Leeds are also important financial centres. The UK is home to some of Europe's largest markets including banking, insurance, and fund management. It is also home to the largest foreign exchange market and second largest securities market in the world. In 2004, net exports of UK financial services totalled a record £19bn, 9% up on the previous year. [5]

"Authorised" Firms

25. The UK is a major international centre for investment and private banking and has one of the largest commercial banking sectors in the world (in June 2005 lending to UK residents reached £1,552bn whilst the outstanding value of deposits from UK residents totalled £1,231bn). The UK insurance industry is the largest in Europe and third largest in the world. The London Market is the world's leading market for internationally traded insurance and reinsurance. Gross premiums on the London Market were conservatively estimated at £21.3bn in 2004. The UK is also a leading centre for securities dealing, with a substantial domestic market in equities complemented by London's major role as a centre for trading in international bonds and foreign equities. The UK is one of the largest fund management markets in the world. It has a strong international orientation and attracts significant overseas funds (it is estimated that the UK fund management industry was managing over £2,960bn of funds at the end of 2004). This includes international private wealth management, hedge funds, and private equity.

26. Most types of financial institution are authorised and supervised by the Financial Services Authority (FSA). Under the EU Money Laundering Directives, the host state has AML/CFT regulatory responsibility for branches of EEA passported institutions whereas the home state will be responsible for institutions providing cross-border services. The following types of financial institutions, broken down by business type, were regulated by the FSA as of 31 March 2006.

Financial Sector	FSA Authorised Financial Institutions	EEA Authorised Financial Institutions[6]	
		UK Branches (EEA)	UK (Cross-border) Services (EEA)
Personal Investment	5,005	0	1
Investment Management	1,632	3	0
Securities & Futures	967	6	2
Banking (including Building Societies & e-money issuers)	301	94	5
Insurance[7]	723	74	404
General Insurance	9,473	0	0
Mortgages[8]	3,588	0	1

[5] International Financial Services London, '*International Financial Markets in the UK*' (November 2005)

[6] The EEA-passported financial institutions are institutions which are authorised by another state within the European Economic Area and are permitted to conduct business in the UK by way of a 'passport'. These financial institutions are passported through the relevant EU Single Market Directives. Under EU law, UK branches are supervised by the host country supervisor (FSA). Those providing cross-border services are supervised by the home country; therefore, the FSA does not have any regulatory responsibilities for these 5,224 entities.

[7] "Insurance" covers Composite Insurer, Lloyd's Member Agent, Lloyd's Managing Agent, Life Insurer, Lloyd's and General Insurer.

Professional Firms[9]	652	0	0
Credit Unions	562	0	0
Other[10]	605	5	4
Category not supplied[11]	3	52	4,807
Total	23,511	234	5,224
Overall Total	**28,969**		

27. The main exceptions to FSA authorisation/supervision are money and value transmission agents, known in the UK as "Money Service Businesses" (MSBs) and lending and consumer credit provision. In the UK, three types of business are active that fall under the description of an MSB: (i) Money/value transmitters (MVTs) including Hawala and other alternative remittance providers; (ii) Bureaux de change (BdC); and (iii) Cheque Cashers (CC). All types of MSB are required to register with the UK's tax and customs authority, HM Revenue and Customs (HMRC), which monitors them for compliance with AML/CFT controls. The table below presents an overview of the registered MSB sector in the UK. The majority of MSB premises are used for all three types of MSB activity.

BUSINESS TYPE	REGISTERED PRINCIPALS	NUMBER OF PREMISES	PERCENTAGE PREMISES
Money transmission only	1515	9767	30.3%
Bureau de change only	852	4276	13.3%
Cheque casher only	546	1371	4.2%
Bureau de change and money transmission agent	244	407	1.2%
Cheque casher and money transmission agent	103	311	0.9%
Bureau de change and cheque casher	73	534	1.6%
Bureau de change, cheque casher, and money transmission agent	288	15,465	48.1%
TOTAL	**3621**	**32,131**	**100%**

28. There are also financial activities that come under the FATF definition that are not regulated by either the FSA or HMRC. The largest make up of this non-FSA authorised sector is lending and consumer credit. There are over 100,000 active consumer credit licences. Under the Consumer Credit Act 1974, recently updated by the Consumer Credit Act 2006, consumer credit firms need a licence from statutory regulator the Office of Fair Trading (OFT) before they can set up. Further, the non-regulated sector also includes leasing, some guarantees and commitments and safe keeping services. Legal obligations to comply with AML/CFT controls still apply to these sectors under the MLRs.

29. A large proportion of financial leasing is undertaken through banks, thus bringing it within the FSA's regulatory remit. The activity itself is not regulated, although 95% of non-bank firms are within the main representative trade association which is active in AML forums.

Impact of EU Third Money Laundering Directive

[8] "Mortgages" include Lenders, Advisers, Arrangers and Administrators.

[9] Professional firms are largely comprised of Solicitors and Accountants. They are entitled to practice a profession regulated by a Designated Professional Body and, in practicing it, are subject to its rules, whether or not they are a member of that body. However, they are also carrying out a FSMA-regulated activity which will require FSA authorisation.

[10] "Other" includes: Friendly Societies (173), Collective Investment Scheme (CIS) Trustees (10), CIS Administrators (23), Advising and arranging intermediaries (exc. FAs and Stockbrokers) (376), EEA Advising and arranging intermediaries (exc. FAs and Stockbrokers) (7) Media firms and Service Companies (7), Service firms (16), EEA Service Firms (1), EEA Secondary Appointed Rep (1).

[11] "Category not supplied" – The majority of the 5,458 EEA Authorised Financial Institutions are firms which have exercised their right to passport into the UK under the Insurance Mediation Directive (IMD). Under the IMD, financial institutions can passport into other Member States and notify the FSA accordingly. As such, the information the FSA require from these firms is limited.

30. Measures for implementation of the Third EU Money Laundering Directive in the UK are underway and will be complete by December 2007. This is expected to bring about a number of enhancements to the current AML/CFT system, including a new requirement for all parts of the regulated sector to have a clearly identified supervisor for AML/CFT compliance. Current proposals envisage that the FSA and HMRC will have an expanded supervisory remit and other relevant regulators such as the OFT will be required to cover AML/CFT compliance for the first time.

b. Overview of DNFBPs

31. All types of "designated non-financial businesses & professions" (DNFBPs) as defined in the FATF methodology are active in the UK and all are within the scope of the MLRs 2003.

Casinos

32. On 31 March 2006, there were 165 licensed casinos in Great Britain, operated by 26 parent companies. Of these, 140 were actually operating. These casinos were established under older legislation (The Gaming Act 1968). As of 29th April 2006, casinos can only be established under The Gambling Act 2005.

33. The table below demonstrates the concentration of casino ownership in the hands of a small amount of companies:

Company	**No. of licensed casinos**
Stanley Leisure Group Plc	**45** casinos (4 in London)
Rank Group Plc	**44** casinos (6 in London)
Gala Group	**32** casinos (5 in London)
London Clubs International Plc	**12** casinos (5 in London)
A & S Leisure Group	**6** casinos (1 in London)
Aspinall's	**3** casinos (1 in London)
Blue Chip Casinos Ltd	**3** casinos (none in London)
Clockfair Ltd	**2** casinos (none in London)
Remainder operated as single company / single casino businesses	**17** casinos (4 in London) **1** dedicated card club
	Total: 165*

*Only 140 are currently operating.

34. Currently, the establishment of an internet casino in the UK is illegal. However, when the Gambling Act will come into effect later in 2007, internet casinos will be allowed to be established in the UK. They will have to follow the same license application process as non-remote casinos.

35. The total drop (money exchanged for gaming chips) in casinos in Great Britain during the financial year 2005/06 was £4,231 million, an increase of £73 million on the 2004/05 figure. These figures exclude income from gaming machines, which, with greater numbers of machines being permitted, could in future represent a significant proportion of many casinos' profits.

Real Estate Agents

36. Property markets in the UK have been consistently buoyant for several years, fuelling the demand for the services that "Estate Agents" (as real estate agents in the UK are known) provide. Across the UK, there are approximately 10,000 firms. Estate agents are primarily regulated by the Estate Agents Act 1979. The Act is enforced by local Trading Standards Departments (TSDs) and the Office of Fair Trading (OFT). Estate agents do not have to obtain licences but the OFT has the power to consider whether an individual is unfit to continue to practice if they have breached certain criteria

and prohibit them from practicing as an estate agent. TSD's enforcement role is the investigation and prosecution of specific criminal offences under the Act. Breaches by estate agents of the non-criminal obligations of the Act and the supporting Orders and Regulations are primarily the concern of the OFT.

Dealers in precious metals & precious stones

37. All "High Value Dealers" (HVDs), including dealers in precious metals and dealers in precious stones, are covered under the current AML regulations. HVDs are legal entities that accept payment in cash of €15,000 or more for goods by way of business in a single transaction. HVDs are required by law to register with HMRC and pays a fee for each physical location through which it operates. HMRC monitors them for compliance with AML/CFT controls. There are just over 1,500 entities on the HMRC register. Many businesses in the UK that would otherwise be caught by the requirement to register have explicitly imposed a threshold on the cash transactions they will accept, thus reducing their attractiveness to money launderers as well as avoiding the registration requirement.

Lawyers: solicitors, advocates, and licensed conveyancers

38. The legal profession in the UK is, broadly speaking, divided into two branches, namely: solicitors and barristers ("advocates" in Scotland). In general, solicitors deal directly with the client and provide legal advice, whereas barristers / advocates mainly provide advocacy and representation services through the court system on behalf of their clients.

39. There are 126,142 solicitors on the Roll of Solicitors for England and Wales, and of those, 100,938 hold practicing certificates. There are approximately 9,081 private practice firms. The majority of firms in England and Wales are sole practitioners. There are 1,976 solicitors with practising certificates in Northern Ireland, the majority of which are in private practice. Much like England and Wales, there are a majority of firms with 1 or 2 principals. In Scotland, there are 9,637 practising solicitors. Of these, 3,592 (37%) are principals in private practice firms (percentage breakdown of firms by number of partners not available).

40. Barristers / advocates in independent practice operate as a referral or consulting profession and are required to obtain their instructions either from solicitors, or less often from particular clients – such as accountancy firms - which have been licensed by their professional body to provide instructions directly. There are about 14,000 barristers practising in England and Wales, most of them are self-employed. There are 585 barristers in independent practice in Northern Ireland. In Scotland there are about 460 advocates. A barrister or advocate in independent practice provides contentious and non-contentious (advisory) services. Most of an independent barrister's work is contentious work and involves the barrister representing a client in Court (and sometimes in arbitrations or mediations) in relation to a particular case.

41. Licensed conveyancers are in effect specialist property lawyers and can handle funds for their clients. Many licensed conveyancers are employed by solicitors' firms and fall within that regulatory regime; however, there are approximately 230 firms or individuals which operate separately from solicitors and are directly regulated by the CLC, carrying out about 5% of the conveyancing work. Across the profession, the total value of property transactions handled during 2005 was estimated at about £39bn.

Notaries

42. There are about 1,000 "Notaries Public" practicing in England and Wales. Most notaries are also solicitors and do their general legal work in that capacity and under the regulation of the Law Society. In Scotland, *all* notaries are regulated by the Law Society of Scotland. A few in England and Wales (the "Notaries Society" estimates about 70 in total) are not solicitors; these practice only as notaries.

43. Many notaries work for commercial firms engaged in international trade, and for private individuals. The most common tasks are: preparing and witnessing powers of attorney for use overseas; dealing with purchase or sale of land and property abroad; providing documents to deal with the administration of the estate of people who are abroad; authenticating personal documents and information for immigration or emigration purposes, or to apply to marry or to work abroad; authenticating company and business documents and transactions. Notaries can also carry out commercial and property work as well as family and private client work.

44. The rules for notaries are similar to those of solicitors. They must keep clients' money separately from their own and comply with stringent practice rules and rules relating to conduct and discipline. Notaries that are not currently solicitors or accountants are not currently supervised for compliance in England and Wales.

Auditors & Accountants

45. Statutory regulation of the accountancy profession in the UK is limited to three areas: statutory audit, investment business, and insolvency. Of these, only the audit profession is limited to accountants, and statutory audit is restricted to firms or persons registered with officially recognised supervisory bodies (RSBs). Under section 384 of the Companies Act 1985, most companies are required to appoint an auditor.

46. The term "accountant" is used very widely for a whole range of activities such as bookkeeping and other financial services, as well as quite different activities. It is not defined or regulated by law, nor is it necessary to have any formal qualification or to be a member of a professional body to call oneself an "accountant"; therefore, there is a large number of accountants who are not members of any professional body or registered anywhere, so that the total number of practitioners cannot be determined precisely. Some parts of the accountancy profession are self-regulatory. The use of titles owned by individual professional accountancy bodies, such as "Chartered Accountant", "Chartered Certified Accountant" and "Chartered Management Accountant", is restricted to qualified members of a particular body who are also monitored and regulated by that body, according to its specific rules and standards.

Trust & Company Service Providers

47. The business of providing trust and company services (formation, nominee directors, nominee shareholders, professional trusteeships, business addresses, etc) is a diverse and large sector. It includes all legal professionals and accountants who provide such services, all company formation agents, all trust service providers who are not legal professionals, all business address / business service providers, and all professional interim managers. Excluding those service providers who are members of a professional body, it is estimated there are around 5,000 firms and individuals in operation. The size of the market is hard to gauge: trusts and companies are easy to set up and are a ubiquitous mechanism for accomplishing a range of legitimate commercial or private objectives.

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

48. Trusts are a long-standing, popular, and integral part of the legal and economic landscape of the UK. A trust does not count as a legal person or a contract, nor can it own property. However, trusts allow individuals to dispose of their assets according to their particular objectives and for a range of other legitimate and economically important activities. Types of trust encountered in the UK include: "bare", "fixed", "discretionary", "hybrid", "private" and "public / charitable" trusts. The law also allows for "implied", "resulting", and "constructive" trusts to exist in certain circumstances, where there was no clear intention of creating a trust (i.e. an "express" trust). A trust can arise in a wide

range of circumstances, and for a wide range of reasons, including where: money is held by trustees in an occupational pension scheme for the benefit of employees; trustees hold investments in a unit trust and the unit holders are the equitable owners of those investments; property is held for the benefit of people lacking full capacity such as children and incapable adults; assets are held by an unincorporated club or society on behalf of its members; or the trustees of a charity administer the assets of the charity for the purposes for which the charity was established.

49. The UK has a large number of legal forms available for doing business. A distinction can be drawn between those businesses that are bodies corporate and those that are not. A body corporate or "incorporated" business has a legal personality, which is separate from that of the individuals who own, manage or staff its activities. Most business activity in the UK (at least measuring by volume) is carried on by bodies corporate.

50. *Companies Act companies:* Companies account for the largest proportion of any of the forms, which an incorporated business can take in the UK, and the vast majority of companies (currently approximately 2 million) are formed under the Companies Acts. In most respects, the same principles of company law apply to Companies Act companies and those which are not formed under the Companies Acts. Companies formed under the Companies Acts take one of four basic forms: private company limited by shares - members' liability is limited to the amount unpaid on shares they hold and the company may not offer shares or debentures to the public; private company limited by guarantee - members' liability is limited to the amount they have agreed to contribute to the company's assets if it is wound up; private unlimited company - there is no limit to the members' liability and the company may or may not have a share capital; public limited company - the company's shares may be offered to the public and members' liability is limited to the amount unpaid on shares held by them.

51. *Other types of company:* Before the Companies Acts (the first of which were passed in the mid-19th century), companies could only be established by royal charter / letters patent or under company-specific Acts of Parliament. These methods are hardly ever used today, and the number of companies established in such ways in the past and still in existence now is relatively small (and, for various reasons, diminishing). Of those that do still exist, a significant proportion are formed for charitable or quasi-charitable purposes, e.g. learned, professional and artistic societies, schools and universities.

52. *Partnerships:* The term "partnership" is used to cover three distinct business forms in the UK. The traditional form of partnership is defined by the Partnership Act 1890 as "the relation which subsists between persons carrying on a business in common with a view to a profit", other than companies. Many small businesses exist in this form, as do some quite large professional services firms. A more specialised form is the "limited partnership", in which one or more "general partners" are liable for all the debts and obligations of the firm, whilst one or more "limited partners" contribute capital or property to the firm but are not liable for its debts and obligations beyond the amount they have contributed (see the Limited Partnerships Act 1907). Finally, under the Limited Liability Partnerships (LLPs) Act 2000, it is possible to form entities in which all the partners' liability is limited. In England, Wales and Northern Ireland, "traditional" and "limited" partnerships do not have a legal personality separate from that of their members. Under Scots law, they do.

53. *Societies:* A *friendly society* is a voluntary mutual organisation whose main purpose is to assist members (usually financially) during sickness, unemployment or retirement and to provide life assurance. An *industrial and provident society* is an organisation conducting an industry, business or trade either as a co-operative or for the benefit of the community. *Co-operative societies* are run for the mutual benefit of their members with any surplus usually being ploughed back into the organisation to provide better services and facilities. Societies run for the benefit of the community provide services for the people other than their members. There must be special reasons why the society should not be registered as a company. Societies are owned by their members; however, in the case of societies for the benefit of the community the members have no beneficial interest. The governance provisions of both types of society usually provide for each member to have one vote regardless of the size of their investment or borrowing or indeed the number of share accounts.

54. *Building societies* are financial institutions that offer savings accounts and mortgages as their main business. In recent years a number of building societies have diversified and now offer a wide range of personal financial services. Some of these services include current accounts, credit cards cash machines, travel money, unsecured loans, various types of insurance and estate agency services. Building societies are mutual institutions; most people who have a savings account, or mortgage are members and have certain rights to vote and receive information as well as to attend and speak at meetings. Each building society has a board of directors.

55. Under the law of the European Union, it is possible to create certain kinds transnational corporate entity known as the "*Societas Europea*" ("SE"), the "*European Economic Interest Grouping*" ("EEIG"), *Open-Ended Investment Company* ("OEIC"), and *Societas Cooperativa Europa* (SCE). As required by EU law, there is UK legislation dealing with aspects of these forms at the national level. The SE and EEIG forms in particular have so far been very little used in practice.

1.5 Overview of strategy to prevent money laundering and terrorist financing

a. AML/CFT strategies & priorities

56. The UK is committed to identifying and interdicting the flow of illicit funds across and within its borders; and to the disruption and dismantling of the money laundering and terrorist finance networks that move such funds. This is made clear in the Government's Anti Money Laundering Strategy, published in October 2004.

57. The Government's policies for AML/CFT are underpinned by three key objectives: to *deter***,** through the establishment of enforceable safeguards and supervision; to *detect,* using the financial intelligence generated by money laundering controls to identify and target criminals and terrorist financiers; and to *disrupt*, maximising the use of available penalties such as prosecutions or asset seizures.

58. Current priorities are: the domestic implementation of the Third EU Money Laundering Directive, and the adoption of appropriate domestic controls derived from the payments regulation and the mandatory declaration of currency regulation; reform of the "suspicious activity reporting" framework further to a comprehensive analysis of its current effectiveness (the "SARs Review", a.k.a. the "Lander Review"); development of an enhanced regulatory environment for money service businesses based on a domestic assessment of the significance of MSBs in facilitating money laundering and terrorist finance; an assessment of the extent to which current controls for charitable organisations are fit for purpose in respect of terrorist financing (further to the development of the Interpretative Note for FATF SR.VIII); the European Commission's 2005 "Communication" on this topic, and domestic intelligence assessments; and measures to further restrict couriering cash through the implementation of a new set of European controls.

59. The UK's annual "Threat Assessment" on serious and organised crime includes a section on money laundering that recounts the effectiveness of the UK's controls in meeting the threat and identifies areas for improvement. Law enforcement and the wider AML/CFT community contribute to the development of these Threat Assessments. The development of new policy on AML/CFT takes account of the findings of the Threat Assessments.

60. At the time of the on-site visit, a joint Treasury – Home Office – SOCA exercise was underway to map and define UK strategy on money laundering and terrorist financing for the future. This new AML/CFT strategy was published on 28 February 2007.

61. Preparations to implement the Third Money Laundering Directive will continue to be a significant source of AML/CFT policy work over the next 18 months. New "Money Laundering

Regulations" are in development; a first draft was issued for public comment in January 2007 and are available at: http://www.hm-treasury.gov.uk/consultations_and_legislation/money_laundering directive/consult_thirdmoney_2007.cfm.

b. The institutional framework for combating money laundering and terrorist financing

(i) Ministries and co-ordinating committees

62. **Her Majesty's Treasury (HM Treasury or HMT)** is responsible for all policy on the regulation of the UK's financial services sector, which includes joint overall co-ordination of UK AML/CFT policy with the Home Office. The Treasury has a dedicated Financial Crime Team whose responsibilities include: negotiation and domestic implementation of EU Money Laundering Directives and related European legislation; domestic implementation of international financial sanctions obligations imposed at both UN and EU level, and the application of unilateral financial sanctions and asset freezes; leading the UK delegation to the FATF & representing the UK at other international fora or conferences concerning AML/CFT; and approval of industry guidance on compliance with money laundering and terrorist financing controls.

63. The **Home Office**[12] serves as both the ministry of justice and the ministry of the interior for England and Wales. It is responsible for the funding and oversight of the 43 police forces in England and Wales, and the Serious Organised Crime Agency (SOCA). It is also responsible for national security across the UK. The Home Office has a Specialist Crime Directorate and a Terrorism Policy Unit to cover these responsibilities: all UK primary legislation concerning money laundering and terrorist financing; overall police strategy and targets for money laundering and terrorist financing investigations and prosecutions; overall strategy and targets for asset seizure and confiscation in England & Wales; leading on domestic counter-terrorism policy; coordinating mutual legal assistance treaties and requests; implementing EU Framework Decisions and Conventions on money laundering and other criminal issues. While the Northern Ireland Executive remains suspended, the equivalent justice and interior functions for that region are fulfilled by the Northern Ireland Office. In Scotland, the relevant Home Office functions listed here are fulfilled by the **Justice Department of the Scottish Executive**.

64. The **Foreign and Commonwealth Office (FCO)** is the UK's ministry of foreign affairs. It has little direct responsibility for the domestic AML/CFT framework; however, it does have lead responsibility for UK entry into international agreements, such as ratification of UN treaties, and negotiation of UN Security Council Resolutions.

65. The **Department for Trade and Industry (DTI)** is the ministry responsible for trade, business, employees, consumers, science and energy. As such, it is responsible for the law relating to legal persons and is responsible for two relevant executive agencies: (1) the Companies House – which incorporates and dissolves companies in the UK on behalf of the registrar of companies, and stores information that companies are obliged to provide under the Companies Act 1985; and (2) Companies Investigation Branch, which investigates companies for adherence to company law.

66. The **Money Laundering Advisory Committee (MLAC)** is jointly chaired by Home Office and HMT and is a forum for key public and private stakeholders to co-ordinate the UK's AML regime and review its efficiency and effectiveness. Most financial services sector trade associations are represented.

67. The **Terrorist Finance Action Group (TFAG)** is an inter-governmental committee that forms part of the wider government framework on counter-terrorism. It is focused on the development of

[12] Note: in May 2007 the functions of the Home Office were split, resulting in the creation of a new Ministry of Justice

policy to combat terrorist financing, and brings together representatives from central government, regulators, intelligence, and law enforcement.

(ii) Criminal justice and operational agencies

68. **Serious Organised Crime Agency (SOCA)** became operational on 1 April 2006. The functions of the National Crime Squad and the National Criminal Intelligence Service (NCIS) were transferred to SOCA and those agencies have been abolished. SOCA also absorbed the investigative functions of HM Revenue and Customs (HMRC) in relation to drug trafficking and related criminal finance, and a small part of the Immigration Service. The **UK FIU** is located within SOCA.

69. **Police:** There are 43 regional police forces in England and Wales funded by and subject to Home Office oversight, 8 in Scotland funded by and subject to Scottish Executive oversight, and 1 in Northern Ireland funded by the Northern Ireland Office and answerable to the Northern Ireland Policing Board. In Scotland there is also a dedicated Scottish Crime and Drug Enforcement Agency "SCDEA" which tackles money laundering as part of its remit. Of the 43 forces in England & Wales the majority have specialist financial crime investigation units, accounting for approximately 2,700 trained financial investigators.

70. There are also 5 **Regional Asset Recovery Teams** in England and Wales. Funded through the Recovered Assets Incentivisation Fund (RAIF), these multi-agency teams provide financial investigation expertise for money laundering, cash seizure and confiscation in support of criminal prosecution and provide assistance to law enforcement agencies within their region (London, North East, North West, West Midlands and Wales).

71. **National Terrorist Finance Investigation Unit (NTFIU)** is the lead authority for the investigation of terrorist financing in the UK, although individual forces also undertake such investigations when relevant or appropriate. NTFIU relies on CPS, PPSNI, or COPFS to take forward prosecutions.

72. The **Assets Recovery Agency (ARA)** was set up under the Proceeds of Crime Act 2002. In addition to criminal confiscation (i.e. working with law enforcement agencies to assist them with confiscation proceedings), it has the unique power to pursue asset recovery from criminals by civil means as well as specific taxation. All financial investigators operating in the UK must be accredited by ARA in order to utilise powers available under POCA (in Scotland, financial investigators can be trained by the Scottish Police College rather than ARA). The ARA also currently manages and administers the Joint Asset Recovery Database (JARD), a central repository of information covering all aspects of asset recovery. In respect of civil recovery in Scotland, the **Civil Recovery Unit (CRU)** has a separate remit from that of ARA. Since the on-site visit, the UK government has announced its intention to merge ARA with SOCA.

73. The **Serious Fraud Office (SFO)** is an independent government department that investigates and prosecutes serious or complex fraud, headed by a Director who is appointed by and accountable to the Attorney General. The SFO's jurisdiction covers England, Wales, and Northern Ireland but not Scotland. The SFO has a limited role in the investigation of money laundering except where the laundering has formed part of a larger more complex financial crime.

74. The **Crown Prosecution Service (CPS)** is the principal independent prosecuting authority in England and Wales and is responsible for prosecuting criminal cases investigated by the police and SOCA. It advises the police and SOCA on cases for possible prosecution and reviewing cases received; determines the charge in all but minor cases; prepares cases court; and applies for restraint, receivership and confiscation orders in respect of CPS prosecutions. The CPS is headed by the Director of Public Prosecutions who is superintended by the Attorney General.

75. The **Public Prosecution Service Northern Ireland (PPSNI)** is the Government Department responsible for prosecuting criminal cases investigated by the police, HMRC, and SOCA in Northern Ireland. It is headed by the Director of Public Prosecutions Northern Ireland who is accountable to the Attorney General Northern Ireland.

76. The **Scottish Crown Office and Procurator Fiscal Service (COPFS)** prosecutes all crime in Scotland. One of its current key objectives is the recovery of assets of those involved in criminal activities. COPFS is headed by the Crown Agent who is accountable to the Lord Advocate, the principal law officer of the Crown in Scotland.

77. **Her Majesty's Revenue and Customs (HMRC)** is primarily responsible for the collection of taxes, and the enforcement of import / export controls. HMRC's jurisdiction is UK-wide. It has two key functions relating to AML: (1) *Investigative:* including the investigation of tax matters, smuggling and money laundering activities (not including drugs, currently the responsibility of SOCA); and enforcement relating to the seizure and confiscation of cash at ports and other frontiers; and (2) *Regulatory:* HMRC registers money service businesses and high value dealers, and has enforcement powers in relation to these two sectors. As of June 2007, HMRC will also be responsible for enforcing the provisions of EU Council Regulation No 1889/2005 ("the Cash Controls Regulation").

78. The **Revenue and Customs Prosecution Office (RCPO)** is an independent government department responsible for prosecuting all HMRC criminal cases and SOCA investigations of drug trafficking and related money laundering in England and Wales. It is headed by the Director of Revenue of Customs Prosecutions who is accountable to the Attorney General. RCPO defers to the Crown Office for prosecutions in Scotland and the PPSNI in Northern Ireland.

(iii) Financial sector bodies—government

79. **The Bank of England (BoE)** is the central bank of the United Kingdom. Its two key functions are the promotion and maintenance of monetary stability and financial stability. The BoE acts as the agent of HMT in the day-to-day administration of financial sanctions (asset freezing etc). In this regard, the BoE produces and maintains an up to date list of financial sanctions targets, notifies the financial services sector of changes to the list, and issues licences for humanitarian exemptions to financial sanctions where appropriate.

80. The **Financial Services Authority (FSA)** is an independent non-governmental body, given statutory powers by the Financial Services and Markets Act (FSMA) 2000, and is a company limited by guarantee. HMT appoints the FSA Board for fixed terms. The Board consists of a Chairman, a Chief Executive Officer, three Managing Directors, and 9 non-executive directors. The FSA is accountable to Treasury Ministers, and through them to Parliament for its performance. It is operationally independent of Government and sets its own budget which is funded entirely by the firms it regulates. The FSA is the main statutory regulator (as well as AML/CFT regulator) for the financial services industry in the UK and regulates nearly 29,000 firms and approximately 165,000 individuals within these firms. The FSA authorises and regulates most financial services markets, exchanges and firms. It has a wide range of rule-making, investigatory, and enforcement powers. One of its four statutory objectives is the reduction of financial crime, including fraud or dishonesty, market misconduct and money laundering.

81. The **Office of Fair Trading (OFT)** is responsible for making markets work well and as part of this general function, is the statutory regulator of consumer credit providers; this includes licensing such providers, and enforcing the obligations contingent on such a licence.

82. **Exchanges:** A list of "Recognised Investment Exchanges" (RIEs) can be found at: (http://www.fsa.gov.uk/register/exchanges.do). RIEs are required to comply with the high-level requirements set out in The Financial Services and Markets Act 2000 (Recognition Requirements for

Investment Exchanges and Clearing Houses) Regulations 2001. These requirements set out high-level principles in relation to, *inter alia*, governance, systems and controls, financial resources, and financial crime and market and abuse; they are designed to ensure that RIEs regulate their markets to appropriate standards. RIEs act as "front-line regulators" of their markets to the extent that they are responsible for monitoring their markets for compliance with their own rules and for referring potential suspicious behaviour and transactions to the FSA. RIEs are required to report potential cases of market abuse or criminal offences to the FSA.

(iv) Financial sector bodies & associations

83. The **Joint Money Laundering Steering Group** (JMLSG) is a private corporation on which the majority of financial service provider trade associations are represented. This body concerns itself with the development of industry guidance for meeting legal and regulatory obligations and on developing best practice with respect to AML/CFT. The guidance prepared by JMLSG has been formally approved by HMT in accordance with relevant provisions in AML legislation.

84. **British Bankers Association** (BBA) is the principal trade association for banks operating in the UK. It is a leading representative body in the financial services sector and has 218 members, as well as many associate members, which fund its not-for-profit activities. Eighty-five per cent of its members are involved in providing wholesale banking services, and 75% of the membership is of non-UK origin, representing 60 different countries. BBA members hold 90% of the UK banking sector's assets and represent 95% of all banking employment in the UK.

85. **Building Societies Association (BSA)** is the trade association for the UK's building societies. There are 61 building societies in the UK with total assets of over £275 billion. About 15 million adults have building society saving accounts and over two and a half million adults are currently buying their own homes with the help of building society loans. Every building society in the UK is a member of the BSA.

86. **Finance and Leasing Association (FLA)** is the principal representative of the asset, consumer and motor finance sector in the UK. FLA members comprise banks, subsidiaries of banks and building societies, the finance arms of leading retailers and manufacturing companies, and a range of independent firms.

87. **Association of British Insurers (ABI)** represents the collective interests of the UK's insurance industry. The Association speaks out on issues of common interest to the sector, helps to inform and participate in debates on public policy issues, and also acts as an advocate of high standards of customer service in the insurance industry. The Association has around 400 companies in membership, representing 94% of domestic insurance services sold in the UK.

88. **Investment Management Association (IMA)** is the trade body for the UK's £2800 billion asset management industry. The money their members manage is in a wide variety of investment vehicles including authorised investment funds, pension funds and stocks and shares ISAs. IMA's key aims are to bring about improvements in the legal, regulatory and fiscal environment in which its members operate, and to maintain and enhance the reputation and standing of the industry.

(v) DNFBP and other matters

89. The **Gambling Commission** is a Non-Departmental Public Body set up under the Gambling Act 2005. From September 2007 it will regulate all commercial gaming in the UK; at present it regulates all casinos, bingo, gaming machines and lotteries. From 2007, it will have responsibility for the regulation of betting and remote gambling.

90. **British Casino Association (BCA)** is a trade association that represents over 90% of the casino industry in the UK. The BCA has close links with a number of government departments, such as the

Gambling Commission and the Department for Culture, Media and Sport and negotiates with them on matters of interest to the industry. The BCA takes a lead in keeping its members up-to-date with all the latest industry news, including changes to legislation, rules and regulation.

91. The **Casino Operators Association** was established in 2001 to represent the smaller casinos in the UK; their needs being somewhat different from those of the larger chain casinos represented largely by the BCA. The Association provides information on legislative changes and regulatory advancements via its website and has close links with the Gambling Commission, the statutory regulator for the gambling industry.

92. The **Royal Institute of Chartered Surveyors (RICS)** is an industry body for real estate agents and other professionals involved in land, property, construction, and environmental issues. RICS produces guidance and news bulletins on AML/CFT legislation and developments for its members on its website and has worked with the **National Association of Estate Agents (NAEA)**, a trade body, to produce "*protecting against money laundering: a guide for members*". The guidance produced by RICS includes sector-specific guidance on customer due diligence, including guidance on CDD in relation to different sectors such as companies, trusts, and charities.

93. The **Law Society England and Wales (LSEW)** is a self-regulatory organisation (SRO) that was the representative body and AML supervisory authority for solicitors in England and Wales at the time of the on-site visit. It has maintained a formal separation between its representative and regulatory functions since January 2006. In January 2007, the Solicitors Regulatory Authority (SRA) was established to provide a new identity for the regulatory functions. .The LSEW had a range of sanctions in place for material breaches of the professional conduct rules which have now passed to the SRA. The LSEW issued Money Laundering Guidance to provide a practical interpretation of the ML Regulations 2003, the Proceeds of Crime Act 2002 and the Terrorism Act 2000. The Guidance is not at present approved by HMT, so the courts are not yet required to take it into account, but may do so when assessing the behaviour of a solicitor.

94. The **Law Society Northern Ireland (LSNI)** is a Committee-based organisation answering to an elected Council of 30 members. It has statutory powers to discipline, educate, and control the solicitors' profession in Northern Ireland, as set out in the Solicitors (NI) Order 1976. The LSNI utilises the AML guidance (as well as other guidance) produced by the LSEW.

95. **Law Society Scotland (LSS)** is the professional body and SRO for all solicitors in Scotland, and has a similar status and range of powers to the other Law Societies, including the ability to apply administrative sanctions. Solicitors in Scotland are required to adhere to the MLRs as an explicit part of their professional conduct rules – a breach of these rules may result in a referral to the Scottish Solicitors Discipline Tribunal which is independent of the Society and has the power to revoke a solicitor's practice certificate.

96. **Bar Council England and Wales (BCEW)** and the **Bar Council Northern Ireland (BCNI)** are the SROs for barristers in England and Wales, and Northern Ireland, respectively. Barristers are subject to the each Council's Code of Conduct. Failure to comply with the provisions of the MLRs, POCA, or TACT in respect of the relevant AML/CFT controls would be considered by the BCEW and BCNI to be professional misconduct. Disciplinary sanctions available include the imposition of a fine and the withdrawal of the barrister's practice certificate.

97. **Faculty of Advocates (Scotland)** is the SRO for advocates in Scotland, who are subject to the Faculty's Code of Conduct. Failure to comply with the provisions of the MLRs, POCA, or TACT in respect of the relevant AML/CFT controls would likely to amount to professional misconduct for Advocates in Scotland.

98. The **Council for Licensed Conveyancers (CLC)** is the statutory regulator for licensed conveyancers in England and Wales. The CLC produces both prescriptive guidance and an

interpretative "toolkit". The CLC's "Discipline and Appeals Committee" has statutory sanctions that include the power to levy fines on licensed conveyancers and the power to withdraw licences to operate; these sanctions can be applied in circumstances where the conveyancer has failed to abide by AML/CFT controls.

99. The major accountancy professional bodies in the UK and Ireland joined together in 1974 to form the **Consultative Committee of Accountancy Bodies (CCAB)**. CCAB is now a limited company with six members: The Institute of Chartered Accountants in England and Wales (ICAEW); the Institute of Chartered Accountants of Scotland (ICAS); the Institute of Chartered Accountants in Ireland (ICAI); The Association of Chartered Certified Accountants (ACCA); the Chartered Institute of Management Accountants (CIMA); and the Chartered Institute of Public Finance and Accountancy (CIPFA). CCAB has also issued non-binding AML/CFT guidance; individual CCAB member bodies monitor their members for AML/CFT compliance against this guidance and any additional guidance or requirements they have imposed.

100. **The Society of Trust and Estate Practitioners (STEP)** is a professional body which provides education, training, representation and networking for its members, who are professionals specialising in trusts and estates, executorship, administration and related taxes. Members advise clients on the broad business of the management of personal finance. STEP also provides guidance on AML/CFT legislation and developments for its members and is active in encouraging compliance amongst its members.

101. The **Association of Company Registration Agents (ACRA)** is a professional body which provides guidance and support to practitioners in the field of company registration.

102. The **National Association of Goldsmiths** was established in 1894 to support the Jewellery Industry of Great Britain and Ireland. The Association promotes high professional and ethical standards among its membership to inspire consumer confidence and to enhance the reputation of its members. There is a Code of Practice to which elected Members must agree to adhere to and by which applicants for membership are judged.

103. **Companies House:** All limited companies in the UK are registered at Companies House, an Executive Agency of the Department of Trade and Industry. The main functions of Companies House are to: incorporate and dissolve limited companies; examine and store company information delivered under the Companies Act and related legislation; and make this information available to the public.

104. The **Charity Commission for England & Wales** is a non-Ministerial government department responsible for the registration and regulation of charities in England and Wales. Its governing body is appointed by but independent from Ministers. It is accountable to Parliament for its efficiency and to the High Court for the decisions made by the Commission in exercising its legal powers. It has a range of civil and administrative powers that are used in a remedial way to correct abuse within the charitable sector, including abuse arising from money laundering or terrorist financing.

105. The **Office of the Scottish Charities Regulator (OSCR)** is the independent registrar and regulator for Scottish Charities. It is a non-Ministerial government department and part of the Scottish Administration. Its governing body is appointed by and answerable to Scottish Ministers. It has a range of civil and administrative powers that are used in a remedial way to correct abuse within the charitable sector, including abuse arising from money laundering or terrorist financing.

c. Approach concerning Risk

106. The "risk-based approach" forms an integral part of the UK's AML/CFT regime. The Government's Anti-Money Laundering Strategy of October 2004 sets out the Government's commitment to "ensuring risk-based controls and setting flexible high-level principles rather than prescriptive, detailed requirements." According to the UK authorities, high-level legislation allows

firms flexibility in implementation, so that they are able to put in place risk-based and proportionate controls. Also, the 2003 and 2006 editions of the JMLSG Guidance, the revised FSA's money laundering Rules in 2006; the FSA's Financial Crime Strategy which was agreed in May 2006 and much of the guidance produced by and for the DNFBP sector build on this principle.

107. The FSA's approach has, since its inception, been based on a clear statement of the aims and limits of regulation, taking into account both necessity (the FSA has finite resources for regulating over 29,000 firms) and a conscious decision, taken in the interest of efficiency. The FSA's risk-based approach to AML/CFT consists of four key strands:

- **Risk-sensitive regulatory policy:** The FSA makes decisions about the allocation of resources on the basis of risk, applying greater resources to areas that it considers carry greater risk and to those which will have the greatest impact. As a consequence, the nature and extent of the FSA's supervisory relationship with an individual financial institution depends on how much risk the FSA considers it could pose to its regulatory objectives (which include the reduction of financial crime). In supervising firms, the FSA calculates risk based on "impact" and probability of an event taking place at that firm using its own risk model (ARROW). The initial "impact assessment" is determined by the size of the firm; however, the results can be adjusted based on a number of specific concerns, and any intelligence that may suggest the firm be "upgraded" to a more closely supervised entity.
- **Risk-sensitive regulatory practice:** The FSA places great emphasis on its aim of sensitive and well-informed supervision, which focuses on outputs and recognises that firms have options for managing their money laundering risks.
- **High-level rules:** In 2006, the FSA replaced its detailed and prescriptive money laundering rules with high-level requirements relating to firms' AML systems and controls and risk management. It also re-emphasised the importance of senior management responsibility.
- **Publicising the FSA's expectations**: the FSA uses its public pronouncements (e.g. speeches and publications) to make clear its commitment to firms having high AML standards based on a risk-based approach, and to encourage firms to act in a more risk-based way.

108. Firms use risk-based practices to manage their businesses across a number of areas including AML/CFT. Firms will have to demonstrate the appropriateness of their policies and procedures in view of their money laundering and terrorist financing risks to their supervisors.

109. The JMLSG Guidance, which advocates and promotes the risk-based approach, is formally approved by HMT and is explicitly referred to in the FSA's Handbook. Chapter 4 of the 2006 JMLSG Guidance sets out in detail what the risk-based approach entails, and describes the steps needed to identify the most effective and proportionate way to manage and mitigate a firm's ML and TF risks in line with their legal and regulatory obligations:

- **Risk identification and assessment** – identifying the money laundering and terrorist financing (as well as associated legal, regulatory and reputation) risks facing the firm given its customers, products and services, delivery channels and geographical profile. Assessing the potential scale of those risks and of the possible impact if they occur;
- **Risk mitigation** – identifying and applying measures effectively to mitigate the material risks emerging from the assessment;
- **Risk monitoring** – putting in place management information systems and keeping up to date with changes to the risk profile through changes to the business or to the threats;
- **Documentation** – having policies and procedures that cover the above and deliver effective accountability from the board and senior management down.

d. Progress since the last mutual evaluation or assessment

110. The UK was last subject to an FATF mutual evaluation in 1996. The recommendations identified for the UK's systems were as follows, with progress indicated since that time.

111. ***Improvements to confiscation / forfeiture legislation:*** The Proceeds of Crime Act 2002 (POCA), the Terrorism Act 2000 (TACT) and the Anti-terrorism Crime and Security Act 2001 (ATCS) have all improved confiscation and forfeiture legislation, providing a range of powers for the seizure, restraint, confiscation, and civil recovery of property connected with criminal conduct or terrorism.

112. ***Extension of cross-border cash seizure to all serious crime and financial instruments other than cash:*** POCA has updated cash seizure powers to meet this requirement

113. ***Improved performance in recovery of assets against confiscation orders:*** Specialist government agency "The Assets Recovery Agency" has, in the financial year 2005/2006, achieved recovery of £4.1M assets against £4.6M of recovery orders (annual report 2005/2006). Between 2001/2002 and 2005/2006, annual funds recovered grew considerably—from £25.2M to £96.8M.

114. ***FIU improvements: more efficient processing of reports; more consistent, relevant feedback to stakeholders; and greater level of strategic analysis and intelligence.*** The KPMG Review 2003 noted that the backlog of SARs received by the UK FIU in paper form but awaiting entry to the SAR database was some 54,000. The average time taken to disseminate a SAR was about 10 months. By 31st March 2006 the FIU had removed the backlog and introduced efficiency changes and had reduced the dissemination time for all SARs down to a maximum of 7 days.

115. Following the KPMG Review 2003, the FIU set up a Liaison Team in order to establish a systematic dialogue between the FIU and reporters and law enforcement agencies. Consultation during the Jill Dando Institute of Crime Science Review of SARs activity (2005) and the SARs Review (2006) noted significantly increased satisfaction by the reporting sectors in the contact with the FIU; SOCA has made further improvements to consistent, relevant feedback, for example by establishing a private sector group with high level government security clearance to discuss emerging threats.

116. ***Increased resources for FIU (manpower & IT):*** In NCIS (the location of the FIU up to 31 March 2006) the UK FIU had 80 directly employed staff plus some external contractors and attachments from other agencies. The staff costs for the financial year 2005-06 were £3.2 million plus £0.5 million in running costs. UK FIU within SOCA now has 97 staff and plans to increase this to 200 directly employed staff plus external contractors during 2007 at a cost of about £7 million. Funding on development of the SAR database in 2005-06 was approximately £1 million; in 2006-07 SOCA has resolved to spend about £4 million with a further £2.5 million in 2007-08.

117. ***Extension of AML obligations to all business conducted by a lawyer****:* The Money Laundering Regulations 2003 extended AML/CFT obligations to cover legal services which involve participating in any of the activities listed in FATF Recommendations 12 and 16 (e.g. company formation, handling client money).

118. ***Some form of supervision of MSBs (particularly bureaux de change):*** MSBs have been subject to supervision by the UK's customs agency (HM Revenue and Customs, formerly Customs & Excise) since 2001. The regulatory and supervisory environment for MSBs has recently been formally reviewed by the Government and proposals for further enhancement are being consulted upon.

119. ***Faster turn around times for mutual legal assistance requests submitted to the UK Central Authority (UKCA):*** MLA Guidelines have been introduced which specifically include a code of practice which sets time limits for the processing of requests by the UKCA. In 2006, independent management consultants reviewed the systems and procedures used by the UKCA in processing

requests. As a result of this review changes have been made to increase its efficiency effective from 1st August 2006.

2. Legal System and Related Institutional Measures

Laws and Regulations

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

2.1.1 Description and Analysis

The Proceeds of Crime Act 2002

120. The current legislation that criminalises money laundering is the Proceeds of Crime Act (POCA) 2002 (sections 327-340). POCA updated, expanded, and reformed the criminal law in the United Kingdom with regard to money laundering. The relevant Part 7 provisions, which came into force on 24 February 2003, set out the three principal money laundering offences:

- Concealing etc. criminal property (Section 327 POCA): the act of concealing, disguising, converting or transferring criminal property, or removing criminal property from the UK;
- Arrangements in respect of criminal property (Section 328 POCA): the act of assisting another person to retain, acquire, use or control criminal property through entering into an arrangement to facilitate this objective; and
- Acquisition, use or possession of criminal property (Section 329 POCA).

121. In addition to the three principal money laundering offences, there are related offences of failing to report where a person has knowledge, suspicion or reasonable grounds for knowledge or suspicion that another person is engaged in money laundering, where the information came to him in the course of business in the regulated sector (i.e. businesses with legal obligations to comply with UK AML/CFT controls) (Sections 330-332 POCA). These offences will be discussed in more detail in respect of Recommendation 13.

122. The money laundering offences of sections 327 to 329 of POCA cover a very wide range of acts which may be performed in connection with criminal property and in this regard corresponds with the requirements for the criminalisation of money laundering in terms of the Vienna and Palermo conventions.

123. The money laundering offences of sections 327 to 329 of POCA apply to acts carried out in relation to "*criminal property*" which means that the meaning and scope of the term "criminal property" is central to the coverage of these three offences. "Criminal property" is property which constitutes or represents, directly or indirectly, a person's benefit from criminal conduct (Section 340(3) POCA). "*Property*" refers to all property wherever situated (Section 340 (9) POCA); there are no limits on the value of the criminal property involved in the money laundering offences. For the purpose of applying the three offences it is immaterial who carried out the criminal conduct and who benefited from it (Section 340(4) POCA).

124. The property in question must in fact be criminal property as defined in section 340(3) of POCA. This objective fact may be proven by means of circumstantial evidence. It is not necessary to obtain a conviction for a predicate offence in order to prove that property is "criminal property". The circumstantial evidence relied upon can include a combination of factors such as the means of the accused in relation to his or her lifestyle, the manner in which the property was disposed of, expert evidence of a financial nature concerning the accused's transaction activity, evidence of previous bad character, including the accused criminal record, etc.

125. The UK takes an "all crimes" approach to money laundering, that is: there is no finite list of crimes that constitute predicate offences. The criminal conduct to which the concept of "criminal property" applies includes conduct which constitutes an offence in any part of the UK. It also includes

conduct which would constitute an offence in the UK had the conduct occurred in the UK (Section 340(2) POCA). As a result the money laundering offences of the POCA can be applied to proceeds derived from any offence under UK criminal law as well as predicate offence which occurs outside of the UK. The designated categories of offences are criminal offences according to the following provisions:

- participation in an organised criminal group and racketeering – UK relies on the offences of conspiracy under section 1 of the Criminal Law Act 1977 and the common law offence of conspiracy to defraud as regards participation in a criminal organisation. These provisions would also deal with conduct that amounts to "racketeering";
- terrorism, including terrorist financing – offences in Terrorist Act 2000 (terrorist financing sections 15- 23) and Anti-Terrorism Crime and Security Act 2001;
- trafficking in human beings – trafficking for sexual exploitation sections 57 – 60 of the Sexual Offences Act 2003. for non-sexual exploitation offence under Immigration and Asylum (Treatment of Claimants) Act 2004;
- sexual exploitation (including that of children) – offences under the Sexual Offences Act 2003;
- illicit trafficking in narcotic drugs and psychotropic substances – offences under the Misuse of Drugs Act 1971;
- illicit arms trafficking – Schedule 2 of POCA and the Firearms Act 1968;
- illicit trafficking in stolen and other goods – as regards trafficking in and out of the UK there are offences under the Customs and Excise Management Act 1979; as regards within the UK there is the offence of handing stolen goods under section 22 of the Theft Act 1968, for trading in illicit cultural artefacts there is the offence under section 1 of the Trading in Cultural objects (Offences) Act 2003;
- corruption and bribery – common law offence of bribery, section 1 of the Prevention of Corruption Act 1906, section 1 Public Bodies corrupt Practices Act 1889, section 109 Anti-terrorism Crime and Security Act 2001 (bribery and corruption committed outside the UK);
- fraud – the Fraud Act 2006 (commencing January 15 2007) and the common law offence of conspiracy to defraud;
- counterfeiting currency – offences under the Forgery and Counterfeiting Act 1981;
- counterfeiting and the piracy of products - offences under the Copyright Designs and Patents Act 1988 and the Trade Marks Act 1994;
- environmental crime – offences under the Environmental Protection Act 1990;
- murder, grievous bodily injury – common law offence of murder and section 18 and 20 of the Offences Against the Person Act 1861;
- kidnapping, illegal restraint and hostage taking; the common law offence of kidnapping and false imprisonment and the offence under section 1 of the Taking of Hostages Act 1982;
- robbery or theft – sections 1, and 8 of the Theft Act;
- smuggling – offences under the Customs and Excise Management Act 1979;
- extortion – the offence of blackmail under section 25 of the Theft Act 1969;
- forgery – offences under the Forgery and Counterfeiting Act 1981;
- piracy – the common law offence of piracy jure gentium and section 2 of the Piracy Act 1837;
- insider trading/market manipulation – sections 52 – 64 Criminal Justice Act 1993; section 397 of FSMA 2000.

126. The money laundering offences under POCA apply to "*a* person" which means that there is no qualification as to who the person concerned is: these offences can apply equally to a person who commits a predicate offence and carries out the money laundering activities as well as a person who carries out the money laundering activities without being involved in the predicate offence. This is reinforced by section 340(4) of POCA which provides that it is immaterial who carried out the conduct and who benefited from it.

127. Conspiracy and attempts to commit offences, aiding and abetting the commission of an offence and counselling the commission of crime exist as substantive offences under various statutes and the general principles of UK criminal law. For England and Wales, attempt is covered by section 1 of the Criminal Attempts Act; conspiracy is covered by section 1 of the Criminal Law Act. Other ancillary offences are covered by section 8 of the Accessories and Abettors Act 1861. For Scotland, these are covered under Criminal Procedure (Scotland) Act 1995 section 294 (attempt); section 293 (aiding and abetting); conspiracy is covered by common law principles. Ancillary offences apply in Northern Ireland in the same way they do for England and Wales.

128. In addition, one of the money laundering offences under POCA applies specifically to those who enter into, or become concerned in, an arrangement which they know or suspect facilitates the laundering of criminal property on behalf of another person (Section 328 POCA).

129. The three money laundering offences of sections 327-329 of POCA are all offences for which intent is required. Hence these offences apply to persons who knowingly engaged in the conduct in question. In respect of the nature of the property concerned POCA provides that the alleged offender should know or suspect that the property constitutes, or represents, the benefit from criminal conduct (Section 340 (3) POCA. POCA does not contain specific provisions on how to prove the knowledge or suspicion. However, as with all other offences involving intent, the prosecution need to rely on inferences that can be drawn from certain facts to prove the accused's state of mind. Such inferences may therefore be drawn from the factual circumstances in considering offences of money laundering in order to establish intent.

130. The money laundering offences in POCA refer to "a person". The term person, when used in legislation, includes natural and legal persons as provided for under the Interpretation Act 1978 which states that "person" is defined as including a body of persons corporate or unincorporate (Schedule 1 Interpretation Act 1978). As a result, there is no distinction in UK law between natural and legal persons in as far as the application of criminal liability is concerned, which means that legal persons can be subjected to criminal liability in the same way that natural persons are.

131. Under section 334 of POCA, a person guilty of a principal money laundering offence under section 327-329 is liable on conviction on indictment to a maximum term of imprisonment of 14 years, or to a fine, or both. Statistics provided by the UK authorities indicate that the average terms of imprisonment for 2003 and 2004 are 49.5 and 30.6 months, respectively. The maximum penalty for failing to disclose, for the nominated officer offences, and for the tipping off and prejudicing an investigation offences, is five years imprisonment. In all cases, an unlimited fine can be imposed as well.

132. It is the policy of the UK prosecuting authorities that all prosecuting staff be able to prosecute the money laundering offences in POCA as a general part of their functions. Hence, all lawyers in the Crown Prosecution Service (responsible for England and Wales) and the RCPO receive training in relation to POCA, including the money laundering provisions. The same applies to the Public Prosecution Service Northern Ireland. In both cases this includes independent counsel, who are eligible to be briefed in money laundering prosecutions. In England and Wales as well as Northern Ireland, a system of appointing "proceeds champions" for the various regions is used. Proceeds champions are responsible for assisting colleagues with cases relating to proceeds of criminal conduct. In Scotland prosecutions are undertaken by the Crown Office. Within this office a special team has been appointed to undertake money laundering prosecutions.

Precursor legislation

133. Before 24 February 2003, POCA money laundering was criminalised in terms of two separate pieces of precursor legislation, namely the Criminal Justice Act 1988 and the Drug Trafficking Act 1994. The scope of the money laundering offences under these two pieces of legislation differed in that the Drug Trafficking Act 1994 applied to money laundering in respect of predicate offences

relating to drug trafficking while the Criminal Justice Act applied to money laundering in respect of all other predicate offences. This distinction is relevant when considering some of the statistical information provided below, since prosecuting authorities using precursor legislation had to have evidence of the nature of the predicate offence in order to establish which legislation to apply.

Statistics: HMRC (England, Wales, Northern Ireland and Scotland)

	2002/2003	2003/2004	2004/2005
investigation	91	95	95
prosecution	81	66	65
conviction	34	30	34

Statistics: England and Wales

Defendants proceeded against for money laundering related offences (Police & SOCA precursor agency investigations) (*Source: Home Office*):

	2003		2004		2005	
Legislation	Proceeded Against	Found guilty	Proceeded against	Found guilty	Proceeded against	Found guilty
POCA	89	15	413	129	1302	566
Criminal Justice Act 1988	131	58	96	50	5	5
Drug Trafficking Act 94	80	50	43	28	20	24

(NB Home Office statistics collected by calendar year, ACPO statistics by financial year)

Sentencing information for ML offences 2003-2005 (Source: Home Office):

2005 ML Offences	Proceeded	Found guilty	Sentenced	CD/ AD*	Fine	Com-munity	Sus-pended	Custody	Avge custody length (mnths)	d/w **
TOTALs	**1327**	**595**	**576**	**54**	**53**	**240**	**29**	**294**	**20.1**	**8**
Criminal Justice Act 1988 - ss 93A, 93B, 93C, 93D	5	5	5			1	2	2	**31**	
Drug Trafficking Act 1994 - ss 49, 50, 51, 52, 53	20	24	24		1	8	2	13	**26.5**	
Total for offences under Proceeds of Crime Act 2002	**1302**	**566**	**547**	**54**	**52**	**231**	**25**	**179**		**5**
Concealing - ss 327/334	392	154	150	8	5	55	7	74	**21**	1
Arrangements - ss 328/334	229	69	69	5	3	26	2	31	**22.2**	2
Acquisition/use/possessio n - ss 329/334	674	343	326	41	44	150	16	73	**17.1**	2
Failure to disclose - ss 330/334	4									
Failure to disclose - ss 331/334	1									
Tipping off – ss 333 and 334 (1)	1									
Prejudicing an investigation - s 342			1							
Failing to comply with disclosure/cust info order - s 359			1						**6**	
2004 ML Offences	**Proceeded**	**Found**	**Sentenced**	**CD/**	**Fine**	**Com-**	**Sus-**	**Custody**	**Avge**	**d/w**

		guilty		AD		munity	pended		custody length (mnths)	
TOTALs	**552**	**207**	**205**	**13**	**8**	**51**	**9**	**116**	**28.8**	**8**
Criminal Justice Act 1988 - ss 93A, 93B, 93C, 93D	96	50	50	2	1	8	6	33	**24.6**	
Drug Trafficking Act 1994 - ss 49, 50, 51, 52, 53	43	28	28	3		3	1	21	**30.1**	
Total for offences under Proceeds of Crime Act 2002	**413**	**129**	**127**	**8**	**7**	**40**	**2**	**62**	**30.6**	**8**
Concealing - ss 327/334	140	39	37	3		7	1	24	**39.7**	2
Arrangements - ss 328/334	79	23	22	2		7		10	**32.4**	3
Acquisition/use/possessio n - ss 329/334	186	61	62	3	7	25	1	26	**23.7**	
Failure to disclose - ss 330/334	3	2	2					2	**3**	
Failure to disclose - ss 331/334	1									
Prejudicing an investigation - s 342	1	1	1			1				
Failing to comply with disclosure/cust info order - s 359	3	3	3							3
2003 ML Offences	**Proceeded**	**Found guilty**	**Sentenced**	**CD/ AD**	**Fine**	**Com- munity**	**Sus- pended**	**Custody**	**Avge custody length (mnths)**	**d/w**
TOTALs	**211**	**108**	**107**	**1**	**1**	**18**	**5**	**82**	**33**	
Criminal Justice Act 1988 - ss 93A, 93B, 93C, 93D	131	58	58			12	3	43	**25.3**	
Drug Trafficking Act 1994 - ss 49, 50, 51, 52, 53	80	50	49	1	1	6	2	39	**38.9**	
Total for offences under Proceeds of Crime Act 2002	**89**	**15**	**12**			**3**		**6**	**49.5**	**3**
Concealing - ss 327/334	29	4	3			0		1	**36.0**	2
Arrangements - ss 328/334	33	4	4			1		2	**78.0**	1
Acquisition/use/possessio n - ss 329/334	25	7	5			2		3	**35.0**	
Failing to comply with disclosure/cust info order - s 359	2									
2002 ML Offences	**Proceeded**	**Found guilty**	**Sentenced**	**CD/ AD**	**Fine**	**Com- munity**	**Sus- pended**	**Custody**	**Avge custody length (mnths)**	**d/w**
Total for all offences	**256**	**86**	**86**		**2**	**17**	**6**	**60**		**1**
S93A Criminal Justice Act 1988 - assisting	40	13	13			4	1	8		
S93B CJA 1988 - acquisition/possession/ use	34	20	20			7	1	12		
S93C CJA 1988 - concealing/transferring	53	13	13			2	2	9		
Totals	127	46	46			13	4	29		
S49 Drug Trafficking Act 1994 - concealing / transferring	66	19	19			1	1	16		1
S50 DTA 1994 - assisting	37	6	6			2		4		

S51 DTA 1994 - acquisition/possession/use	25	13	13		1	1	1	10		
S52 DTA 1994 - failure to disclose		1	1					1		
S53 DTA 1994 - tipping off	1	1	1		1					
Totals	129	40	40		2	4	2	31		1

**"CD/AD" = conditional discharge / absolute discharge*
***"d/w" = otherwise dealt with*

Police (England & Wales): Financial Investigations & Money Laundering Prosecutions 2004 – 2006 (Source: ACPO / Home Office):

	Number of Financial Investigations completed	Number of Money Laundering Prosecutions	Number of Financial Investigations completed	Number of Money Laundering Prosecutions
	2004-2005	**2004-2005**	**2005-2006**	**2005-2006**
Avon & Somerset	237	16	265	23
Bedfordshire	24	0	34	8
Cambridgeshire	62	6	37	8
City of London	77	0	56	0
Cheshire	80	1	78	1
Cleveland	98	21	59	22
Cumbria	20	0	63	8
Derbyshire	240	3	152	0
Devon & Cornwall	62	1	112	1
Dorset	254	2	167	4
Durham	16	4	12	3
Dyfed-Powys	14	1	19	1
Essex	328	0	177	1
Gloucestershire	178	3	192	0
Greater Manchester Police	766	0	611	17
Gwent	26	0	27	3
Hampshire	478	0	538	0
Hertfordshire	57	0	227	0
Humberside	501	0	242	1
Kent	332	2	300	0
Lancashire	86	3	48	3
Leicestershire	87	29	85	34
Lincolnshire	229	0	144	2
Merseyside	87	6	213	15
Metropolitan Police Service	148	40	Not available	Not available
Norfolk	59	0	32	3
N Yorkshire	59	0	33	0
N Wales	158	1	141	4
Northamptonshire	119	0	114	5
Northumbria	26	0	39	2
Nottinghamshire	164	18	149	40
S Wales	99	1	183	0
S Yorkshire	94	0	52	1
Staffordshire	127	1	194	5
Suffolk	60	0	46	4
Surrey	10	0	53	14
Sussex	159	4	317	2
Thames Valley Police	310	2	252	0

Warwickshire	100	0	45	0
W Mercia	386	10	424	1
W Midlands	186	2	251	19
W Yorkshire	50	0	112	7
Wiltshire	80	0	71	0
British Transport Police	121	0	88	5
Total England & Wales	6854	267	6454	365

NB: statistics show prosecutions where ML was the main charge. Many financial investigations may have been initiated for other financial crime issues and resulted in other charges (fraud, theft, etc).

Statistics: Northern Ireland

DPPNI statistics: defendants proceeded against for POCA money laundering offences in Northern Ireland (*Source: NIO*)

Legislation	Proceeded Against 2003	Found guilty 2003	Proceeded against 2004	Found guilty 2004
POCA	1	1	1	1

Statistics: Scotland

134. In 2005, **1** conviction for money laundering was secured by the COPFS; in 2006 to date there have been **7** convictions. The following data were provided for the convictions:

AGENCY	YEAR SENTENCED	M/L AMOUNT	POCA SECTION	SENTENCE
COPFS	2005	£3,400	328	Fined £100
SCDEA	2006	£348,120	329 329 327 327	7 yrs imp 4 yrs imp 7 yrs imp 4 yrs imp
HMRC	2006	£2.4million	330/329 x 2 330/329/327	7 yrs imp 6 yrs imp
HMRC	2006	£191,689 ?	327 x 2	2 yrs imp
D & G	2006	£259,780	327	5 yrs imp
COPFS	2006		329	2 yrs imp
Strathclyde	2006	£84,491	327	3 yrs 9mths imp
HMRC	2006	£98,451.41 £40,743.18	328 328	16 mths imp 10 mths impr

2.1.2. Recommendations and Comments

135. The money laundering offences in the UK are broad in their scope and appear to be used frequently. The introduction of POCA brought about a major improvement over the precursor

legislation since it is no longer necessary for UK authorities to distinguish between drug trafficking and other predicate offences upon the evidence at their disposal.

136. Although the conviction rates for money laundering offences are lower than the general averages for other offences, the prosecuting authorities indicate that it is in line with what they would expect for offences that are similar in nature – i.e. complex cases involving financial investigation and circumstantial evidence combined with a jury trial. In addition, in England and Wales, the number of investigations, prosecution and convictions under POCA all show a positive trend—they have each been increasing substantially each year since POCA first came into force in 2003.

137. In spite of all the structures in place in the various prosecuting authorities it is noticeable from the statistics provided that the numbers of prosecutions and convictions in Northern Ireland and Scotland are significantly lower than in England and Wales. The authorities indicate that they expect the numbers of prosecutions in Northern Ireland and Scotland to increase as more investigations under POCA are completed and the training for prosecutors in these jurisdictions starts taking effect. Scottish authorities informally indicated that statistics have already increased in 2006, although specific statistics were not yet available.

2.1.3 Compliance with Recommendations 1 & 2

	Rating	Summary of factors underlying rating
R.1	C	
R.2	C	

2.2 Criminalisation of Terrorist Financing (SR.II)

Description and Analysis

Special Recommendation II

Terrorism Act 2000

138. Part III of the Terrorism Act 2000 ("TACT") sets out the principal offences relating to terrorist property:

- Fund raising (Section 15 TACT): this includes three distinct acts namely:
  - the act of inviting another to provide money or other property with the intention that it be used for terrorism or having reasonable cause to suspect that it may be used for the purposes of terrorism,
  - the act of receiving money or other property with the intention that it be used for terrorism or having reasonable cause to suspect that it may be used for the purposes of terrorism, and
  - the act of providing money or other property with the intention that it be used for terrorism or having reasonable cause to suspect that it may be used for the purposes of terrorism;
- Use and possession (Section 16 TACT): the act of using money or property for terrorism as well as the possession of money or property with the intention that it be used for terrorism or having reasonable cause to suspect that it may be used for the purposes of terrorism;
- Funding arrangements (Section 17 TACT): the act of entering into or becoming concerned in an arrangement to make money or other property available to another person while knowing or having reasonable cause to suspect that it is to be used for the purposes of terrorism;
- Money laundering (Section 18 TACT): the act of entering into or becoming concerned in an arrangement which facilitates the retention or control of terrorist property.

The Terrorism (United Nations Measures) Order 2006

139. The Terrorism (United Nations Measures) Order 2006 ("2006 UN Order") allows the Treasury to designate certain persons based on their involvement in terrorism or their inclusion in Council Decision 2006/379/EC as provided for in Article 2.3 of Regulation (EC) No 2580/2001 of 27 December 2001. A total of 84 individuals and 58 entities had been designated under the 2006 UN Order at the time of the on-site visit.

The Al-Qaida and the Taliban (United Nations Measures) Orders 2002 and 2006

140. The Al-Qaida and the Taliban (United Nations Measures) Order 2002, as amended by the Al-Qaida and the Taliban (United Nations Measures) Order 2006 ("2006 Al-Qaida Order"), allows the Treasury to designate certain persons on the basis of their designation by the committee of the Security Council of the United Nations established pursuant to S/RES/1267(1999).

141. The terrorist financing offences of TACT, in particular section 15, clearly apply to the acts of providing or collecting of funds. The purpose for which the funds in question is to be provided or collected, namely "terrorism" is defined in section 1 of TACT and includes the use or threat of actions involving serious violence against a person, serious damage to property, endangering the life of a person, creating serious health or safety risks or seriously interfering with an electronic system which is aimed at influencing the government or intimidating the public in order to advance a political, religious or ideological cause. This definition of "terrorism" closely matches that of Article 2(1)(b) of the TF Convention.

142. With regard to Article 2(1)(a) of the TF Convention, the UK has acceded to, or ratified all the Conventions and Protocols referred to in the Annex to the TF Convention. As part of the processes of accession to, or ratification of, these Conventions and Protocols the UK also criminalised the activities by the Conventions and Protocols. However, neither the offences under sections 15 to 18 of TACT, nor the definition of "terrorism" in section 1 of the Act, refer expressly to the activities contemplated in the various Conventions and Protocols referred to in the Annex to the TF Convention. As a result the financing of these activities is not criminalised expressly in terms of a self-standing offence.

143. The fund-raising and other terrorist financing offences under sections 15 to 18 of TACT apply to "terrorism" as defined in that Act. As a consequence the scope of the terrorist financing offences is determined by the scope of the definition of "terrorism". For conduct to fall within the definition of "terrorism" it must:

a) involve an action, or a threat of action, of a certain nature namely involving serious violence against a person, involving serious damage to property, endangering a person's life, creating a serious risk to the health or safety of the public or a section of the public, or being designed seriously to interfere with or seriously to disrupt an electronic system, *and*
b) must be designed to influence the government (of any country) or to intimidate the public (of any country), *and*
c) must be done for the purpose of advancing a political, religious or ideological cause.

144. The references in the definition of "terrorism" to actions defined in (a) above could include the majority of the activities referred to in the Conventions and Protocols of the Annex to the TF Convention. This means that the terrorist financing offences under sections 15 to 18 of TACT could apply to the financing these particular activities if the activity to be financed included the purposive elements described in (b) and (c) above (i.e., the purpose of influencing a government, intimidating the public, and advancing a political goal). While these provisions would thus cover the financing of the majority of activities referred to in the Conventions and Protocols of the Annex to the TF Convention, there may still be some instances where this would not be the case, in particular in relation to those activities which do not involve violence or the threat of violence, or lacks the purposive elements referred to above. In relation to such instances, the UK authorities indicated that they would rely on the offences of aiding and abetting, conspiracy and complicity in the principle offences which were created to comply with the various Conventions and Protocols in question. As a result it can be said that the UK relies on a combination of the fund-raising and other terrorist financing offences under sections 15 to 18 of TACT and aiding and abetting, conspiracy and complicity in the principle offences which were created to comply with the various Conventions and Protocols in question to meet the requirements of Article 2(1)(a) of the TF Convention.

145. When section 15 of TACT, which provides for the offence of raising funds for the purposes of terrorism, is read with the definition of the term "terrorism" in section 1(1) of TACT, it is clear that this offence expressly covers the provision or collection of funds for the purpose of carrying out a terrorist act(s).

146. Part II of TACT provides for a process of proscribing certain organisations. Currently 42 international and 14 Irish organisations are proscribed under the provisions of this Part. An organisation may be proscribed if the organisation is believed to be involved in terrorism. The determining factors are that it commits or participates in terrorism, prepares for terrorism, promotes or encourages terrorism or is otherwise concerned in terrorism. Section 1(5) of TACT provides that the concept of an action taken for the purpose of terrorism includes an action taken for the benefit of a proscribed organisation. If this provision is read together with section 15 of TACT the act of raising funds for the benefit of a proscribed organisation would be considered to be raising funds for the purposes of terrorism and would be an offence under section 15 of TACT.

147. Outside the context of proscribed organisations, the raising funds for an organisation which is involved in terrorist activities would have to be considered in relation to the provisions of section 15

of TACT, and the other offences relating to money or property destined to be used for the purposes of terrorism under sections 16 to 18 of TACT. These offences include situations where a person has *reasonable cause to suspect* that the money or property in question *may* be used for terrorism without having any actual knowledge or any motive as to the manner in which the money or other property is to be used by the organisation in question. In the case where a person raises funds knowing that those funds are destined for an organisation which is involved in terrorism, the person will be taken to have reasonable cause to suspect that the funds in the hands of the organisation may be used for the purpose of terrorism. Hence the offences of raising funds for the purposes of terrorism under section 15 of TACT, and the other offences relating to money or property destined to be used for the purposes of terrorism under sections 16 to 18 of TACT, include the providing and collecting of funds for use by a terrorist organisation which is not proscribed.

148. The same argument would apply in respect of the providing and collecting of funds for use by an individual terrorist. In the case where a person raises funds knowing that those funds are destined for an individual who is considered to be a terrorist, the person will be taken to have reasonable cause to *suspect* that the funds in the hands of the individual in question *may* be used for the purpose of terrorism. Hence the offences of raising funds for the purposes of terrorism under section 15 of TACT, and the other offences relating to money or property destined to be used for the purposes of terrorism under sections 16 to 18 of TACT, include the providing and collecting of funds for use by an individual terrorist.

149. These provisions are further strengthened by the provisions of the 2006 UN Order, which are primarily aimed at freezing the funds and economic resources of designated persons. In addition to the provisions relating to the freezing of economic resources, the order also contains a provision which makes it an offence to provide funds, economic resources and financial services to such persons (Paragraph 8 of the 2006 UN Order). The offence referred to above applies to the providing of funds to a terrorist organisation or to an individual terrorist if such an organisation or individual was designated under the Order. The offence does not, however, include the collection of funds for use by designated person or entities.

150. The 2006 Al-Qaida Order follows the same construction as the 2006 UN Order and contains a comparable provision which makes it an offence to provide funds, economic resources and financial services to designated persons (Paragraph 8 of the 2006 Al-Qaida Order). The 2006 Al-Qaida Order also contains the same definitions for the terms “economic resources” and “funds”. The earlier remarks concerning the scope and application of the offence under the 2006 UN Order would therefore apply with equal force in relation to the offence under the 2006 Al-Qaida Order.

151. The TACT definition of the term “terrorist property” refers to “money or other property” (Section 14(1) TACT). The term “property” in turn is defined as “property wherever situated and whether real or personal, heritable or moveable, and things in action and other intangible or incorporeal property” (Section 121 TACT). This therefore closely mirrors the definition provided by the Terrorist Financing Convention.

152. The term “funds” in the 2006 UN Order and the 2006 Al-Qaida Order is given a wide definition which extends beyond cash and balances in bank accounts to include instruments such as securities dividends and letters of credit (Paragraph 2 of the 2006 UN Order and the 2006 Al-Qaida Order, respectively). The term “economic resources” is also given a relatively wide definition and includes assets of every kind, whether tangible or intangible, movable or immovable, which are not funds but can be used to obtain funds, goods or services.

153. Neither TACT nor the 2006 UN and 2006 Al-Qaida Orders contains a provision which expressly provides that it is necessary to show that the funds concerned were actually used to carry out a terrorist act or can be linked to a terrorist act. Section 15 of TACT refers to the collection or provision of money or other property which a person has reasonable cause to suspect that it *may* be used for *terrorism*. In addition, section 14(1)(a) TACT defines the term “terrorist property” as "(a)

money or other property which is *likely* to be used for the purposes of terrorism (including any resources of a proscribed organisation), (b) proceeds of the commission of acts of terrorism, and (c) proceeds of acts carried out for the purposes of terrorism." These references indicate that it would not be necessary to show that funds have actually been used to carry out terrorist acts or that they can be linked to specific terrorist acts. In such cases the conviction for the relevant offence is based on the factual basis of the mere possibility that the money or property may be used for the purpose of terrorism.

154. The provisioning offences under the 2006 UN and 2006 Al-Qaida Orders relate to the providing of funds to persons and entities designated under the Orders and do therefore not require that the funds concerned be actually used in a terrorist act or linked with such an act.

155. Attempts to commit, or conspiracies and aiding and abetting the commission of, any of the offences under TACT or the 2006 UN and 2006 Al-Qaida Orders, outlined above, are substantive offences under the general principles of UK criminal law. (See paragraph 127 under the description of Recommendation 1 for a more detailed explanation of these provisions.)

156. As described above, the money laundering offences under POCA apply to all crimes, which means that there is no finite list of crimes that constitute predicate offences. (Section 340(2) POCA). As a result the offences relating to terrorist financing under sections 15 to 18 of TACT is automatically deemed to be a predicate offence for money laundering purposes.

157. Section 1(4) of TACT provides for an extra-territorial element to the concept of terrorism. The action referred to in the definition of terrorism includes action outside the UK (Section 1(4)(a) TACT). The reference to a person or property affected or threatened by the action applies to a person or property wherever situated (Section 1(4)(b) TACT). The reference to the public to be intimidated by the action, includes the public of a country other than UK (Section 1(4)(c) TACT). The reference to the government to be influenced by the action, includes a government of a country other than UK (Section 1(4)(d) TACT). As a result of this wide meaning that is accorded to the term "terrorism", the terrorist financing offences of sections 15 to 18 of TACT include the financing of terrorists, terrorist organisations and terrorist acts outside the UK.

158. As pointed out earlier in relation to the money laundering offences under POCA, in all cases of offences involving intent, the prosecution needs to rely on inferences that can be drawn from certain facts in order to prove the accused's state of mind. The same would apply in relation to the terrorist financing offences under sections 15 to 18 of TACT where inferences may be drawn from the factual circumstances in considering the accused's intent.

159. The terrorist financing offences under sections 15 to 18 of TACT all refer to "a person". As was pointed out earlier the term "person", when used in legislation, includes natural and legal persons as provided for under the Interpretation Act 1978 which states that "person" is defined as including a body of persons corporate or unincorporate (Schedule 1, Interpretation Act 1978).

160. The maximum penalties prescribed for the terrorist financing offences under sections 15 to 18 of TACT are imprisonment for a period of 14 years or an unlimited fine or both (Section 22 TACT). Following conviction of an offence under Section 15 to 18 of TACT, the court may order forfeiture of any money or property (Section 23 TACT).

Investigation and prosecution of FT

161. The UK authorities have created a dedicated capacity for the investigation of terrorist financing offences, namely the National Terrorist Finance Investigation Unit (NTFIU). NTFIU reported that, as a matter of policy, every investigation into terrorism includes a financial investigation. It appears, however, that in the majority of cases the financial investigations are not primarily focused on the terrorist financing provisions under the TACT, but are rather intended as a means to investigate

terrorist activities themselves. Terror cells encountered by UK law enforcement tend to have multiple skill sets: separate financiers who are not also involved in actual or intended terrorism are rare. The NTFIU has conducted 19 investigations where the *primary focus of the investigation* is countering terrorist finance. At the time of the on-site visit, four such investigations had been undertaken in 2006 (one of which includes several entities e.g. numerous charities).

Terrorist Finance prosecutions

(2001 to 2004 reports of Independent Reviewer on operation of the TACT)

			2001	2002	2003	2004	2005
Charges with TF offences	**Fund raising (s. 15 of the TACT)**	Northern Ireland	4	9	6	2	n/a
		Great Britain	4	6	2	2	4
	Use and possession (s.16 of the TACT)	Northern Ireland	0	0	0	0	n/a
		Great Britain	2	0	3	0	6
	Funding arrangements (s. 17 of the TACT)	Northern Ireland	0	0	0	0	n/a
		Great Britain	4	0	2	4	1
	Money laundering (s. 18 of the TACT)	Northern Ireland	0	0	0	0	n/a
		Great Britain	0	6	0	1	0
Total			14	21	13	11	11

162. The results of the cases reflected in these statistics in respect of Great Britain (i.e. excluding Northern Ireland) are as follows:

2001 - number charged - 10
5 convictions
5 cases discontinued

2002 - number charged - 12
0 convictions
1 awaits extradition to US
3 found not guilty
3 jury could not come to a decision and charge remains on file
5 cases discontinued

2003 - number charged - 7
2 convictions
5 cases discontinued

2004 - number charged - 7
0 convictions
1 awaits extradition to US
3 found not guilty
3 cases discontinued

2005 - number charged - 11
1 conviction
1 currently on trial
2 found not guilty
7 cases discontinued

163. The cases marked "discontinued" refer to cases which resulted in a conviction for a more serious offence and no verdict was returned in respect of the terrorist financing charges. In these instances the courts were not required to pronounce a verdict in relation to the terrorist financing offences, as this would not have added to the sentences imposed in respect of the more serious

offences of which the accused had been convicted. The terrorist financing charges are "left on file" (effectively neither open nor closed) and the authorities have the option of further pursuing these charges should the accused succeed in having their convictions of the more serious offences reversed on appeal.

164. UK officials also described an investigation in late 2001 into a group using bank and credit card fraud to fund terrorism. Eventually, 20 individuals were charged in relation to this investigation. 18 of the individuals were prosecuted for and convicted of fraud and related charges. The other two were prosecuted for and convicted of making money and other equipment available for terrorists.

2.2.2 Recommendations and Comments

165. The provisions criminalising terrorist financing under sections 15 to 18 of TACT, read together with the definitions in sections 1 and 14 have a very wide coverage. The UK authorities are firmly of the opinion, and the evaluation team agreed, that this is sufficient to ensure the successful prosecution of the provision or collection of funds for use by terrorist organisations and individual terrorists. Although these interpretations appear to be reasonable and plausible, they would have to be applied in practice in order to confirm their acceptability in the UK courts.

166. As indicated above the UK relies on a combination of the fund-raising and other terrorist financing offences under sections 15 to 18 of TACT and aiding and abetting, conspiracy and complicity in the principle offences which were created to comply with the various Conventions and Protocols in question to meet the requirements of Article 2(1)(a) of the TF Convention. While most of the activities covered in the Annex to the TF Convention would conceivably involve serious violence against a person, involve serious damage to property, endanger a person's life, create a serious risk to the health or safety of the public or a section of the public or be designed seriously to interfere with or seriously to disrupt an electronic system, the activity would only amount to "terrorism" (and therefore financing of these activities is only punishable) if the other two criteria in TACT are also met—i.e. it is designed to influence the government or to intimidate the public and is done for the purpose of advancing a political, religious or ideological cause. Whether this is the case would depend on the circumstances of each case.

167. As in the case of prosecution of the provision or collection of funds for use by terrorist organisations and individual terrorists, the interpretation of the fund-raising and other terrorist financing offences of sections 15 to 18 of TACT to include the financing of the activities covered by the Conventions and Protocols referred to in the Annex of the TF Convention, would have to be applied in practice in order to confirm its acceptability in the UK courts. Should the UK courts not accept this interpretation the UK authorities would have to rely solely on the offences of aiding and abetting, conspiracy and complicity in the principle offences which were created to comply with the various Conventions and Protocols in questioning order to deal with the financing thereof.

168. It is therefore recommended that the UK authorities make the link between the terrorist financing offences under the TACT and the Conventions and Protocols referred to in the Annex to the TF Convention more explicit to remove any doubt which there may be in this regard. UK authorities should also improve their system for statistics for FT prosecutions and convictions.

2.2.3 Compliance with Special Recommendation II

	Rating	Summary of factors underlying rating
SR.II	C	

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

2.3.1 Description and Analysis

Recommendation 3

General

169. UK law provides for the confiscation of laundered property which represents proceeds from, instrumentalities used in, and instrumentalities intended for use in the commission of ML, FT or other predicate offences, and property of corresponding value. Since the introduction of the Proceeds of Crime Act (POCA) in 2002, the United Kingdom has had in place four different schemes for confiscation and recovery measures with regard to proceeds of crime. These are: (1) confiscation following a criminal conviction; (2) civil recovery; (3) taxation; (4) seizure-forfeiture of cash.

170. Only the confiscation regime requires a conviction and therefore the identification of a specific offence. Confiscation is considered as part of the sanction process when sentencing a convicted defendant. The other measures are not dependant on conviction of the perpetrator; only that unlawful conduct in general is the root of the proceeds.

171. POCA also contains provisional measures for restraining dealings in property, such as restraint orders, interim receiving orders, and detention of cash. There are three principal pieces of legislation providing scope for confiscation and recovery of laundered money or proceeds of crime:

Legislation	Date relevant provisions brought into force
Proceeds of Crime Act 2002	Various dates between 30 December 2002 to 24 March 2003
Terrorism Act 2000	19 February 2001
Anti-terrorism, Crime and Security Act 2001	20 December 2001

Confiscation of proceeds

Proceeds of Crime Act 2002[13]

172. Confiscation is available where a defendant has been convicted of an offence that has resulted in a financial gain or proprietary benefit (Section 6 POCA). A decision to confiscate is an order to an offender to pay a sum of money equal to the value of his particular or general criminal conduct ("the proceeds"), or a smaller sum where less is available (Section 7 POCA).

173. The use of confiscation powers is not *mandatory* at the point of conviction. The process is however mandatory once the confiscation process has been initiated either by the prosecutor or (in England, Wales, & NI) the Director of the Assets Recovery Agency; or alternatively the court decides *ex officio* that it is appropriate to proceed to confiscation (Section 6(3) POCA).

174. When considering confiscation, the court must decide whether the defendant has a "criminal lifestyle". A defendant will be deemed to have a criminal lifestyle if one of the three conditions in Section 75(2) POCA is satisfied. There has to be a minimum total benefit of £5,000 for the second two of the three conditions below to be satisfied. The three conditions are: (i) it is a 'lifestyle offence' specified in Schedule 2 of POCA (for example, drug trafficking is a lifestyle offence); (ii) it is part of a 'course of criminal conduct' (particular combinations of offences and convictions must apply to

[13] Part 2 of POCA covers confiscation in England and Wales, Part 3 covers Scotland, and Part 4 covers Northern Ireland. The description uses Part 2 citations; the equivalent section numbers for Scotland and Northern Ireland have not been inserted as they have the same effect as the England and Wales provisions.)

demonstrate this); or (iii) it is an offence committed over a period of at least 6 months and the defendant has benefited from it.

175. The court is required to calculate benefit from criminal conduct using one of two methods:

(1) General criminal conduct ("criminal lifestyle confiscation") – this method is used when the defendant is deemed to have a criminal lifestyle. The court must assume (as set out in Section 10 POCA) that:

- any property transferred to the defendant from after a date 6 years prior to the commencement of the criminal proceedings was obtained as a result of criminal conduct;
- any property held by the defendant at any time after the date of conviction was obtained as the result of criminal conduct;
- any expenditure over the 6 year period mentioned above was met by property obtained as a result of criminal conduct;
- for valuation purposes, any property obtained by the defendant was obtained free of third party interests.

176. Where the criminal lifestyle condition is satisfied, the burden of proof in respect of the origin of the property is then effectively reversed, i.e. the prosecution has met its evidential obligation and the defendant has to prove - on a balance of probabilities - that a particular asset, transfer, or expenditure has a legitimate source.

(2) Particular Criminal Conduct ("criminal conduct confiscation") – this method is used when the defendant is not deemed to have a criminal lifestyle. This requires the prosecutor to show what property or financial advantage the defendant has obtained from the specific offence charged. POCA permits the prosecutor to trace property or financial advantage that directly or indirectly represents benefit (for example, property purchased using the proceeds of crime). There is no minimum threshold for this method of calculation of benefit.

Terrorism Act 2000: Forfeiture of money or property

177. If a person is found guilty of an offence relating to terrorist funding, or terrorist money laundering under Sections 15 – 18 of the Terrorism Act ("TACT"), Section 23 of that Act provides that certain money and property relating to those offences may be ordered by the court to be forfeited:

- if a person is convicted of an offence under Section 15 (1) or (2) or 16 of TACT, the court can order the forfeiture of money or property that was in his possession, or under his control, at the time of the offence and which he intended should be used, or had reasonable cause to suspect would be used, for the purposes of terrorism;
- if a person is convicted of an offence under Section 15(3) of TACT, the court can order the forfeiture of money or property that was in his possession, or under his control, at the time of the offence and which he knew, or had reasonable cause to suspect, would be used for the purposes of terrorism;
- if a person is convicted under Section 17 of TACT, the court can order the forfeiture of money or other property which related to the arrangement in question under Section 17 and which he knew, or had reasonable cause to suspect, would be used for the purposes of terrorism;
- if a person is convicted under Section 18 of TACT the court can order forfeiture of money or property to which the arrangement in question under section 18 relates.

178. Forfeiture can also be ordered in respect of any payment or reward received by the defendant in connection with the commission of the offence. All these forfeiture provisions require the defendant to have been convicted.

Anti-terrorism, Crime and Security Act 2001: Seizure/forfeiture of cash

179. Section 1 and Schedule 1 of the Anti-terrorism, Crime and Security Act 2001 ("ATCS") provide for the seizure of cash by the police or HMRC where they have reasonable grounds for suspecting that:

- the cash is intended for use for the purposes of terrorism, or
- represents the assets of a proscribed organisation, or
- represents property obtained through terrorism, or
- is property that has been earmarked as terrorist property ("terrorist cash").

180. The cash can be subsequently forfeited by order of the court in civil proceedings if the court is satisfied that the cash is terrorist cash. The scheme has no minimum threshold although a direct link to terrorism needs to be demonstrated.

Civil recovery

Civil recovery/taxation

181. Part 5 of POCA includes a civil recovery scheme, which is operated by the Assets Recovery Agency (ARA) established in 2002 in England and Wales and Northern Ireland, and by the Civil Recovery Unit (CRU) of the Crown Office in Scotland on behalf of Scottish Ministers (who are defined as the enforcement authority in Scotland). This scheme empowers the Director of the ARA, or Scottish Ministers, to recover by way of civil proceedings property that is or represents the proceeds of unlawful conduct whether or not criminal proceedings have been brought (Section 240(2) POCA). The principal criteria for civil recovery are:

- a law enforcement agency or prosecution authority must normally refer the case;
- criminal prosecution must have been considered and either failed, proved impossible to complete, or been successful but there was no subsequent fully successful confiscation proceeding;
- recoverable property must have been identified and have an estimated value of at least £10,000 (Section 287 POCA and the Proceeds of Crime Act 2002 (Financial Threshold for Civil Recovery) Order 2003);
- recoverable property must include property other than cash or negotiable instruments (although cash is recoverable if it is in addition to other property);
- it must be shown that the property that is to be recovered is recoverable property which means that it is property obtained through unlawful conduct. To show that property was obtained through unlawful conduct there must be evidence of criminal conduct that is supported to the civil standard of proof: which is *not less than* 'on the balance of probabilities' but can be as high as 'beyond reasonable doubt'

182. Civil recovery cases are referred to the ARA or CRU by the law enforcement authorities. Unless the property holder agrees to the recovery of property without an order, the Director of the ARA or Scottish Ministers apply to the Court for an interim order freezing assets, and subsequently at a full Court hearing for the final civil recovery. Proceedings must be brought within 12 years from the moment the property was obtained. The financial threshold below which civil recovery is not pursued is set by the Home Secretary (currently the threshold is £10,000).

183. One special feature of the civil recovery regime is the appointment of the interim receiver once an application for an interim order freezing assets is made, to not only manage the assets covered by the order but also to act as the investigator in the case and prepare a report for final consideration of the court. The ARA has no further powers of investigation and its initial findings are taken over by the interim receiver who, with the powers of investigation given under POCA, pursues the investigation to conclusion and present a report to court. Based on the report, the ARA will decide

whether or not to issue a claim for civil recovery. A list of interim receivers is maintained from which appointments are made and they are, normally private sector accounting firms. Costs of the fees of the interim receiver are met by ARA.

184. Although certain powers of international cooperation are provided for in POCA, in practice ARA experiences difficulties in making out-going requests for assistance because the nature of the recovery proceedings are civil rather than criminal and therefore do not easily fit within foreign regimes for mutual legal assistance in criminal matters. The interim receiver can rely on certain standard procedures available to litigants in civil proceedings.

185. The Director of the ARA has the power to assume certain functions in relation to tax if he has reasonable grounds to suspect that income or gain for a particular tax period is the proceeds of crime. This measure is available to the Director of ARA throughout the UK, including Scotland. The power is an alternative to civil recovery, and may be used when there are reasonable grounds to suspect that a person has received income or profit from criminal conduct. In such cases, POCA enables the Director of ARA to exercise the functions of the UK's tax authority to assess a person's income and tax it.

186. POCA states that the Director of ARA must have regard to any guidance given by the Secretary of State. Guidance approved by the Home Secretary sets out a hierarchy of options that states (1) the first option remains criminal confiscation as part of a successful prosecution (2) the next stage is to consider civil recovery (3) the last option for consideration is taxation. Civil recovery will normally be pursued by ARA ahead of taxation however the Guidance on the hierarchy allows for a degree of flexibility and the Director is considering taking more cases straight to tax. To date, the taxation powers have not been heavily relied upon by ARA.

187. ARA is a non-ministerial department funded by direct vote through Parliament. For the year 2005/2006, ARA spent in the region of 16 million sterling (against aggregate payments received of about 5 million sterling). Although the aim is to make ARA effectively self-funding from the realisation of funds recovered as proceeds of crime, to date this has not happened. The realisation of funds has been significantly lower than forecast and the process of working through the POCA mechanisms to final forfeiture orders has taken longer than expected.

Seizure/Forfeiture of cash (non-conviction based provision)

188. Section 1 and Schedule 1 of the Anti-terrorism, Crime and Security Act 2001 ("ATCS") provide for the seizure of cash by the police or HMRC where they have reasonable grounds for suspecting that:

- the cash is intended for use for the purposes of terrorism, or
- represents the assets of a proscribed organisation, or
- represents property obtained through terrorism, or
- is property that has been earmarked as terrorist property ("terrorist cash").

189. The cash can be subsequently forfeited by order of the court in civil proceedings if the court is satisfied that the cash is terrorist cash. The scheme has no minimum threshold although a direct link to terrorism needs to be demonstrated.

190. Under Sections 294—300 of POCA, the police or HMRC can seize, detain and seek the forfeiture of cash of not less than £1,000 (pursuant to the limits set by the POCA (Recovery of Cash in Summary Proceedings: Minimum Amount) Order 2006) which they reasonably suspect of being recoverable property or intended for use in unlawful conduct. The definition of "cash" in POCA is broad, and encompasses notes, coins, cheques, postal orders, bankers' drafts, bearer bonds and bearer shares (POCA section 289(6)). This measure is primarily aimed at situations of criminal conduct, such as drug dealing in the street, where sums of illegally obtained cash are carried by the perpetrator. Once the funds have been seized (on suspicion) the authority that has seized the funds must prepare a case to satisfy the court that the cash is either recoverable property or intended for use in unlawful

conduct. If the court is satisfied to the civil standard of proof that the cash meets this test, it may order forfeiture (Section 297 POCA). (NB In Scotland, the forfeiture of seized cash is at the instance of Scottish Ministers not HMRC or the police – Section 298(1)(b) POCA).

Seizure and confiscation of instrumentalities

191. POCA makes no provision for the seizure and confiscation of instruments used or intended for use in the commission of criminal offences. However, miscellaneous provisions can be found in various Acts depending upon the nature of the offence and the circumstances of each case. In general, these broadly cover property used in or intended for use in the commission of ML, FT and predicate offences. These provisions are listed below:

United Kingdom

- Cash seizure (s294 POCA 2002) and cash forfeiture (s298 POCA 2002) - Extended definition of cash (s289(6) POCA 2002)
- Forfeiture of instrumentalities of crime committed (s21 Proceeds of Crime Act 1995 – Part II of this Act is the only part left in effect following POCA 2002)
- Seizure of items discovered during the course of an authorised search under section 44 (TACT), which the officer reasonable suspects are intended to be used in connection with terrorism (s45 TACT)
- Deprivation Order (s143 Powers of Criminal Courts (Sentencing) Act 2000)
- Forfeiture Order (s27 Misuse of Drugs Act 1971)
- Forfeiture Order (s23 TACT)
- Seizure and forfeiture of counterfeit currency (Forgery and Counterfeiting Act 1981)
- Forfeiture provisions – Customs & Excise Offences (Customs and Excise Management Act 1979)
- Forfeiture and disposal of firearms (s52 Firearms Act 1968)
- Forgery forfeiture (s7 Forgery and Counterfeiting Act 1981)
- Forfeiture of a vehicle, ship or aircraft – Immigration Offences (s25C Immigration Act 1971)
- Forfeiture of indecent photographs of children (s5 Protection of Children Act 1978)
- Forfeiture of knives (s6 Knives Act 1997)
- Forfeiture of obscene articles (s3 Obscene Publications Act 1959)
- Forfeiture of racially inflammatory material (s25 Public Order Act 1986)
- Forfeiture of instrumentalities of poaching (c114 Poaching Prevention Act 1862)
- Forfeiture of vehicle, ship or aircraft or of telegraphy apparatus (s54 Wireless Telegraphy Act 1949)
- Forfeiture of vehicle (s33 Road Traffic Offenders Act 1988)

Scotland

- Disposal or possession of dangerous creatures (c45 Civic Government Scotland Act 1982)
- Forfeiture of tools held by convicted thieves which can be reasonably suggested may be used to commit a crime (c45 Civic Government Scotland Act 1982)
- Confiscation of animals (Fur Farming (Prohibition) (Scotland) Act 2002)
- Forfeiture of vehicles or instruments related to salmon poaching (Salmon and Freshwater Fisheries (Consolidation) (Scotland) Act 2003 ASP 15)

Northern Ireland

- Forfeiture of property which has been/is intended for use to commit a crime (Article 11 Criminal Justice (Northern Ireland) Order 1994).

HM Revenue & Customs

- Forfeiture of goods due for shipping (S53 & 66 Customs and Excise Management Act 1979)
- Forfeiture of vehicles, aircraft and ships (S139-143 Customs and Excise Management Act 1979)

Scope of "property"

192. *Confiscation and seizure under POCA:* The approach to confiscation based on the "criminal lifestyle" criteria (see paragraphs 174-175 above) provides for the assumptions that: *any* property transferred to the defendant, or any expenditure incurred by the defendant, from a date six years prior to the start of the criminal proceedings, and any property held by the defendant after the date of his conviction, was obtained as a result of criminal conduct. Such property may therefore be subject to a confiscation order and need not necessarily comprise property directly derived from criminal conduct (Section 10 POCA). This interpretation also applies to property which may be subject to civil recovery proceedings under POCA (see below).

193. The recoverable amount, for the purposes of a confiscation order, is equal to the amount of the defendant's benefit from his criminal conduct (Section 7 POCA). A person is deemed to benefit from conduct if he obtains property as a result of, or in connection with, the conduct (Section 76 POCA) and this therefore includes direct and indirect proceeds of crime.

194. Sections 77 and 78 of POCA allow for gifts made by the defendant to other persons to be recovered in satisfaction of a criminal confiscation order. The confiscation regime therefore extends to property held by third parties.

195. *Forfeiture under Terrorism Act:* Forfeiture under this provision applies to property of the convicted person received wholly or partly, and directly or indirectly, as a payment or other reward in connection with the commission of the offence (Section 23 TACT).

196. *Seizure/forfeiture under Anti-terrorism, Security and Crime Act 2001:* The provisions for seizure/forfeiture of cash include cash intended for use in terrorism, resources of a proscribed organization and money which is, or represents, property obtained through terrorism (Section 1 ATSCA). The definition is sufficiently broad as to encompass property derived directly or indirectly from the proceeds of crime.

197. *Property held by third parties:* The nature of the POCA offences (ss 327-329) enables criminal prosecutions to be brought against any person with an involvement in money laundering, including whether they concealed criminal proceeds, assisted another person to retain criminal proceeds, or acquired, used or possessed criminal proceeds. On bringing criminal prosecutions, the court has the jurisdiction to seek confiscation of property held by the defendant. If, therefore, a third party is successfully prosecuted for a money laundering offence it may be possible to commence confiscation proceedings against them on conviction.

198. Under the 'confiscation following conviction' scheme, Section 77 POCA makes provision in certain circumstances for gifts made by the defendant to be regarded as "tainted". Section 78 POCA provides that property transferred to third parties at significantly less than market value should be treated as a gift (and therefore a tainted gift if it meets the conditions set out in Section 77 POCA). Tainted gifts form part of recoverable amount.

199. Under the civil recovery regime, Section 305 of POCA provides for property to be traced into the hands of a third party to whom the recoverable property has been disposed. Section 306 POCA provides for recoverable property to be recovered even where it has been mixed with property belonging to a third party. The main exception to the this is where property has been received in good faith, without notice, and for market value by a third party, after which the property is no longer recoverable (Section 308 POCA).

200. The civil recovery scheme under the provisions of Part 5 of POCA does not require criminal proceedings to have been brought (Section 240(2) POCA). The scheme also enables recovery of property to be sought from any person, whether or not they have been charged or convicted of a connected criminal offence. It therefore allows the recovery of money and property from third parties: the scheme is about the *providence of assets*, not who holds such assets or whether they are guilty of an offence.

Provisional measures

201. There are three principal pieces of legislation providing scope for provisional measures in relation to laundered money or proceeds of crime:

Legislation	Date relevant provisions brought into force
Proceeds of Crime Act 2002 (POCA)	Various dates between 30 December 2002 and 24 March 2003
Serious Organised Crime and Police Act 2005 (SOCPA)	1 January 2006
Police and Criminal Evidence Act 1984 (PACE)	1 January 1986

202. (For offences committed before 24 February 2003, POCA precursor legislation applies. This legislation, which is: The Criminal Justice Act 1988 and the Drug Trafficking Act 1994.)

Proceeds of Crime Act 2002 (POCA)

203. *Restraint Orders:* Sections 40 and 41 of POCA set out provisions for obtaining restraint orders which apply where a criminal investigation has started or criminal proceedings are ongoing and where there is reasonable cause to believe that the defendant has benefited from his criminal conduct. The order is to *restrain* property, rather than to *freeze*, in that the property in question remains in the hands of its owner. The principal features of this measure are:

- A restraint order can be made in respect of any 'realisable property' which is defined as any 'free property' held by the defendant or a recipient of a tainted gift (Section 83 POCA). 'Free property' is any property unless there are certain other legislative provisions which already claim that property, such as a Terrorism Act forfeiture order;
- A restraint order prevents the specified person from dealing with any realisable property (Section 41 POCA);
- These orders are available in the trial court, as soon as an investigation has begun and at any time thereafter (Section 40 POCA);
- The prosecutor, the Director of the ARA, or a financial investigator trained and accredited by the ARA may apply for such an order (Section 42 POCA);
- Anyone affected by a restraint order may appeal to have the order varied or discharged (Section 42 POCA);
- A police office or customs officer can seize property subject to a restraint order to prevent removal from England and Wales (Section 45 POCA).

204. Section 42(1)(b) POCA enables the application for a restraint order to be made *ex parte* to a judge in chambers. The power of a police or customs officer to seize property to prevent its removal

from the jurisdiction (Section 45 POCA) may be exercised without recourse to the courts. Applications for search and seizure warrants may also be made *ex parte* to a judge in chambers (Section 356 POCA).

205. *Interim Receiving Orders and Interim Administration Orders:* In circumstances where civil recovery proceedings could be initiated, Section 246 POCA provides for interim receiving orders (for E&W and NI) and interim administration orders (for Scotland). This interim measure provides for the detention, custody or preservation of property and for that property to be held by an interim receiver who must report to the court. The principal condition for obtaining such an order is that there is a good case that the property in question is recoverable or associated property.

206. *Cash detention under POCA:* The provisions of Section 295 POCA provide for the detention of seized cash for an initial period of 48 hours, followed by extended periods on application of 3 months and up to a maximum period of 2 years. The provisions apply to forfeiture of cash of not less than £1,000 which the police or customs officers suspect as being the proceeds of crime or intended for unlawful use. In practice, this measure enables cash to be seized and further investigated.

Serious Organised Crime and Police Act 2005 (SOCPA)

207. Section 98 of the Serious Organised Crime and Police Act inserted a new Section 245A into POCA which allows the Assets Recovery Agency to impose a Property Freezing Order (PFO) where there is a risk of dissipation of assets. Such orders prevent those who own potentially recoverable property from dealing with their assets in any way, while the investigation in to whether or not the property is recoverable continues. These are similar to interim receiving orders but do not require the appointment of a receiver. A similar provision exists for Scotland: a "prohibitory property order."

Police and Criminal Evidence Act 1984 (PACE)

208. If cash is being seized as *evidence* under Section 19 of PACE (which does not apply to Scotland), a police constable may, in the course of a search, seize anything if he has reasonable grounds for believing that it has been obtained in consequence of the commission of an offence or if it is evidence in relation to an offence that he is investigating. In both cases, the constable must also believe that it is necessary to seize it in order to prevent it from being concealed, lost, destroyed, etc.

Powers to identify and trace property

209. The Serious Organised Crime and Police Act 2005 (SOCPA), and POCA have introduced significant investigation powers enabling the seizure of proceeds of crime, or compelling the production of material and information which could be used in relation to proceedings for recovering the proceeds of crime. The relevant provisions of SOCPA and POCA came into force on 1 April 2006 and 24 February 2003, respectively.

Serious Organised Crime and Police Act 2005 (SOCPA)

210. *Disclosure Notice:* Sections 62 and 63 SOCPA provide for disclosure notices to be issued for disclosure of information of substantial value to an investigation into offences concerning proceeds of crime. The powers enable investigating authorities to copy or retain documents or to require a person to explain the documents.

211. *Power of entry, search and seizure:* Section 66 SOCPA provides for a power of entry, search and seizure in respect of the documents that could be covered by a disclosure notice where there has been non-compliance with a disclosure notice, or it is not practicable to give a disclosure notice, or that giving a notice might seriously prejudice the investigation.

212. *Financial Reporting Order:* Sections 76 and 77 SOCPA enable a court to issue a financial reporting order against a defendant convicted of certain offences. Such an order requires the defendant to provide financial information over a specified period.

Proceeds of Crime Act 2002 (POCA)

213. *Production Order:* Sections 345 and 380 POCA provide for production orders to be issued against persons subject to a confiscation or money laundering investigation, or in relation to property which is subject to a civil recovery investigation, requiring the recipient to provide or allow access to specified material relevant to the investigation. Sections 347 and 382 include provision to a right of entry to attach to the production order.

214. *Search and Seizure warrant:* Sections 352 and 387 POCA provide for search and seizure warrants to be issued by a judge on certain conditions in connection with confiscation, money laundering or civil recovery investigations.

215. *Disclosure Order:* Sections 357 and 391 POCA provide for disclosure orders to be granted on certain conditions in connection with confiscation or civil recovery investigations. A disclosure order requires the recipient to answer questions, provide information or produce documents.

216. *Customer Information Order:* Sections 363 and 397 POCA provide for customer information orders to be issued by a judge on certain conditions in connection with confiscation, money laundering or civil recovery investigations. A customer information order is an order that a financial institution covered by the application for the order must provide any such customer information as it has relating to the person specified in the application. Such information will include bank and personal details.

217. *Account Monitoring Order:* Sections 370 and 404 POCA provide for account monitoring orders to be issued by a judge on certain conditions in connection with confiscation, money laundering or civil recovery investigations. Such an order requires the specified financial institution, for the period stated in the order, to provide account information such as deposits and withdrawals.

218. *Letter of Request:* Section 376 POCA provides for letters of request to be issued by a judge or the Director of the Assets Recovery Agency on certain conditions to a court or authority abroad in connection with confiscation, money laundering or civil recovery investigations in the UK. This is available to other prosecutors under the Crime (International Co-operation) Act 2003 and the Criminal Justice (International Co-operation) Act 1990. In Scotland, the provisions of the Crime (International Co-operation) Act 2003 are used. This is covered in detail in section 6 of this report.

Protection of bona fide third parties

219. *Confiscation Orders:* Third parties have the right during a sentencing process to apply to the court for restitution or compensation. These issues are dealt with in advance and separately from the confiscation mater. The court can settle these disputes in advance or issue both a confiscation order and compensation order under the Powers of Criminal Courts (Sentencing) Act 2000.

220. Confiscation orders are based on the monetary value of recoverable property: they do not change the ownership of property. Confiscation orders can therefore be made that take into account assets or property belonging to genuine third parties. The court decides the rights of third parties when the confiscation order is enforced. Funds on which there is a prior lien such as orders of the court in other criminal or civil judgments are not taken into account when calculating the available amount (section 9 of POCA).

221. *Civil Recovery Orders:* Recoverable property which may be the subject of a civil recovery order does not include legitimate property transfers by a defendant to a third party. This is because transfers of property to third parties "*in good faith, for value, and without notice that it was recoverable*

property" would not constitute tainted gifts and consequently could not be taken into account in calculating the available amount. Prior liens such as orders of the court in other criminal or civil judgements relating to the defendant are also not taken into account when calculating the available amount. (Sections 9 and 308 of POCA.)

222. Section 266 POCA provides that recovery orders should not be made where a third party has received recoverable property in good faith and without notice that the property was recoverable and has since acquiring the property altered his position such that a recovery order would be detrimental to him. Section 281 POCA affords protection to victims of theft (subject to certain conditions) where they can demonstrate to the court that recoverable property belongs to them.

223. Section 283 POCA makes provision for compensation to be payable to a property owner where the court does not deem property to be recoverable where an interim receiving order had previously been in place in relation to that property.

224. *Cash forfeiture by police/HMRC:* Section 301 POCA provides that where cash had been detained under Section 295 POCA and that a third party claims that the cash belongs to him, the court can order that the cash be released. Section 302 POCA provides for compensation to the owner where detained cash is not subsequently forfeited.

225. *Terrorism Act*: Section 23 TACT makes specific provision for third parties who have the right to be heard in circumstances where they claim to be the owner or otherwise interested in anything liable to forfeiture.

Authority to void actions and contracts

226. The use and operation of POCA and its provisions are governed by, and dependent upon, due judicial process and the decisions of the appropriate courts. The courts have the legal authority and power to be able to take decisions to prevent or void actions whether contractual or otherwise as described.

Additional elements

227. POCA allows for confiscation orders to be made against companies and partnerships if they are convicted in that capacity (Parts 2, 3 and 4 of POCA). In some circumstances, the court may 'lift the corporate veil' and treat an organisation's property as being that of a convicted natural person, if the company was a sham. Civil recovery is taken against physical assets which may also be the property of organisations (Part 5 of the Act).

228. Part 5 of POCA includes a civil recovery scheme, which is operated by the Assets Recovery Agency (ARA) in England & Wales, and NI; or the Civil Recovery Unit Scotland. This scheme empowers the Director of the ARA or CRU to sue by way of civil proceedings to recover the proceeds of unlawful conduct whether or not criminal proceedings have been brought (Section 240(2) POCA). See above for more details.

229. In civil recovery proceedings, the court will consider evidence from the defendant as to the lawful origin of the property concerned (with the exception of applications made ex parte). The defendant would also have the opportunity to demonstrate the lawful origin of property within any subsequent appeal process.

Statistics on freezing, confiscation and forfeiture

230. The Joint Asset Recovery Database (JARD) was developed to provide a central repository of information covering all aspects of the asset recovery process. It encompasses cash seizure, asset restraint, criminal confiscation, civil recovery and criminal taxation cases flowing from the use of

POCA provisions. It is the central database into which all agencies deploying POCA powers feed, and it recovers data from all UK jurisdictions. JARD has been operational since 2004.

231. JARD enables financial investigators, prosecutors, and magistrates' courts across the asset recovery community to manage the end-to-end process of a case as it passes through the justice process. It is a cross-government and cross-law enforcement database. Agencies pass recovered funds to the central government, and are able to reclaim a "share" of the funds they have recovered for use in operational budgets. Access to their "share" is only valid if the relevant information has been entered on JARD; this helps to maintain up-to-date JARD statistics and improves performance management data for the whole system. JARD is administered by ARA. Monthly statistics are submitted to the Concerted Inter-Agency Criminal Finances Action Group (CICFA).

232. The tables below describe the use of restraint orders and confiscation orders under POCA. Unless otherwise specified, the data below has been extracted from JARD. JARD also records the use of confiscation orders under POCA precursor legislation (Drug Trafficking Act 1994, Criminal Justice Act 1988), as many investigations recorded were initiated pre-POCA. It will be noted that the ratio of pre-POCA orders to POCA orders is seen to decline over the period covered by these figures.

Table 1: Use of restraint and confiscation under POCA, by agency[14], financial year 2004-2005

- No of restraint orders obtained
- No of confiscation orders obtained and value of funds confiscated

Restraint Orders	Agency	No of Restraint Orders	
	HMRC/RCPO	69	
	CPS/Police E&W	118	
	CPS/NCS (SOCA)	21	
	CPS/RCPO/ RARTS	38	
	Other LE Agency E&W	0	
	Police Scotland	152	
	Scotland - Other LE Agency	0	
	DPPNI/PSNI	18	
	Total Restraint Orders (UK)	**416**	
Confiscation Orders	**Agency**	**No of confiscation orders**	**Value £**
	HMRC/RCPO	83	5,201,906
	CPS/Police E&W	1366	10,724,722
	CPS/NCS (SOCA)	12	388,266
	CPS/RCPO/ RARTS	57	1,025,856
	Other LE Agency E&W	13	872,089
	Police Scotland	14	196,074
	Scotland - Other LE Agency		
	Other LEA	15	196,657
	DPPNI/PSNI	4	117,451
	Total Orders Obtained (UK)	**1564**	**18,723,024**

[14] For ease of reference, SOCA and HMRC are included throughout these tables, although HMRC did not exist before 2005 and SOCA did not exist before 2006. There is a clear continuity between HM Customs and Excise and HMRC; and similarly between the NCIS and SOCA.

Confiscation Orders obtained under POCA precursor legislation (Drug Trafficking Act, Criminal Justice Act)	**891**	**111,135,640**
Total	**2455**	**129,858,664**

Table 2: Use of restraint and confiscation under POCA, by agency, financial year 2005-2006

- Number of restraint orders obtained
- Number of confiscation orders obtained and value of funds confiscated

Restraint Orders	Agency	No of Restraint Orders	
	HMRC/RCPO	56	
	CPS / Police E&W	377	
	CPS /NCS (SOCA)	45	
	CPS/RCPO/RARTS	41	
	Police Scotland (Inc. FCU)	213	
	PSNI /DPPNI	13	
	Other Law Enforcement (E&W & NI)	7	
	Other LEA	0	
	Total Restraint Orders (UK)	**752**	
Confiscation Orders	**Agency**	**No of confiscation orders**	**Value £**
	HMRC (Inc. RCPO)	364	9,070,142
	CPS / Police E&W	2398	22,029,248
	CPS /NCS (SOCA)	47	1,052,579
	CPS/RCPO/RARTS	106	6,844,553
	Police Scotland (Inc. FCU)	26	431,911
	PSNI /DPPNI	7	117,341
	Other Law Enforcement (E&W & NI)	42	1,822,178
	Other LEA	5	80,514
	Total Orders Obtained (UK)	**2995**	**41,448,470**
Confiscation Orders obtained under POCA precursor legislation (Drug Trafficking Act, Criminal Justice Act)		**746**	**86,345,903**
Total		**3741**	**127,794,373**

Table 3: Use of restraint and confiscation under POCA, by agency, *April – July 2006*

- No of restraint orders obtained
- No of confiscation orders obtained and value of funds confiscated

Restraint Orders	Agency	No of Restraint Orders	
	Police E&W	112	
	SOCA	0	
	RARTs	8	
	HMRC	10	
	PSNI	7	
	Police Scotland	44	
	SFO	0	

	ARA	2	
	DWP	0	
	Other LEAs (Trading Standards, Pensions Regulator, MOD, DEFRA)	0	
	Total Restraint Orders (UK)	**172**	
Confiscation Orders	**Agency**	**No of confiscation orders**	**Value £**
	Police E&W	876	11,330,686
	SOCA	6	68,286
	RARTs	46	5,105,886
	HMRC	104	2,632,340
	PSNI	2	121,348
	Police Scotland	122	3,469,739
	SFO	0	0.00
	ARA	4	706,680
	DWP	11	486,929
	Other LEAs (Trading Standards, Pensions Regulator, MOD, DEFRA, etc)	1	500
	Total Orders Obtained (UK)	**1050**	**23,922,396**
Confiscation Orders obtained under POCA precursor legislation (Drug Trafficking Act, Criminal Justice Act)		**154**	**21,477,495**
Total		**1204**	**45,399,891**

Table 4: Figures for amounts actually recovered from confiscation and forfeiture orders made, both in the criminal and civil POCA regimes:

	2004/2005	2005/2006
Criminal	(i) POCA precursor legislation: £47,504,786 (ii) POCA: £6,611,435	(i) POCA precursor legislation: £48,204,426 (ii) POCA: £19,370,941
Civil	ARA & CRU aggregate payments received: £4,371,686	2005/2006 ARA & CRU aggregate payments received: £5,011,513

Table 5: Use of POCA cash seizure powers by agency financial year 2004-2005:

- Number of detention orders granted subsequent to seizure, and value
- Number of forfeiture orders granted subsequent to detention, and value

(NB forfeiture may relate back to earlier seizures)

Cash Seized	Agency	No of Cash Detention Orders	Value £
	NCS (SOCA)	27	1,367,695
	Police E&W	548	14,828,570
	RARTs	37	2,264,117
	PSNI	22	363,422

	Police Scotland	57	1,160,538
	HMRC	684	20,591,576
	Total Cash Detained (UK)	**1375**	**40,575,921**
Cash Forfeited	**Agency**	**No of Cash Forfeiture Orders**	**Value £**
	NCS (SOCA)	13	910,327
	Police E&W	257	6,355,014
	RARTs	17	1,393,448
	Police Scotland	31	762,164
	PSNI	1	40,621
	HMRC	302	12,987,763
	Total Cash Forfeited (UK)	**621**	**22,449,340**

Table 6: Use of POCA cash seizure powers by agency financial year 2005-2006:

- Number of detention orders granted subsequent to seizure, and value
- Number of forfeiture orders granted subsequent to detention, and value

(NB forfeiture may relate back to earlier seizures)

Cash Seized	**Agency**	**No of Cash Detention Orders**	**Value £**
	NCS (SOCA)	47	3,402,655
	Police E&W	773	38,169,146
	RARTs	32	1,101,356
	PSNI	32	668,387
	Police Scotland	59	1,125,319
	HMRC	411	19,469,860
	Total Cash Detained (UK)	**1354**	**63,936,725**
Cash Forfeited	**Agency**	**No of Cash Forfeiture Orders**	**Value £**
	NCS (SOCA)	17	940,366
	Police E&W	402	10,274,059
	RARTs	13	567,467
	Police Scotland	51	749,269
	PSNI	12	200,168
	HMRC	346	18,717,791
	Total Cash Forfeited (UK)	**841**	**31,449,123**

Table 7: Use of POCA cash seizure powers by agency March – July 2006:

- No of detention orders granted subsequent to seizure, and value
- No of forfeiture orders granted subsequent to detention, and value

(NB forfeiture may relate back to earlier seizures)

Cash Seized	**Agency**	**No of Cash Detention Orders**	**Value £**
	Police E&W	0	0.00
	SOCA	38	628,577
	RARTs	4	287,627
	HMRC	138	3,622,494
	PSNI	13	137,496

	Police Scotland	10	241,114
	Total Cash Detained (UK)	**469**	**13,455,823**
Cash Seized	**Agency**	**No of Cash Forfeiture Orders**	**Value £**
	Police E&W	168	4,962,816
	SOCA	3	65,723
	RARTs	15	697,473
	HMRC	46	2,247,045
	PSNI	5	55,445
	Police Scotland	27	275,291
	Total Cash Forfeited (UK)	**264**	**8,303,795**

Table 8: HMRC statistics on cash seizures at UK frontiers (non-JARD Data)

Period	Number of seizures at frontiers (ports, airports, etc)	Value of seizures
1/4/04 – 31/3/05	1085	**£21,227,702**
1/4/05 – 31/3/06	745	**£34,358,528**

Table 9: POCA Civil Recovery Provisions: ARA & CRU (Scotland)
Financial Year 2004 – 2005

- Funds restrained pending investigation
- Civil recovery orders granted / tax assessments undertaken

Restraint Orders		**Number of restraint orders**	**Value of funds restrained**
	ARA	29	11,115,000
	CRU (Scotland)	15	Not recorded
	Total Restraint Orders (UK)	**44**	**11,115,000**
Recovery Orders/Tax Assessments		**Number of Recovery orders / Tax assessments**	**Value of funds restrained**
	ARA	13	5,614,100
	CRU (Scotland)	2	203,407
	Total Recovery Orders (UK)	**15**	**5,817,507**

Table 10: POCA Civil Recovery Provisions: ARA & CRU (Scotland)
Financial Year 2005 – 2006

- Funds restrained pending investigation
- Civil recovery orders granted / tax assessments undertaken

Restraint Orders		**Number of restraint orders**	**Value of funds restrained**
	ARA	70	49,489,235
	CRU (Scotland)	1	Not recorded
	Total Restraint Orders (UK)	**71**	**49,489,235**

Recovery Orders/Tax Assessments		**Number of Recovery orders / Tax assessments**	**Value of funds restrained**
	ARA	24	4,594,706
	CRU (Scotland)	2	761,602
	Total Recovery Orders (UK)	**26**	**5,356,308**

Table 11: Figures for amounts of recovered property shared back to law enforcement agencies are as follows:

2005/2006	
Funds obtained under POCA precursor legislation shared with law enforcement agencies	£ 42,437,071
Funds obtained under POCA shared with law enforcement agencies	£ 18,025,277
TOTAL:	**£ 60,462,348**
Amount of the shared funds provided to police forces	£ 39,000,000

2.3.2 Recommendations and Comments

233. The introduction of POCA has had a significant and positive impact on the UK's ability to restrain, confiscate and recover proceeds of crime. The provisions of the Act, particularly on the criminal confiscation side, appear to be working reasonably well in practice. The steady increase in restraint and confiscation and recovery figures, combined with positive feedback received from a range of law enforcement and prosecution agencies involved with the use of the new provisions, demonstrates an increased appreciation and understanding of the effective use of criminal confiscation to interrupt money laundering activities, as well as recover proceeds at the post-conviction stage.

234. POCA does not address the question of seizure and recovery of instrumentalities used in or intended for use in the commission of criminal offences. The courts have powers upon sentencing to make "deprivation orders", and there are various other powers scattered through individual Acts to confiscate instrumentalities depending upon the type of offence and the particular circumstances of each case. The UK should consider enacting a broad stand-alone provision enabling seizure and confiscation of instrumentalities of crime, including in cases when there has been no conviction. It is noted that legislation was recently introduced under the Criminal Justice (International Co-operation) Act 1990 (Enforcement of Overseas Forfeiture Orders) Order 2005 to give effect to *foreign* restraint and forfeiture orders for instrumentalities of crime.

235. The introduction of the civil recovery regime under POCA is another positive development in the UK regime. The ARA continues to be funded by direct vote through Parliament and has not yet reached its aim of being self-funded through its own activities in the recovery of proceeds of crime realised. The targets originally set by the ARA may have been overly optimistic. The actual realisation of funds recovered is lower than originally anticipated and the process of working through the POCA mechanisms to final forfeiture orders has taken longer than expected.

236. The use in civil recovery cases of the interim receiver as an "investigator" once appointed is a special feature of UK legislation which creates special issues of its own. Whilst this brings a degree of independence and outside expertise to the process, the ARA also loses a degree of control and direction over the process which itself becomes more fragmented. In addition, the cost of paying private sector interim receivers to run the investigation significantly impacts the overall operating costs of the ARA. The more recent introduction of freezing orders without the appointment of interim receivers may go some way to address these issues in more straightforward cases.

237. The UK authorities should review the current arrangements in civil recovery cases both at the legislative and operational level with a view to making the process more effective and timely,

including the better facilitation of international cooperation. ARA is encouraged to take a more aggressive approach in pushing litigation forward to final forfeiture orders. The assessment team notes that on 11 January 2007, the Home Office announced that it will move forward with plans to merge ARA into SOCA and to explore the possibility of extending the power to initiate civil recovery proceedings to CPS, RCPO and SFO. It is understood that subject to the necessary legislation being enacted, the ARA/SOCA merger is likely to take effect in 2008.

2.3.3 Compliance with Recommendation 3

	Rating	Summary of factors underlying rating
R.3	C	

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

2.4.1 Description and Analysis

General

238. As member of the European Union, the United Kingdom is bound by the EU freezing mechanism. The EU has adopted two Regulations and a Common Position to implement S/RES/1267(1999), its successor resolutions, and S/RES/1373(2001). These two Regulations and the Common Position lay down the basic framework for freezing of terrorist assets, but do not fully cover the two UN Security Council resolutions.

239. Freezing of terrorist assets is part of the EU Common Foreign and Security Policy (CFSP), also sometimes referred to as the second pillar. The main features are: exclusive focus on foreign policy (article 11 EU Treaty) and a unanimous decision making process. The Council of the European Union[15] ("the Council" or "the Council of Ministers") is the highest decision making authority for the CFSP. The Council is the meeting of the competent ministers of all member states. For the CFSP, the competent ministers are the ministers of Foreign Affairs.

240. The main two legal instruments used in the CFSP are the Common Position (CP) and the Regulations. The Common Position is unique to the CFSP. The Member States are required to comply with and uphold such Common Positions which have been adopted unanimously at the Council. The second legal instrument is the Regulation, used also in other policy areas. A Regulation is binding in its entirety, directly applicable in all European Union (EU) member states (Article 249 of the Treaty establishing the European Community). Regulations do not need to be implemented. This is different from EU Directives (see for example Section 3 of this Report on the EU Money Laundering Directives), that bind the Member States as to the results to be achieved and have to be transposed into the national legal framework.

241. Regulations need to be published in the Official Journal of the European Communities to be in force. Should there be a conflict between national law and a Regulation, the Regulation would have priority over national law and render it invalid. But, since the national law and the Regulation form one set of law, the national law in a specific member state can be a source of law for the interpretation of a Regulation in that member state.

242. In addition to the EU instruments, which are automatically in force in the UK, the UK incorporates its provisions (and in some cases, expands upon them), into its two main domestic provisions for implementing S/RES/1267(2001) and S/RES/1373(2002), which can be summarised as follows:

- *The Al-Qaida and the Taliban (United Nations Measures) Order 2006 (previously 2002):* This secondary legislation implements S/RES/1267 and successor resolutions in the UK. This legislation performs three main functions: (i) it implements financial restrictions in the UK against persons who have been designated under the relevant Security Council resolutions at the UN; (ii) it enforces in the UK financial restrictions against persons who have been designated under the relevant Security Council resolutions where those restrictions are implemented by the EU under EC Regulation 881/2002; and (iii) it gives the UK a power to impose financial restrictions where the UK has reasonable grounds to suspect a person is or may be designated under the relevant Security Council resolutions; a person acting on behalf

[15] The Council of the European Union should not be confused with the European Council (term used to describe the regular meetings of the Heads of State or Government of the European Union Member States) or the Council of Europe (a separate international organization based in Strasbourg of 46 member states in the European region that focuses on Human Rights, Democracy, the Rule of Law) and that also hosts Moneyval, one of the Associate Members of FATF.

or at the direction of a designated person; or a person directly or indirectly owned or controlled by a designated person.

- *The Terrorism (United Nations Measures) Order 2006 (previously 2001):* This secondary legislation implements UNSCR 1373 and successor resolutions in the UK. This legislation performs two main functions: (i) it enforces financial restrictions in the UK against individuals who have been designated at the EC under EC Regulation 2580/2001; and (ii) it gives the power to impose financial restrictions against persons who the UK has reasonable grounds to suspect are terrorists (i.e. persons who commit, attempt to commit, facilitate or participate in the commission of acts of terrorism); persons acting on behalf of or at the direction of terrorists; or persons directly or indirectly controlled or owned by terrorists.

UK processes for asset freezing

243. Co-ordination across relevant departments and agencies is ensured through the meetings of: the Asset Freezing Working Group (AFWG), the Terrorist Finance Action Group ("TFAG"), both chaired by HMT, and the Special Cases Oversight Board ("SCOB") which is chaired by the Home Office and which coordinates the handling of a variety of measures in relation to certain "special cases" which may include proposing that asset freezing measures be pursued. See the discussion under Recommendation 31 for more for a more thorough description of AFWG and TFAG.

Procedures for implementing S/RES/1267(1999) and successor resolutions

244. The Al-Qaida and Taliban (United Nations Measures) Order 2006 came into force on 16 November 2006 (updating and replacing a similar order from 2002). The Order prohibits dealing with funds and economic resources (see scope of "funds" and "economic resources" below) that belong to, or are owned or held by a designated person, any person owned or controlled, directly or indirectly by a designated person, or any person acting on behalf or at the direction of a designated person.

245. To "Deal with" is broadly and comprehensively defined to include (for "funds") to "use, alter, move allow access to or transfer; deal with in any other way that would result in any change in volume, amount location, ownership, possession, character or destination, or make any other change that would enable use." For economic resources, this includes "use to obtain funds, goods, or services in any way, including (but not limited to) by selling, hiring or mortgaging the resources."

246. A "designated person" is also broadly defined and includes:

- a person who is made subject to financial restrictions imposed under S/RES/1267(1999) and successor resolutions;
- a person acting on behalf of or at the direction of the designated person;
- a person owned or controlled, directly or indirectly, by the designated person; or
- a person whom HMT has reasonable grounds to suspect of falling in one of these categories.

247. Council Regulation 881/2002 also prohibits directly or indirectly making any funds or economic resources available to or for the benefit of designated persons, and granting, selling, supplying or transferring technical advice, assistance or training related to military activities (article 3). An asset freeze imposed under the Order (which incorporates asset freezes imposed by the directly applicable Council Regulation 881/2002) applies from the date on which the UN, EC or HMT makes the person subject to financial restrictions. Therefore the asset freeze is imposed without prior notice to the designated person.

248. Failure to abide by an asset freeze under the Order is a criminal offence with a maximum penalty on conviction of seven years imprisonment and an unlimited fine.

249. The 2006 Order includes transitional provisions relating to asset freezes imposed under the Al-Qaida and Taliban (United Nations Measures) Order 2002. Those which give effect to a UN decision now have effect under the 2006 Order.

250. In the EU context, Regulation 881/2002 (27 May 2002) imposes specific restrictive measures directed against certain persons and entities associated with Usama bin Laden, the Al-Qaida network and the Taliban and orders the freezing of all funds and economic resources belonging to, owned or held by, a natural or legal person, group or entity designated by the United Nations 1267 Sanctions Committee (i.e. persons and entities linked to Usama bin Laden, the Al-Qaida network and the Taliban) in all member states of the EU. While Regulation 881/2002 does not require the freezing of funds that are controlled by designated persons or persons acting on their behalf or at their direction, as required by the FATF Recommendations, this deficiency is adequately addressed by the national system—Al-Qaida and Taliban (United Nations Measures) Order 2006 as described above.

251. Any designation by the UN is immediately followed by an amendment of the list annexed to Regulation 881/2002 and is directly applicable in the entire EU. Regulation 881/2002 requires that freezing action must occur without delay and without giving prior notice to the persons concerned.

252. The Bank of England, as HMT's agent on asset freezing, is responsible for issuing notices with respect to persons designated under S/RES/1267 and its successors at the UN. The Bank's standard practice is to issue a news release drawing attention to the listing of any individual by the United Nations on the same day that the listing was identified. The Bank's procedure is to check the UN website each morning. In the event that a name had been added, a news release drawing attention to the listing is prepared and agreed for publication on the same day. The Bank's consolidated list of financial restrictions targets is updated and published at the same time as the news release. These procedures would normally mean that publication of a name by the UN in New York would be drawn to the attention of financial institutions in the UK on the next working day (bearing in mind the time difference between New York and London).

Procedures for implementing S/RES/1373(2001)

253. With regard to the freezing of the assets of terrorists and terrorist entities resulting from S/RES/1373(2001), Council Regulation 2580/2001 of 27 December 2001 on specific restrictive measures directed against certain persons and entities with a view to combating terrorism, creates a mechanism similar to that of Regulation 881/2002 by instituting an obligation to freeze the assets of the natural or legal persons, groups or entities, as defined in resolution S/RES/1373(2001).

254. Since S/RES/1373(2001) does not create a list of person or entities to be frozen (in contrast to S/RES/1267(1999)), a list of persons and entities concerned is drawn up by the Council. Any EU member state can submit to the Council a request to list an entity, as can any other non-EU jurisdiction through the President of the Council. Article 2 of Regulation 2580/2001 states that the Council, acting by unanimity, shall establish, review and amend the list of persons, groups and entities to which the Regulation applies, in accordance with the provisions of the Common Position 2001/931/CFSP.

255. Article 1(4) of the Common Position states that a list should be drawn up on the basis of precise information or material in the relevant file which indicates that a decision has been taken by a competent authority, irrespective of whether it concerns the instigation of investigations or prosecution for a terrorist act, an attempt to perpetrate, participate in or facilitate such an act based on serious and credible evidence or clues, or condemnation for such deeds. The actual list of entities is an annex to Common Position 2001/931/CFSP.

256. The list is divided into two parts. Since listing is undertaken under the CFSP, a listing of an entity needs to have an external link (outside the territory of the EU). Entities with an external link are designated and have to be frozen. Entities without external link (the internal list) bear an asterisk (*) with their name on the list. Internal entities are only subject to intensified police- and judicial co-

operation and not to freezing. The exact criteria to designate as internal or external are confidential. Any designation (internal or external) by the Council is immediately followed by an amendment of the list annexed to Common Position 2001/931/CFSP and is directly applicable in the entire EU. Regulation 2580/2001 requires that freezing action must occur without delay and without giving prior notice to the persons concerned.

257. The list drawn up by the Council mentions (1) natural persons who commit or attempt to commit terrorist acts or who participate in or facilitate the commission of terrorist acts; (2) legal persons, groups or entities that commit or attempt to commit terrorist acts or that participate in or facilitate the commission of such acts; (3) legal persons, groups and entities owned or controlled directly or indirectly by one or more natural or legal persons referred to at points (1) and (2); and (4) persons, groups and entities acting on behalf of or under the direction of one or more persons, groups or entities referred to at points (1) and (2). The notion of control of a legal person, group or entity is defined at Article 1 of the Regulation.

258. Supplementing the European system, the UK's domestic measures allow for an even broader range of designations and freezing of assets. The Terrorism (United Nations Measures) Order 2006 came into force on 12 October 2006. An asset freeze under the Order prohibits the acts of: dealing with funds (which includes financial assets) and economic resources (i.e. other assets of every kind) that belong to or are owned or held by a designated person or terrorist, and/or making funds and economic resources available to a designated person or terrorist. The Order 2006 includes the Council Regulation designations but also expands upon it because it also allows for domestic (UK) designations without having to be approved by the EU system, and including EU "internals" (whose assets are not frozen within the EU system but rather only subject to intensified monitoring). A "designated person" includes:

- a person designated at the EC level under Regulation (EC) 2580/2001;
- a person designated by HMT on reasonable grounds to suspect he is or may be:
  - a person who commits, attempts to commit, participates in or facilitates the commission of acts of terrorism;
  - a person identified in a Council Decision (i.e. designated at the EC level);
  - a person owned or controlled, directly or indirectly, by a designated person; or
  - a person acting on behalf of or at the direction of a designated person.

259. An asset freeze imposed under the Order applies from the date on which the EC or HMT makes the person subject to financial sanctions. Therefore, the asset freeze is imposed without prior notice to the designated person.

260. Failure to abide by an asset freeze under the Order is a criminal offence with a maximum penalty on conviction of seven years imprisonment and an unlimited fine. The UK's procedures allow it to take asset freezing action very quickly, e.g. on the advice of the police or the Security Service, helping to prevent asset flight and maximise the operational benefits of the action. The UK's procedures are as follows:

- The referring body (e.g. the police or Security Services) submit a draft statement of case to the Asset Freezing Working Group (or to Treasury officials when there isn't time for a full AFWG meeting) setting out the case for asset freezing action.
- The Group reviews the statement of case and requests further evidence where necessary. At this point, the group checks whether there is any additional evidence available that would either strengthen or challenge the recommendation to take action.
- If the group is satisfied that the statement of case is complete and meets the requirements under the Terrorism (United Nations Measures) Order 2006, Treasury officials submit advice to the relevant HMT Minister.

- If the Minister approves the asset freeze, then the Treasury instructs the Bank of England to notify the freeze to financial institutions and other parties.
- Currently, the targets of restrictions are informed by the institution holding their funds of the asset freeze against them. However, whenever the 2006 Order is used, the Treasury will write to individuals informing them of the freeze when they are designated.
- Asset freezes are kept under review by the Treasury to check whether the justification for the freeze remains. Individuals are also able to request a review of an asset freeze against them. There is judicial oversight of the system since the imposition of an asset freeze may be challenged before the courts either under the Terrorism Order or under general legal principles such as the principle that the Governments' administrative actions can be challenged before the courts.

261. In contrast with past experience, when the Treasury only designated persons on the basis of open source evidence, Treasury Ministers have decided to use closed source evidence (i.e. classified material) in those cases where there is a strong operational and evidential basis for action and where there is insufficient open source material to meet the legal test for designation. Closed source material has recently been used as the basis for continuing the freezes against some of the 19 terror suspects whose assets were frozen in August 2006. The careful use of closed source material, with proper judicial safeguards, will further strengthen the UK's asset freezing regime.

262. The UK has used the powers available under the Terrorism (United Nations Measures) Order 2001 (and now the 2006 Order) on a number of occasions to take rapid asset freezing action against suspected terrorists. This includes four individuals suspected of carrying out the attempted London tube bombings of 21 July 2005, as well as 19 individuals arrested in August 2006 in connection with the alleged plot to blow up airplanes leaving the UK.

Case Study: Asset Freezes of 11 August 2006

263. On 10 August 2006, the police arrested 24 individuals in connection with an alleged terror plot to blow up planes leaving the UK in mid-flight. Given the security assessment that a terrorist attack could be imminent, the police requested rapid asset freezing action in relation to 19 of the individuals to prevent the risk of assets being diverted to associates. On the basis of police advice, the Chancellor agreed to freeze the assets of the 19 individuals, and a notice to this effect was published on the Bank of England website in the early hours of 11 August – less than 24 hours after the arrests and before bank opening hours the next day. The police confirmed that in terms of immobilising assets the freezing action was extremely beneficial to this particular counter – terrorist operation.

264. In view of the early timing of the freeze and the ongoing investigations into the alleged plot, the UK authorities have kept these 19 asset freezes under close review. In particular, authorities have re-examined cases where individuals have subsequently been released without charge.

Examining and giving effect to freezing mechanisms of other jurisdictions

265. The UK authorities can examine and, if appropriate, give effect to designations under freezing mechanisms of other jurisdictions. A jurisdiction may ask the UK to impose an asset freeze using HMT's power to make a direction to that effect under the Terrorism (United Nations Measures) Order 2006 (implementing S/RES/1373(2001)). The UK will consider (in practice through an AFWG meeting) whether the request and any additional information available provide grounds for the UK to impose an asset freeze under that power. AFWG will put any recommendations for an asset freeze to HMT Ministers, who may decide that HMT should direct that the assets freeze is imposed. The asset freeze will take effect from the date of the direction.

266. However, if the requesting jurisdiction is another EU Member State, that jurisdiction may consider putting the proposal for an asset freeze to the EC who may impose an asset freeze across all

EC Member States under a Regulation. As any such legislation is directly applicable, the asset freeze would take effect in the UK from the date on which the EC legislation comes into force.

267. Asset freezing action in another jurisdiction may also give UK law enforcement agencies information suggesting that an offence under sections 15 to 18 of the Terrorism Act 2000 (i.e. offences of raising or using funds for the purposes of terrorism) may have been committed. The relevant UK law enforcement agencies may, in the course of investigate such an offence, apply to the Court for a restraining order which can have the effect of freezing the alleged terrorist property. The Court may grant a restraining order in relation to funds that it considers may be forfeited during the criminal proceedings for the substantive offence.

268. The UK has also used evidence provided by another country to support a domestic designation. For example, HMT imposed an asset freeze on an individual on the basis of information provided by another country in 2001. In theory, the designation process need take no more than a day. If a statement of case was received that was considered to meet the requirements of the legislation, and was sufficiently urgent, then it could be put up to Ministers for approval immediately, and the relevant Bank of England notices prepared immediately thereafter. In practice, other considerations such as foreign policy issues or law enforcement investigations might need to be weighed up in the decision making process: exactly what these considerations are varies on a case by case basis.

Definition of funds

269. The term "funds" is broadly defined (with the UK's Al-Qaida and Taliban (United Nations Measures) Order 2006 and the Terrorism (United Nations Measures) Order 2006 using the same language of Council Regulation 881/2002) to include: "financial assets and economic benefits of every kind, including but not limited to cash, cheques, claims on money, drafts, money orders and other payment instruments; deposits with financial institutions or other entities, balances on accounts, debts and debt obligations; public and privately traded securities and debt instruments, including stocks and shares, certificates presenting securities, bonds, notes, warrants, debentures, derivatives contracts; interest, dividends or other income on or value accruing from or generated by assets; credit, right of set-off, guarantees, performance bonds or other financial commitments; letters of credit, bills of lading, bills of sale; documents evidencing an interest in funds or financial resources, and any other instrument of export-financing". The term "economic resources" covers "assets of every kind, whether tangible or intangible, movable or immovable, which are not funds but can be used to obtain funds, goods or services".

270. The asset freezes described in the Al-Qaida and Taliban (United Nations Measures) Order 2006 and the Terrorism (United Nations Measures) Order 2006 apply to all funds and economic resources held belonging to, owned or held by:

(1) any person who commits, attempts, to commit, participates in or facilitates the commission of acts of terrorism;
(2) any designated person;
(3) any person owned or controlled, directly or indirectly by any designated person or any person who commits, attempts, to commit, participates in or facilitates the commission of acts of terrorism; or
(4) any person acting on behalf of or at the direction of any designated person or any person who commits, attempts, to commit, participates in or facilitates the commission of acts of terrorism.

271. Therefore, the asset freeze will, for example, prohibit the sale (except under licence) of a house or the use of funds in a joint account if that house or account is jointly owned by a designated person and a non-designated person.

Restrictions on the payment of household benefits

272. The Economic Secretary to the Treasury announced to Parliament in July 2006 that the Government was introducing restrictions on the payment of state benefits to the households of UN listed terror suspects. As set out in the Minister's statement, this has been done to meet the requirement in UN Security Council Resolution 1390 (2002) that funds, financial assets or economic resources are not made available, directly or indirectly, for the benefit of a listed person. The Government has decided that, given the fact that household income is generally pooled, state benefits paid to individuals sharing the same household with a listed person would be, directly or indirectly, for the listed person's benefit and should therefore be subject to appropriate restrictions and conditions and procedures.

273. The following procedures are applied to state benefits paid to a household which includes a listed person, or to which a listed person is attached:

- When a person is listed, state benefit payments are suspended pending the granting of a licence by the Treasury;
- Licences are issued by the Treasury in accordance with legal obligations. Where licensed payments are approved, the Treasury applies appropriate detailed safeguards to ensure that surplus funds are not made available to the listed person. These safeguards are assessed on a case-by-case basis on the basis of risk.

274. This procedure is currently applied to benefits paid to five spouses of listed persons, and in one case to benefits paid to a listed person himself. In four of these cases, on the basis of a risk assessment, the Government has decided to apply "higher risk" safeguards whereby benefits are paid into an account held at the Office of the Paymaster General and the onward disbursement of funds is controlled to protect against the risk of diversion and to ensure that all licensing conditions are complied with.

275. Three of the spouses affected by these procedures have launched judicial review proceedings against the Government. On 22 September 2006, the High Court ruled that the Government's policy of restricting benefit payments to the spouses of listed persons was lawful and was consistent with the requirements of the UN Resolution. The applicants appealed against this decision at the Court of Appeal, the case was heard in December 2006 and judgment is awaited.

System for communicating actions to the financial sector

276. The Bank of England maintains a comprehensive list of all persons subject to asset freezing measures under UK law. This list is immediately updated when changes are made to add, amend or delete information on those persons, regardless of whether that change is made by the UN, EC, UK or concerns additional information provided by another jurisdiction. The Bank also provides a subscriber service that immediately notifies subscribers of changes to the list. Currently, there are 2,500 subscribers to this service. The Bank draws attention to changes in the list through the publication of press notices and, where appropriate, Bank Notices.

277. The information provided by the Bank is publicly available through either a request to the Bank or through the internet. The list, press notices and Bank Notices are published on the Bank of England's website: www.bankofengland.co.uk. Between January and August 2006, there were on average 246,325 'hits' per month on the Bank of England's financial sanctions website. In August 2006, when a number of persons had their assets frozen in connection with an alleged plot to bomb commercial aircraft leaving the UK, the number of hits went up to 580,235.

278. The Bank also acts as a contact point for questions concerning asset freezing action. The Bank, the FSA and the Treasury have regular contact with the financial sector. The financial sector has

indicated that there is widespread awareness of the information the Bank of England provides on financial sanctions.

Guidance to financial institutions and DNFBPs

279. The Bank of England makes available on its website up-to-date guidance on the operation of asset freezes, including guidance on the obligations of persons who hold funds or economic resources that are subject to an asset freeze. That guidance makes it clear that queries concerning asset freezes, such as questions about the identity of designated people and the procedures for applying for licences, can be addressed to the Bank.

280. Industry guidance for financial institutions provided by the JMLSG (cf Section 3, below) also includes a specific section on financial sanctions and asset freezing and the obligation on financial institutions to comply with such measures. Some industry bodies have also provided guidance, often in consultation with the relevant authorities. For example, the Law Society (of which every English and Welsh solicitor must be a member) provides guidance on the financial sanctions mechanisms.

281. While, as noted above, communication between the authorities and the financial sector is comprehensive, systematic outreach and guidance to DNFBPs could be more proactive, as it depends to some extent on DNFPB taking the initiative themselves (e.g. by becoming a subscriber to the website).

282. In order to mitigate this, the BoE has also made presentations through its outreach programme to raise the aware of financial sanctions with the major professional bodies, for them in turn to pass the message on to their members. SOCA Terrorist Finance Team (TFT) has also explicitly raised awareness of the BoE list amongst DNFBPs as part of its general outreach on terrorist finance issues. For DNFPB, while there are provisions in the JMLSG regarding terrorist financing, these need to be built out some more to enhance guidance in this area, particularly concerning the application of financial sanctions. However, there is evidence of compliance: some of the alerts received by the Bank in relation to frozen funds have come from DNFBPs as a result of positive checks against CFT lists. The TFT has also processed SARs from DNFBPs that were triggered by information presented on the Bank's consolidated list of designated persons.

Mechanisms for de-listing, unfreezing, and challenging measures in court

283. There are several mechanisms to notifying individuals about de-listing and unfreezing procedures:

- The Orders specifically provide the procedure by which a person affected by an asset freeze can challenge that asset freeze before the Courts.
- The FCO writes to persons designated at the UN or the EU informing them of their listing and the de-listing procedures.
- from November 2006, HMT began issuing letters for domestic designations in the same way the FCO does for international designations (this was previously done by the institution who had taken the decision to freeze the particular funds or economic resources).
- BoE Notices advising of the imposition of an asset freeze contain advice on how the imposition of that asset freeze can be challenged.
- BoE's webpages on financial sanctions are being updated and will include guidance on de-listing procedures.
- BoE's Financial Sanctions Unit has a general role in answering queries, including questions about de-listing procedures.

284. In addition, HMT does not rely on individuals challenging their own designation. It keeps all asset freezes under review and re-examines cases as and when new information emerges. For

example, HMT has done this with regard to several of the individuals whose assets were frozen on 11 August 2006.

285. The competent authorities ensure that the legal framework and identifying information required for assets to be frozen are kept up to date and publicly available. This includes immediate updates if a person is no longer to be included on the list of restrictions targets published by the BoE.

286. It is the responsibility of the private sector or benefit paying authority to search for and freeze affected assets, and the onus is on them to assess whether the freeze applies in the particular case. If they are unsure whether certain funds ought to be frozen, they will consult with the BoE's Financial Sanctions Unit. This service is offered by the Bank explicitly to help prevent the application of a freeze to the wrong person. The Bank has a well-developed network of government and law enforcement contacts to enable it to de-conflict false matches.

287. A financial institution (or any other entity) that had wrongly or inadvertently frozen assets, would in theory immediately unfreeze them on discovery of the mistake, since there would be no legal basis for freezing those assets. To the knowledge of the UK authorities, this has never arisen in practice.

288. A person affected by an asset freeze may challenge that before the Courts under the specific procedure provided in the Orders or under general legal principles (e.g. under private laws such as laws for the enforcement of a contract or under administrative laws such as the laws that administrative actions can be challenged before the courts by persons affected by those actions).

289. Under the EU system, natural and legal persons have to right of direct access to the EU Court of First Instance to appeal against acts of Community institutions (addressed to them or directly concerning them as individuals) or against a failure to act on the part of those institutions. This applies to the two EU freezing Regulations. Additionally, UK courts can ask the EU Court of Justice for preliminary rulings to seek clarification of the Community rules and even though these requests are made by a national court, parties concerned may take part in the proceedings before the Court of Justice. Entities have (unsuccessfully) challenged their designations before the EU Court of First Instance.

290. It is not common for UK asset freezes to be challenged. However, there is one current case of an individual challenging an asset freeze under administrative laws. That case is stayed pending parallel proceedings before the European Court of Justice.

Authorising access to funds for certain expenses

291. Regulation 881/2002 is amended by Regulation 561/2003 of 27 March 2003, as regards exceptions to the freezing of funds and economic resources. As a result, Regulation 881/2002 allows for an exception, upon a request made by an interested natural or legal person, to the national competent authority, for certain types of funds and economic resources with the approval of the Sanctions Committee. These provisions are consistent with the Security Council resolutions (S/RES/1452(2002).

292. The Al-Qaida and Taliban (United Nations Measures) Order 2006 allows HMT to authorise acts that are otherwise prohibited under the asset freeze (e.g. the act of making funds available to a person acting on behalf of a designated person). HMT will consider authorisation on the basis of the exemptions set out in UNSCR 1452 and the equivalent provisions in the relevant EC and UK legislation (i.e. Council Regulation 881/2002 and the Al-Qaida and Taliban (United Nations Measures) Order 2006).

293. The procedure for granting such authorisations is as follows. The person who wishes to undertake the prohibited act applies (either to the BoE or HMT) for a licence. The person is asked to

provide all information that is relevant to his application. HMT considers the application for a licence and decisions on individual licence applications are taken at Ministerial level, generally by the Economic Secretary to the Treasury. If HMT concludes that a licence should be granted, it will ask the FCO to seek the requisite approval of the UN Al-Qaida and Taliban Sanctions committee.

294. Council Regulation 881/2002 (as enforced in the UK through the Al-Qaida and Taliban (United Nations Measures) Order 2006) exempts from the effect of the asset freeze: payments of interest or other earnings on frozen funds so long as the payment is then frozen, and payments of otherwise frozen funds that due under contracts, agreements or obligations that arose prior to the date on which the funds or economic resource became subject to the asset freeze.

295. The UK has been active in implementing its procedures to ensure that persons designated internationally or domestically are able to access basic expenses and, where appropriate, extraordinary expenses. For 2005 and 2006, the following licences have been issued under the Al Qaida and Taliban (Untied Nations Measures) Order 2002, as replaced by the Al-Qaida and Taliban (United Nations Measures) Order 2006.

- 21 Licences for legal expenses or legal aid;
- 25 Licences for basic expenses;
- 0 licences for extraordinary expenses.

Freezing, Seizing and Confiscation in other circumstances

296. There are other financial powers available to UK law enforcement and other UK authorities under the Terrorism Act 2000, the Anti-terrorism Crime and Security Act 2001 and the Proceeds of Crime Act 2002.

297. *Terrorism Act 2000 (TACT).* This legislation: makes it unlawful to raise or use funds for the purposes of terrorism; enables the courts to prohibit dealing with terrorist funds at the start of a criminal investigation; and enables the court to order the forfeiture of terrorist funds.

298. *Anti-terrorism, Crime and Security Act 2001 (ATCS):* This legislation allows: (i) HMT to freeze assets of governments or residents of other countries where there are reasonable grounds to suspect the government or resident poses a threat to the UK economy or the lives or property of UK nationals or residents; and (ii) empowers an authorised officer would seize any cash if he has reasonable grounds for suspecting that it is terrorist cash (i.e. funds that are intended to be used for terrorist purposes, consists of resources of a proscribed organisation and property that is earmarked as terrorist property); forfeiture of seized terrorist cash must be decided by the courts.

299. *The Proceeds of Crime Act 2002 (POCA):* POCA consolidated, updated and reformed previous UK legislation relating to money laundering in the context of the recovery of illegally obtained assets more generally. The legislation covers all criminal property. It criminalises all forms of money laundering and creates offences where someone fails to report a suspicion of money laundering. It also establishes the ARA to recover criminal assets.

300. Figures for the amounts of money frozen, seized and confiscated under terrorism-related powers since 2001:

- £440,000 of cash seizures (28 seizures) under ATCS;
- £650,000 of funds seized under the Proceeds of Crime Act – this is solely terrorist-related money seized under the Act;
- Additionally, around £500,000 of terrorist assets is currently frozen in the UK under the 2006 Orders or the preceding Orders;

- £78m assets belonging to the former Taliban Government of Afghanistan were frozen under the first piece of domestic legislation relating to UNSCR 1267 (since replaced) – these funds were released in 2002 in accordance with UNSC agreements.

Protection of bona fide third parties

301. Freezing of funds, other financial assets and economic resources, in good faith that such action is in accordance with Council Regulation 881/2002, shall not involve the natural or legal person, group or entity implementing it, or its directors or employees, in liability of any kind unless it is proved that the freezing was due to negligence (article 6).

302. The focus is on ensuring that the asset freeze is only applied to the appropriate funds and economic resources. It is the institution holding the funds or economic resource which must decide whether the asset freeze applies to those particular funds or economic resources. An institution can seek further information from the BoE in order to reach that decision.

303. This process, that aims to ensure that the asset freezing only applies to appropriate funds and economic resources, has meant that there have not been any cases in which bona fides third parties have brought proceedings to allege that their rights have been undermined by the mistaken imposition of an asset freeze.

304. In the case of asset freezes concerning Al-Qaida and the Taliban, Article 6 of the directly applicable EC legislation (i.e. Council Regulation 881/2002) provides an indemnity. However, in the case of asset freezes concerning other terrorists, there is no indemnity in the relevant EC legislation (i.e. Council Regulation 2580/2001).

305. The scope for HMT to grant licences that permit acts otherwise prohibited by the asset freeze and the scope to challenge asset freezing in court (described above) is also relevant to this point.

Monitoring compliance with freezing obligations

306. Regulation 881/2002 obliges member states to lay down rules on sanctions applicable to infringements of the provisions of this Regulation and ensure that they are implemented. Those sanctions must be effective, proportionate and dissuasive (article 10 of the Preamble). Regulation 2580/2001 obliges member states to lay down rules on sanctions applicable to infringements of the provisions of this Regulation and ensure that they are implemented. Those sanctions must be effective, proportionate and dissuasive (article 12 of the Preamble).

307. Both the Al-Qaida and Taliban (United Nations Measures) Order 2006 and the Terrorism (United Nations Measures) Order 2006 require bodies such as financial institutions to inform HMT or the BoE as soon as is reasonably practicable if they know or suspect that a person with whom they have dealings (including former customers) is subject to an asset freeze or has breached an asset freeze. Failure to comply with this requirement is a criminal offence with a maximum penalty on conviction of 6 months imprisonment and a fine of up to £5,000.

308. The Orders also allow HMT (and, in practice, the BoE) to require from any person in or resident of the UK information or documents for certain purposes including securing compliance with the Orders and obtaining evidence of the commission of an offence under the Orders. Other than privileged legal advice, restrictions on information sharing (e.g. a confidentiality agreement) do not apply for the purposes of responding to such requests. It is a criminal offence to fail to respond to a request without reasonable excuse, to give false information, to wilfully obstruct or to evade the provision of information. The maximum penalty on conviction for any such offence is two years imprisonment and an unlimited fine.

309. Financial institutions' compliance with financial restrictions legislation is covered as part of the FSA's supervisory approach to assess systems and controls in relation to AML/CFT. Guidance on sanction compliance issues is provided within the ARROW AML/CFT guidance to FSA supervisors. In an ARROW risk assessment, assessing compliance with SR III obligations will be covered as part of reviewing the firm's procedures for vetting customers against sanctions, OFAC and PEP lists, mainly because these issues are relevant to customer take-on, transaction monitoring, as well as firms obligations under SYSC 3.2.6 R. These issues will also be covered as part of the ARROW risk assessment interviews with relevant staff within the firm.

310. Supervisors will in the first instance discuss what arrangements are in place, whether any sanction breaches have occurred, and what the firm did in response. Reviews conducted by the Risk Review Department of firms' AML/CFT systems and controls, whether as a result of an ARROW risk assessment or thematic work, will cover the procedures firms have in place to screen clients and payments against sanctions lists. This typically involves gathering information on the frequency and coverage of such checks - for example how often is the entire client base or perhaps a proportion of it screened, how often are sanctions lists held by firms updated, how are false positives cleared and genuine "hits" followed up, how is the process quality assured.

311. In addition, the FSA has also conducted a number of thematic studies e.g. AML/CFT systems and controls in small financial advisers and compliance standards in venture capital firms, which have assessed the effectiveness of AML/CFT standards within firms, including compliance with sanctions lists.

312. FSA supervision does not extend to DNFBPs unless they carry out a FSMA-related activity. Where a supervisor does exist then it should look at this issue for the particular DNFPB it supervises. However, professional bodies in the UK may not be so well equipped to monitor compliance with financial sanctions regimes.

Additional elements

Facilitating communication and co-operation with foreign governments and international institutions

313. The UK is playing an active role in facilitating communication and co-operation with foreign governments and international institutions. The main points to note here are that: the UK works with its EU partners and wider members of the international community to ensure that the maximum amount of supporting and identifying information is included in any designation; the UK works with its EU partners and wider members of the international community to proactively identify and then target terrorist assets; and where the UK intends to propose someone for designation at the international level relevant countries are pre – notified to prevent asset flight.

Ensuring thorough follow-up investigation, co-operation with law enforcement, intelligence and security authorities, and appropriate feedback to the private sector

314. Information from asset freezes is passed from the financial sector to law enforcement and intelligence agencies via the BoE. The sharing of information is dealt with in accordance with relevant reporting and disclosure requirements. This flow of information works very effectively and has allowed the police and the UK FIU to conduct further analysis that supports investigations and informs preventative strategies for the UK financial sector.

315. A particularly important relationship is that which exists between the BoE and NTFIU. The Bank routinely contacts NTFIU in order to clarify identification details of targets or to pass on a query or piece of information from the financial services sector, or to alert them to a breach of an assets freeze. Similarly, NTFIU refers to the Bank to check whether persons under investigation or have been subject to an assets freeze.

Access to assets frozen pursuant to S/RES/1373(2001)

316. Under Article 5 of Council Regulation 2580/2001, the countries may on occasion and under such conditions as it deems appropriate in order to prevent the financing of acts of terrorism, authorise the use of frozen funds to meet essential human needs (food, medicine, rent, etc.) and to pay taxes, compulsory insurance premiums, utility fees and charges due to a financial institution for the maintenance of accounts.

317. The Terrorism (United Nations Measures) Order 2006 allows HMT to authorise acts otherwise prohibited under the Order (e.g. making funds available to a designated person or allowing the payment of otherwise frozen funds that are due under a contract agreed before the asset freeze was imposed). HMT will consider authorisations on the basis of the exemptions set out in UNSCR 1452 and the equivalent provisions in the relevant EC Regulations.

318. Council Regulation 2580/2001 (as enforced by the Terrorism (United Nations Measures) Order 2006) exempts from the effect of the asset freeze payments of interest on frozen accounts so long as any such payments are then frozen.

319. The procedure for granting such authorisations is as follows. The person who wishes to undertake the prohibited act applies (either to the Bank of England or HMT) for a licence. The person is asked to provide all information that is relevant to his application. HMT considers that application for a licence. If HMT concludes that a licence should be granted, it will ask the Foreign and Commonwealth Office to notify the EC.

320. HMT has recently issued legal expenses licences for the 19 individuals who were designated on 11 August 2006. For 2005 and 2006 (up to November) the following licences have been issued under the Terrorism (United Nations Measures) Order 2001, as replaced by the Terrorism (United Nations Measures) Order 2006.

- 22 Licences for legal expenses or legal aid
- 1 licence for other basic expenses
- 0 licences for extraordinary expenses.

Statistics

321. The Bank of England database shows that the equivalent of **US$ 921,393** has been frozen. This amount is held across **188** accounts. The UK authorities state that it is normal policy only to release aggregate data on assets frozen under the Orders.

322. The UK earlier froze 78 million pounds sterling of the former Taliban Government of Afghanistan. The frozen funds were released in 2002 once the relevant names were taken off the target list by the UN Sanctions Committee.

2.4.2 Recommendations and Comments

323. The UK has established a terrorist asset freezing regime which works well in practice. It has an effective domestic designation process which appears rapid, easy and efficient. The system can operate independently of the UN and EU listing mechanisms, where necessary.

324. The Al-Qaida and the Taliban (United Nations Measures) Order and the Terrorism (United Nations Measures) Order have recently been updated to improve their efficiency and effectiveness, indicating a proactive approach by the authorities. Events within the UK have demonstrated a clear need for the provision and on-going maintenance of such effective measures and the UK authorities have responded well to the challenge.

325. The BoE maintains a website for communication purposes, and the Bank, the FSA and HMT have regular contact with the financial sector thereby enhancing communication capabilities. Likewise, financial institutions' compliance with the financial sanctions regime is covered as part of the FSA's supervisory approach to assess systems and controls, but this does not extend to DNFPB unless they carry out a FSMA-regulated activity. Systematic outreach to DNFBPs should be made more proactive. The UK should enhance its communication, guidance and compliance monitoring efforts for DNFBPs.

2.4.3 Compliance with Special Recommendation III

	Rating	Summary of factors underlying rating
SR.III	C	

Authorities

2.5 The Financial Intelligence Unit and its functions (R.26, 30 & 32)

2.5.1 Description and Analysis

326. The functions of the UK FIU (receiving, analysing, and disseminating reports relating to money laundering) were first carried out in 1992 by the Economic Crime Unit (ECU) within the National Criminal Intelligence Service (NCIS).

327. On 1 April 2006, the Serious Organised and Police Act 2005 (SOCPA) created the Serious Organised Crime Agency (SOCA). On the same day, NCIS ceased to exist and SOCA subsumed its functions and resources. Accordingly, the functions of the UK FIU are now within SOCA, and SOCA is responsible for performance management of this unit.

328. POCA 2002 (as amended by section 104 of SOCPA 2005) and the Terrorism Act (TACT) 2000 (as amended by the TACT 2006) require persons within the regulated sector to make disclosures in the form of suspicious activity reports (SARs)[16] to SOCA when they know or suspect, or have reasonable grounds to know or suspect, that another is engaged in money laundering / terrorist financing. A specific operational division, the Proceeds of Crime Department, has been set up within SOCA to take this forward; the **UK FIU** sits within the Proceeds of Crime Department. While the law indicates that SARs come to SOCA in general, internal policies and procedures ensure that they come directly to UK FIU, and are processed, analysed and disseminated solely by UK FIU staff.

329. The legislation also requires persons in the non-regulated sector to make disclosures in the form of SARs to a Constable, Customs Officer, or SOCA, when they know or suspect that another is engaged in money laundering / FT. Through UK FIU outreach ("dialogue team", presentations, seminars, etc) it has become accepted best practice that all disclosures from the non-regulated sector should be made to SOCA. SOCPA gives SOCA powers and functions that are pertinent to its responsibility for the FIU: the prevention and detection of serious organised crime; the mitigation of the consequences of such crime; and gathering, storing, analysing and disseminating information.

330. In March 2006, the recommendations of a SARs review (full title: the "Review of the Suspicious Activity Reports Regime" a.k.a. "the Lander Review") were accepted by the Government, and the report was made publicly available. There are 24 recommendations in the report together with an implementation timetable spanning from March 2006 to October 2007.

"Consent"

331. "Consent" is a statutory mechanism whereby reporting entities that are themselves concerned not to commit a suspected money laundering offence, notify the UK FIU and seek permission to proceed with the identified activity if it involves an amount over £250 (SOCPA, Section 103). All SARs seeking "consent" to continue with identified suspicious activity are individually analysed (by checking in criminal databases) and disseminated as appropriate to law enforcement agencies, where advice is sought as to the importance of stopping that particular transaction or activity.

332. In terms of when consent is granted or not, there are often compelling operational reasons to give consent in order to further an investigation. The need to undertake a cash seizure being a prime example of such. Other examples would include the need to evidence or follow a money trail, the need to avoid alerting a suspect to an investigation, the requirement to manage the risk of harm to the reporter. Similarly, where there is no extant investigation, the granting of consent does not preclude

[16] The UK uses the term "SARs" rather than "STRs" as the Proceeds of Crime Act 2002 requires disclosure of suspicious activity rather than specific transactions, such as arrangements to launder money whether or not any transactions have been conducted.

an investigation commencing. It may not be necessary or proportionate to refuse consent to a specific transaction but the information contained within a consent SAR may give rise to a subsequent investigation.

333. The legislation in POCA 2002 allows the authorities seven working days to grant or refuse consent for the reporting sector to carry out a prohibited act. If the UK FIU grants permission to continue the transaction, the reporting entity has a statutory defence to any subsequent charge of money laundering. The reporting entities indicate that, from the moment after a SAR has been filed, the reporting entity has the duty to monitor all the transactions carried on by the same customer, being ready to seek the consent again in all cases that could seem very similar to those for which consent has already been granted. Some financial institutions interpret the current requirement as indicating that they must seek consent on *all* transactions above the threshold from the same customer once a SAR has been filed on that customer.

334. If consent is refused, then law enforcement authorities have 31 days to investigate and, when considered necessary, seek a restraining order against the assets; if no such action is taken by the relevant agency to "protect" the criminal property by the end of 31 days, the disclosing institution is deemed to have the appropriate consent.

335. The theory behind the consent process is that, in cases where a transaction has not been completed, it provides the legal tools to actually prevent movement of potentially criminal funds. However, there are concerns with regard to the effectiveness and workability of the current consent process, especially with regard to consent for all follow-up transactions. In fact, the threshold of £250 seems to be too low and represents a burden for the reporting entities, which is often interpreted as the need to seek consent in most or all subsequent transactions from the same customer. The law provides, however, that a deposit-taking body may ask the UK FIU to vary the threshold amount to any amount above £250. To date, the UK FIU has received only 20 such requests to vary the threshold level. There is also an additional burden placed on SOCA by having to respond to additional consent requests which in many cases may not be useful. Furthermore, the UK authorities were not able to provide statistics on what happened after the 31 days of moratorium period, which could better explain if the refusals of consent have led to a restraint order against the assets or not. These statistics could be helpful to show the effectiveness and workability of the whole consent procedure.

SARs analysis and dissemination

336. The amount of SARs analysed by the UK FIU is small compared to the amount of SARs received; however, the UK FIU seeks to analyse and disseminate SARs which have the greatest impact on reducing risk to the UK or to reduce harm. Almost all SARs received are made available to law enforcement and other end users for end-user analysis. The SARs Control team generally receives and processes SARs, and uses specific search parameters to sort them into certain categories (FT, Professional Standards, etc., as described below) for analysis by specific FIU teams. The teams use further search parameters, data mining, research of other databases, and analytical tools such as link software during their analysis.

337. The FIU is authorised to disseminate financial information to domestic authorities for investigation or action when there are grounds to suspect ML or FT. UK FIU may disseminate information to:

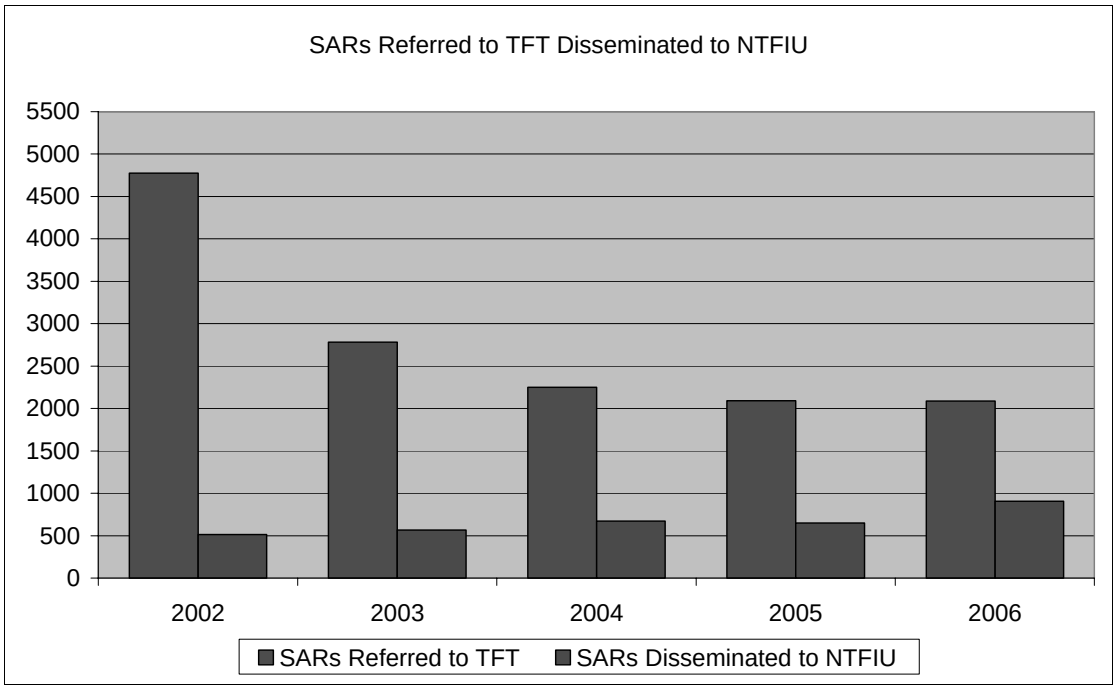
(a) UK Police Forces;
(b) Law Enforcement Agencies;
(c) Such other persons as it considers appropriate in connection with the prevention, detection, investigation or prosecution of offences, or the reduction of crime in other ways or the mitigation of its consequences (including agencies discharging these functions overseas)

Consent SARs:

338. SARs relating to consent are individually analysed by the Consent Team; analysis consists of checking in criminal databases and liaising with law enforcement. So far in 2006 (up to November), the UK FIU has received and analysed approximately 780 such SARs per month and on average actioned them within 2.5 working days. Consent requests are generally disseminated directly to the relevant law enforcement agency, due to the necessary time delay in the process for replicating information on the database and the time frame set by the legislation for responding to consent requests. For the year 2006 to end of September, 67% of all consent disclosures were referred to partner agencies as providing possible opportunities for intervention and/or for their advice on the consent decision. In 2005 approximately, 66% of the 9,514 consent disclosures were analysed and disseminated to partner law enforcement agencies for consideration. For 2005, 8% of consent requests were refused; for 2006 (up to 1 December), 17% were refused. As noted above, consent is sometimes granted where criminality is suspected or known, for operational reasons (e.g. keeping an investigation covert or tracking the movement of the money).

Terrorism and terrorist financing-related SARs:

339. All SARs relating to suspected terrorist financing, whether reported under TACT or POCA, are individually analysed by the Terrorist Financing Team (TFT), and if appropriate, disseminated to the National Terrorist Finance Investigation Unit (NTFIU). The TFT produced a CFT Bulletin on the SARs received, analysed and disseminated to the NTFIU during 2005: 2,091 SARs were accepted into the TFT for analysis; 649 were passed to NTFIU for further development. During 2006, 2,089 SARS were accepted into the TFT for analysis; 907 were passed to the NTFIU for further development.



Clustering projects /strategic analysis:

340. The UK FIU's Intelligence Team also uses a combination of analytical techniques to identify groups of SARs connected by related subjects ("clusters") in specific time periods. These clusters often identify links between persons in the same organised crime grouping or relate to the same crime; many of these relationships would not be visible to the end users without prolonged research. Visual

representation of these clusters allows the FIU to identify key subjects and SARs and identify potential tactical opportunities and leads for law enforcement that might otherwise be missed. A recent example was a comprehensive piece of research of SAR records on Chinese organised crime in the UK.

341. These clustering projects are taken on pursuant to the FIU's own exercises to link SARs; priorities relating to risks identified in the National Intelligence Requirement (NIR), derived from the threats identified in the UK Threat Assessment (UKTA); and pursuant to law enforcement requests. With regard to this last area, agencies that may have additional local/specific priorities, for example: on organised crime amongst particular communities for the Metropolitan Police.

342. For law enforcement requests, the results of the research are evaluated for relevancy and the extent of analysis will vary according to the request and the FIU remit. For instance, SAR information may be cross referenced with other information to produce Intelligence Reports for a particular agency to action further or simply a list of evaluated SARs will be made available to the relevant agency to conduct their own further analysis.

HMRC:

343. There is also a dedicated HMRC team attached to the FIU that leads on evaluating, analysing, and disseminating SARs related to tax evasion, tax credit fraud, VAT fraud, excise fraud, money laundering, cash/foreign currency intelligence, arms proliferation and MSB regulations to appropriate HMRC investigation teams. The FIU has a system whereby target reports are produced by automated searching of Elmer to identify VAT fraud SARs on a daily basis. In the last two years, 16,834 SARs have been disseminated to HMRC tax investigators. Due to the slower nature of tax investigation, only 247 cases have so far been notified to HMRC where a yield has been achieved. Ultimately, the total from the 16,834 referrals is expected to be considerably higher. The total yield from these 247 cases is just under £7.5m, with an average yield of £30k per case.

Professional Standards SARs:

344. All law enforcement agencies have their own "Professional Standards Department" (actual titles vary) that exclusively investigates that agency's officers and staff when intelligence or complaints warrant such an investigation. The UK FIU "SAR Control" team identifies and disseminates SARs that relate to professional standards issues, using an automated report run against the ELMER database every 24 hours analysing data fields for key words in SARs that may be pertinent, followed by manual analysis to corroborate or rule out a professional standards issue.

345. SARs relating to such investigations or providing the initial intelligence impetus for such investigations are separately analysed. Where further action is necessary, the relevant LEA professional standards department will be contacted to establish interest and full dissemination may occur. Between May and August 2006, the SAR Control team has analysed approximately 5,700 SARs. Of these 160 have provoked further interest and 71 have been formally disseminated to relevant professional standards units or departments.

Direct Elmer access by LEAs:

346. Beginning in May 2005, the UK FIU made available a restricted view (approximately 93% of the 820,000) of its SAR database (ELMER) via Moneyweb (described below). There is a seven-day delay between the receipt of SARs onto the full ELMER database and when they are made available on ELMER via Moneyweb, in order to allow sufficient time for UK FIU officers to ensure that particularly sensitive SARs have been filtered (SARs relating to terrorism for example are not released onto Moneyweb, nor are those relating to corruption and SARs / STRs received from foreign FIUs).

347. All appropriately trained and authorised law enforcement officers can access the database via this site. Access to Moneyweb is administered by designated "Points of Contact" (SPOCs); at least one SPOC per agency must be a senior officer. There are currently 1,417 officers with access to Moneyweb. Law enforcement use a variety of search criteria to interrogate the database and analyse SARs themselves, conducting their own analyses of SARs that are of particular interest to that law enforcement agency or police region.

348. The UK FIU takes responsibility for carrying out searches on the full database on request (according to strict criteria) where the requesting agency believes that information may be held on the full database which is relevant to an investigation. Between April 2005 and May 2006, the FIU received and actioned 1,084 such requests.

349. This system ensures maximum dissemination of SAR data to the law enforcement community; financial intelligence is available to add value in terms of new investigations and supporting existing investigations.

Guidance on reporting, SAR forms, and reporting procedures

350. In order to provide guidance to all reporting parties on the use of these methods, SOCA publishes comprehensive guidance on its own website, and within the other sites mentioned above. See http://www.soca.gov.uk/financialIntel/formsGuide.html. The SOCA website also has a preferred form for electronic submission of suspicious activity reports and guidance on completion and submission, including SARs seeking consent. See http://www.soca.gov.uk/financialIntel/disclosure.html. The UK has five methods of reporting:

- **"MoneyWeb" Extranet Site**: A secure extranet system for electronic reporting and submission of SARs for businesses who report 250+ a year.
- **Secure (Encrypted) Email**: A secure email system for the electronic reporting and submission of SARs for major reporters (typically high street banks, Western Union etc.). Users have encrypted email to send SARs directly into, and receive responses from, the UK FIU SARs ("ELMER") database. The SARs are in an agreed format that the ELMER database can process automatically. In order to achieve a secure connection, a valid and authorised digital encryption certificate must be placed on the client's computer or computer system. Emails from users to and from the ELMER database are digitally signed and encrypted.
- **SAR Online:** Secure web based reporting/submission system for users not on MoneyWeb, and who typically submit less than 250+ a year (website reference: http://www.ukciu.gov.uk).
- **The use of data on CD Roms and/or computer disks:** Some organisations' IT systems prohibit encrypted email traffic as it contravenes their IT security policy. In cases such as these, these organisations can output their disclosures to a disk or CD Rom in an agreed format (word template or .csv file) that can be loaded directly on to the ELMER database. ELMER reference numbers are returned to the source for their information.
- **Hard copy submission:** Postal or fax submission of typed or handwritten SARs using copies of the SOCA Preferred Form, letter, or firm's own version of SAR.

351. Guidance is communicated through frequent dialogue with the reporting sectors (including DNFBP and SROs) via meetings, presentations and telephone calls. In addition, many reporting sectors' industry guidance (including the JMLSG) contains UK FIU-approved information on reporting methods and completion. The UK FIU "Consent" team routinely provides tailored advice to persons making a SAR on matters connected with carrying out a prohibited act.

352. For sensitive topics, material is shared with a specially "vetted" group of industry representatives. The group comprises representatives from both the industry and law enforcement sectors with government security clearance who can receive and add their expert knowledge to intelligence relating to AML activity from sensitive sources and can provide external input into

current SOCA operational cases and intelligence assessments drawing on a mix of wider-ranging skills and experiences found within the group. Their principal purpose is to act as an advisory group to consider whether particular SOCA intelligence is of practical use to those in the financial sector and to consider how it can be sanitised to protect relevant sources but still sufficiently detailed to be of practical value to the financial sectors. The group also provides an effective forum for SOCA to discuss and advise on any guidance and policy decisions prior to them being released into the public domain to ensure that they are strategically and operationally acceptable to the sectors.

Access to additional information

353. The UK has direct and indirect access to additional financial, administrative, and law enforcement information. For example, the UK FIU has *direct* access to a number of domestic law enforcement sources, in particular: two other SOCA intelligence databases, the Police National Computer (*effectively a database of all criminal convictions in the UK*), JARD (*The asset recovery database*), and the Egmont Secure Web (ESW). There are no time constraints in relation to the FIU's utilisation of these sources.

354. The FIU also subscribes to a wide range of commercial databases and open sources, for example: World Check, GB Accelerator, TV Licensing, credit reference agencies, Telephone Directory Enquiries, Dunn & Bradstreet companies data, and Factiva (a media website collating open source reporting). The FIU also has *indirect* access to operational, regulatory, and public record information maintained by other agencies: Interpol; HMRC databases; HM Prison Service; Department for Work and Pensions (*distributor of social security payments*); Land Registry; Companies House; Charity Commission; Driver Vehicle Licensing Authority; Local Authorities; UK Passport Agency; and the Public Records Office.

355. Indirect access is made by means of a formal request to the third party to access information held by them. These requests are usually made to government departments or agencies, for example to request for tax details from HMRC. The requests are usually made using a standard written template to ensure legal requirements such as obligations under the Data Protection Act are met. While the FIU reports that the information request for searches of databases are never refused, it is not clear that access to the information that the FIU obtains indirectly (i.e., those databases for which it must file a request with another agency) is always timely. The FIU should consider more direct and timely access to information in order to assist in its SARs analysis.

356. The UK FIU can also request additional information from reporting parties on individual SARs. This is especially the case where consent is sought; the FIU regularly liaises with reporting parties for additional details in these cases since the FIU must then determine whether or not to grant such consent for the transaction to continue.

357. To seek additional information not directly relating to a specific event or transaction mentioned in the SAR would require a court order. The financial investigators within the FIU (currently four with 11 in training) are authorised under POCA to seek further information via production orders; however, this authority has never been used by the UK FIU so far. Current policy is to pass this work to SOCA operational teams and other law enforcement agencies, as specialists in evidence-gathering investigative work. The possibility to go back to the institutions appears somewhat constrained by this provision as, looking at the broader field of the international co-operation, it can often happen that the foreign FIU needs to obtain more general information on the customer's profile, which could include his other relations with the reporting entity or different banking operations.

Operational independence

358. As described above, the UK FIU is a part of SOCA. POCA (as amended by SOCPA 2005) stipulates that the regulated sector must submit their SARs to SOCA. SOCA is authorised to receive, analyse, and disseminate them by virtue of POCA, TACT, and SOCPA 2005. As indicated above,

these functions are carried out by an operational branch within SOCA that for reasons of convenience is referred to as the UK FIU to distinguish it from other SOCA functions.

359. SOCA is an Executive Non-Departmental Public Body sponsored by, but operationally independent from, the Home Office. SOCA's operational objectives are transparent and appear as a public document in its Annual Plan on its website. SOCA's responsibilities towards the UK FIU are also transparent by means of the Government-approved, publicly available SARs Review and the decisions of the SARs Committee.

360. The UK FIU has its own management structure which reports to the Board of SOCA. It therefore appears to be sufficiently operationally independent. Only UK FIU staff receive and analyse SARs. The head of the FIU determines when to disseminate financial intelligence and signs MOUs with foreign FIUs. While the funding for the FIU is within SOCA's budget and controlled by HMT, the FIU can make specific requests. This transparency and operational independence appears to ensure that UK FIU public aims are not undermined by undue influence or interference, including competing demands from elsewhere within SOCA.

Protection of Information

361. Section 3 of SOCPA 2005 gives SOCA (and thus also the UK FIU) the function of gathering, storing, analysing and disseminating information. Sections 33 and 34 of this Act, establish gateways for SOCA to receive information from and share information with, a wide range of partners in pursuit of its functions. The definitions in SOCPA of those partners include all law enforcement agencies (LEAs), government departments and regulators, as well as agencies discharging the same functions overseas (Section 3).

362. On receipt by the UK FIU, all SARs are subject to a "restricted" security classification under the UK Government Protective Marking Scheme that governs the physical handling, storage and dissemination of SARs and is understood by all public sector officials and law enforcement officers. SARs are stored in the SARs Database (ELMER) which is held by SOCA on a Secure Government Site on an approved protectively marked network.

363. Access to the SARs data is restricted to authorised personnel who must hold an appropriate Security Clearance and have access to an authorised terminal (located within a secure room) or via secure infrastructure to PCs with an authorised certificate. Authorised users must also hold a current SARs "account" with a unique user name and password for additional authentication. Access to the database servers is further restricted to authorised SOCA personnel. The use of the SARs database is audited in line with SOCA Professional Standards Unit Policies and all records are stored in line with the UK Data Protection Act.

364. All SOCA staff are security cleared to at least "Security Check (SC)" level in accordance with the Statement of HM Government's Vetting Policy. Security in SOCA is governed by the Manual of Protective Security issued by the Cabinet Office. All SOCA staff are subject to the SOCA Statement of Values and Code of Professional Standards. This means that UK FIU staff maintain a high level of integrity in order to minimise the risk of inappropriate use of FIU information. All UK FIU staff are annually assessed on their adherence to stated SOCA values including integrity.

365. Access to ELMER via Moneyweb is restricted to those persons who have been appropriately trained (there are more than 1,000 trained users). Access is governed by a Partnership Agreement, which details the terms of reference for access, handling, and confidentiality. All end users accept obligations of confidentiality in the handling of SARs as a condition of access to the database. The use of SARs by end users is governed by the terms of the Home Office Circular 53/2005. All breaches of SAR confidentiality notified to SOCA are investigated thoroughly and expeditiously with the relevant end user.

366. The inputting of SARs data is outsourced to a private company. This company signed a contract to take all measures necessary to comply with the provisions of any security that may be applicable. UK FIU staff briefed the company about security requirements. Company staff may not make any public statement relating to the existence or performance of the contract without prior approval from SOCA.

Public reports

367. The UK FIU has not released public reports that would include statistics, typologies and trends, as well as information regarding its activities. However, the SARs Review recommended that the UK FIU should produce an annual report on SAR statistics, and this will also be a legal requirement under the Third Money Laundering Directive.

368. UK FIU statistics, trends, and typologies on money laundering and the proceeds of crime inform MLAC and are available through the HMT website in electronic form as minutes of MLAC meetings. There are also sanitised examples in the AML strategy document available on the HMT website (www.hm-treasury.gov.uk). The SOCA website contains sanitised case studies on how the use of SARs has contributed to investigations, as an indicative guide for reporting sectors.

369. SOCA is also responsible for producing the annual UK Threat Assessment (UKTA) which is a public document available through the SOCA website (www.soca.gov.uk), and to which the UK FIU contributes information on money laundering.

370. Presentations delivered to the reporting sectors on both AML and CFT are regularly reported in the media, and on professional bodies' websites and in publications. SOCA (and NCIS) senior management have written media articles and briefings for journals.

371. Trends and typologies are distributed to law enforcement bodies, government departments and regulators. Government departments and law enforcement receive classified problem profiles and typologies; regulators receive both classified and sanitised material as appropriate; and the reporting sectors receive sanitised typologies on a variety of relevant topics; however, these are not public. With reference to CFT, periodic bulletins are presented to the financial sector at meetings, conferences, and seminars; and electronically through the Moneyweb system. In 2005 four profiles produced on CFT typologies were placed on the Moneyweb site restricted to viewing by law enforcement and authorised reporting sector subscribers.

The Egmont Group

372. The UK FIU was a founding member of the Egmont Group and granted full membership status in June 1995. In accordance with Egmont practice, when SOCA took on FIU responsibilities for the UK, it was required to complete a formal application for Egmont recognition. The SOCA submission was assessed by members of the Egmont Legal Working Group in June 2006, who confirmed SOCA's UK FIU Egmont status. UK FIU is also a participant in FIU.net and the FIU.net Task Force.

373. The UK FIU has regard to the Egmont Group Statement of Purpose and its Principles for Information Exchange Between Financial Intelligence Units for Money Laundering Cases. UK FIU carries out the day to day business of discharging the FIU role, responding to requests from Egmont FIUs and transmitting requests on behalf of UK law enforcement partners to foreign FIUs. There is a dedicated International Team within the UK FIU that works on exchanging information, researching databases, and producing assessed reports.

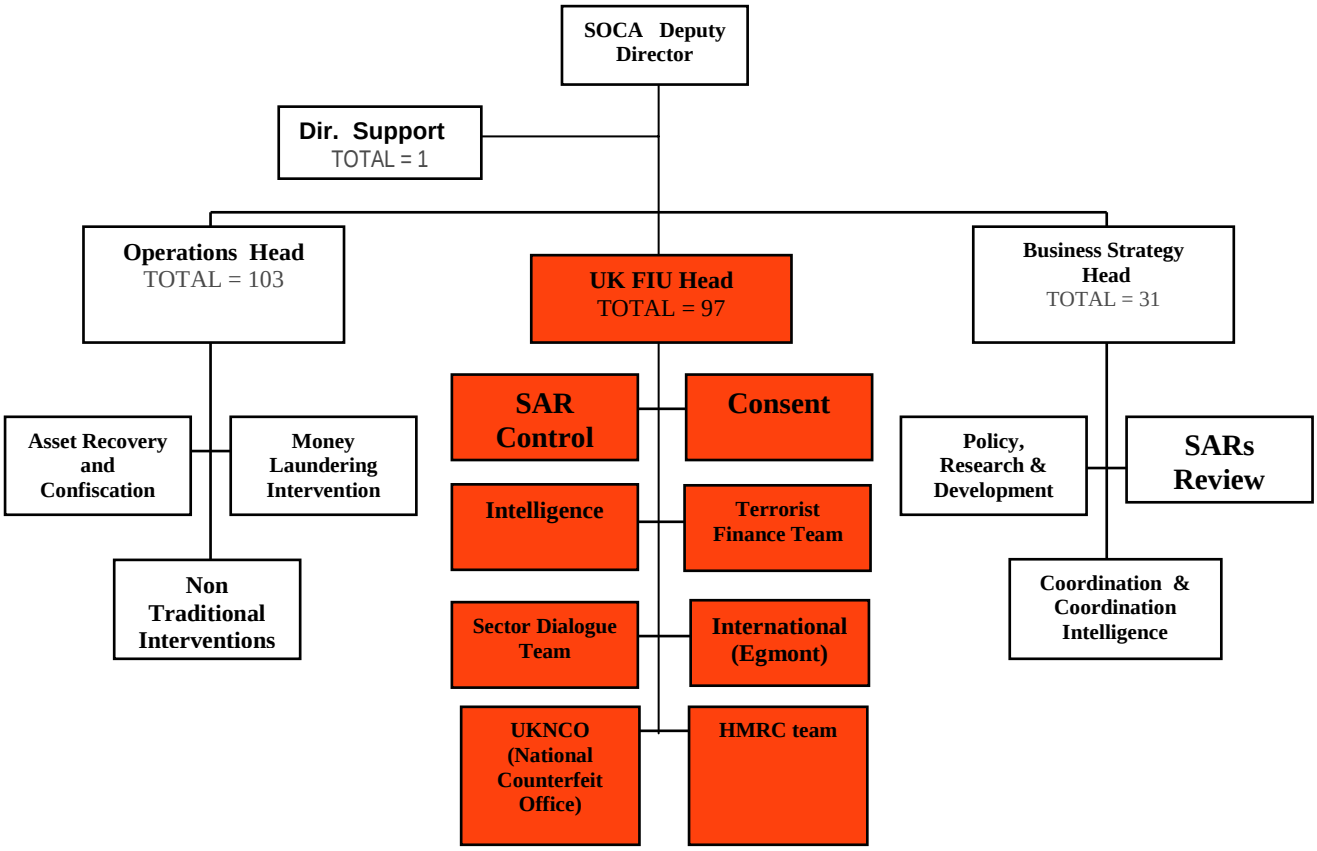
374. All disseminations of information to Egmont partner FIUs are via the Egmont Secure Website system. This system is used daily for the purposes of sharing intelligence with Egmont counterparts. Due consideration is given to the Statement of Purpose and the Principles for Information Exchange between Financial Intelligence Units for Money Laundering Cases. In accordance with the Statement

of Purpose, the UK FIU does not forward any information supplied to it by a partner FIU without seeking prior consent. Any information belonging to an Egmont partner that is passed to a UK LEA is done so on the understanding that it is for intelligence purposes only.

FIU structure, resources, integrity standards and training[17]

375. As indicated earlier, the UK FIU is located administratively within the Proceeds of Crime Branch of SOCA.

Proceeds of Crime branch (total number of staff 321) including UK FIU (total staff 97)



376. The goals and functions of the various departments are as follows:

- *SAR Administration and Control:* Managing the SAR regime and processing Suspicious Activity Reports (SARs) from the reporting sector; maintaining control of the supporting IT; best practice for ELMER use and ELMER feedback; responding to CPIA and evidential obligations.
- *Consent:* Collection, collation and dissemination of consent derived intelligence, working in partnership with LEA and the reporting sector to ensure best practice; developing the use of consent within LEAs and the reporting sector as an intervention tool.
- *Dialogue:* providing the interface between the UK FIU and the operational stakeholders in the SAR regime including the reporting sector, regulators and SARs end users; provide individual feedback to stakeholders on SARs reporting standards and activity and feedback from stakeholders to the UK FIU.

[17] As related to Recommendation 30; see Section 7.1 for the compliance rating for this Recommendation.

- *Intelligence:* Pro-actively analysing SAR-derived intelligence for the purposes of strategic and tactical assessments; maintaining an overall view of the UK anti-money laundering picture in order to provide a context for the exploitation of SARs.
- *International:* Meeting the international obligations of the UK FIU to the Egmont Group and other FIUs through the provision of financial intelligence upon request, both for UK LEAs and for international partners.
- *Terrorist Finance Team and PEPs*: Continuing the specialised approach to terrorist finance-related SARs by pro-actively analysing SAR derived intelligence. The team develops relationships with intelligence agencies and the reporting sectors in this discrete area of work. It is located in secure accommodation with access to appropriate secure communications and has access to current terrorism intelligence databases. Within this secure location, there is also a "PEPs team" responsible for receiving, analysing and disseminating SARs relevant to PEPs matters, international corruption and issues relating to WMD.
- *UKNCO:* The central UK office for all matters relating to counterfeit currency and protected coins.

377. In 2005, the Economic Crime Unit in NCIS had 80 directly employed staff plus some external contractors and attachments from other agencies. The staff costs in 2005-06 were £3.2 million plus £0.5 million in additional running costs. UK FIU within SOCA now has 97 staff and plans to increase this to 200 directly employed staff plus external contractors (bringing to total to 219) during 2006-07 at a cost of about £7 million. The planned staff increase is welcome and it is strongly recommended that the UK FIU follow through with these plans. Staff should in particular be increased in the Intelligence Team to enable the FIU to conduct more pro-active and comprehensive analytical work of SARs.

378. The FIU's budget for IT has also been increasing. In 2005-06, NCIS spent about £1 million on funding the development of the SARs database, whereas in 2006-07 SOCA will spend about £4 million with a further £2.5 million the following year.

379. UK FIU staff are required to maintain high professional standards, including standards concerning confidentiality, and are required to be of high integrity and appropriately skilled. All staff are security vetted to the most suitable level, which also includes checks on personal and financial details. (See paragraphs 361- 366 under "Protection of Information" above for more details).

380. Staff are trained in the following issues at the induction stage: the Data Protection Act, ECHR and Human Rights Act, security issues; money laundering legislation, and the role of the reporting sector, law enforcement, and others; confidentiality of SARs; ELMER database & bespoke data-mining tools. More detailed or specialised training is available later on as appropriate on: the Police National Computer; SOCA intelligence databases; Criminal Procedures and Investigation Act 1996 (CPIA); ARA financial investigator courses; CASS Business School degree in AML. In addition, Knowledge Seminars are provided to enhance understanding of wider SOCA theatres of operation. For example in August 2006 staff attended a lecture by an external expert on the misuse of trusts.

381. Courses offered to more experienced staff and provided by the International Compliance Training School (ICT) cover a wide range of subjects and include: an **AML Certificate, where** students study *inter alia*, the regulatory environment; relationship with regulators; role of the compliance officer; key compliance issues, and understanding financial crime and money laundering; and an AML **Diploma**, which is jointly awarded with the British Bankers Association and in association with the University of Manchester Business School.

Statistics

382. The FIU maintains statistics of SARs received, SARs received by the FIU, including a breakdown of the type of financial institution, DNFBP, or other business or person making the STR. (See section 3.7 of this report for these statistics.) The SARs Review recommended that the UK FIU

should produce an annual report on SAR statistics, and this will also be a legal requirement under the Third Money Laundering Directive. The report will include the annual statistics that are already routinely published (as above) but will also cover: the number of cases investigated across UK; the number of prosecutions; the number of convictions; breaches of confidentiality; property frozen; property seized and property confiscated. The first such report will be published in October 2007 and on an annual basis after that.

383. The FIU does not maintain specific statistics on all the SARs it analyses and disseminates. The FIU retains partial statistics—i.e., those analysed and disseminated relating to terrorism/terrorist financing and SARs seeking consent. Otherwise, SARs are data-mined, evaluated for relevance to the research, and may under go further analysis dependent upon the objective. In addition, UK officials also indicate that most of the SAR database, by being available directly to law enforcement, is automatically "disseminated" to those agencies for analysis and action.

Additional elements

384. Law enforcement agencies have provided feedback on the use of SARs during investigations. However, precise figures on the number of SARs in not available in any standardised format.

2.5.2 Recommendations and Comments

385. Overall, the UK FIU substantially meets the criteria of Recommendation 26 and appears to be a generally effective FIU. The private sector also reported improved relations and co-operation since the transfer of the FIU responsibilities to SOCA in March 2006. However, the UK FIU should increase its analytical capabilities, in order to maintain its role as the national center for receiving, analysing and disseminating SARS, as well as its expertise in analysing and developing ML/FT typologies. In this respect, the UK FIU should continue to increase its staff, especially its analytical staff in the Intelligence Team and other teams, in line with the objective set out in the SARs ("Lander") review.

386. The effectiveness of the current system, especially the burden on available resources, is impeded by the current consent process, especially as regards "follow-up" consent requests (i.e., the requirement for reporting institutions to ask for consent, and for the UK FIU to respond, on each transaction above 250 pounds after a first SAR has been filed for the same customer). The UK authorities should continue to work with the private sector to develop a more workable and efficient system; the revised UK AML Strategy published in February 2007 announced that the Home Office will publish a Consultation Paper in relation to the UK consent regime, based on initial proposals put forward by the UK FIU. The UK FIU should be given more timely and direct access to a number of databases (such as the Public Record's office, the Companies House, and the Land Registry) in order to increase its analytical abilities. The UK FIU should continue to ensure that its functions and authorities remain fully independent from the non-FIU functions carried out by the other parts of SOCA. Finally, the FIU should keep more comprehensive statistics on the total number of SARs analysed and disseminated.

2.5.3 Compliance with Recommendation 26

	Rating	Summary of factors relevant to s.2.5 underlying overall rating
R.26	**LC**	• There are concerns with regard to the effectiveness and workability of the current consent process, especially with regard to what is often interpreted as consent for follow-up transactions from the same customer. • The FIU does not conduct sufficient pro-active analysis on SARs; overly relying on individual LEAs to conduct their own analysis could reduce the importance of the UK FIU as the national center for receiving, analysing, and disseminating SARs; and could ultimately impede the FIU's analytical functions and its own ability to give guidance and to develop its expertise

		about ML/FT methods, trends and typologies. • The FIU does not publish periodic reports including SARs statistics, typologies and trends as well as information regarding its activities.

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 & 32)

2.6.1 Description and Analysis

Recommendation 27

387. All law enforcement agencies, including: all UK police forces, SOCA, HMRC, and SCDEA have responsibility for ensuring that money laundering offences are investigated, and have permanent specialist financial crime teams available for such investigations. All law enforcement agencies have a dedicated financial intelligence unit for assessing SARs disseminated by the UK FIU and analysis of other financial intelligence. In some cases, regional FIUs are part of the financial investigation unit / economic crime unit that carries out financial investigations for that force or agency.

388. ACPO and the National Centre for Policing Excellence have released new guidance for the investigation of Proceeds of Crime. This guidance is intended to help Forces build upon existing Economic Crime structures and processes to improve the exploitation of AML and Proceeds of Crime at every level of policing. Eight Police Command Units (Local Commands covering populations of 150,000-300,000 people) have been selected to pilot the new guidance. The programme, led by a senior police officer with extensive economic crime experience will report back to the Home Office and CICFA in 2007. This will be followed by a national roll out of the procedures and processes that have proven most effective.

389. For the financial year 2006/2007, the Home Secretary introduced a new "Statutory Performance Indicator" for police forces in England and Wales on the recovery of proceeds of crime: the value of cash forfeiture orders and confiscation orders per 1,000 population will form part of the performance against funding data for police forces that is reviewed by central government.

Investigation of terrorist financing

390. National Terrorist Finance Investigation Unit (NTFIU) is the lead authority for the investigation of terrorist financing in the UK, although individual forces also undertake such investigations when relevant or appropriate. NTFIU relies on CPS, PPSNI, or COPFS to take forward prosecutions.

Authority to wave or postpone arrest/seizure

391. An investigator can arrest a person at any time when he has reasonable grounds to suspect the person has committed an offence. It is a matter for the investigator when to arrest any suspect, the decision would be subject to an overall investigation strategy that considers a range of factors, for example: flight risk of the suspect, threats to life, removal of assets from UK, the existence of an audit trail for assets, availability of suitable resources etc.

392. With regards to postponing the seizure of money, this would be an investigating team's decision based on a range of factors (as above) but may also include the amount of money involved and the nature of the investigation. Any decision not to seize funds would be formally risk assessed by the investigation team, and may be subject to senior level approval.

Additional elements

393. There are a wide variety of special investigative techniques that can be applied to a number of offences and are not specific to money laundering. These include the possibility to use controlled delivery, conduct undercover operations, deploy informants, intercept communications, conduct surveillance, trespass onto and interfere with property, granting immunity from prosecution, access to

special procedure material. Guidance is available for law enforcement on investigative techniques such as controlled deliveries and the use of undercover officers.

394. SOCPA Sections 62 and 66, also provide for new powers: Disclosure Notices, and related additional powers of entry, search, and seizure (see criterion 3.4 above).

395. Law enforcement agencies regularly use the full range of special investigative powers in the investigation of ML and FT and predicate offences. A clearly delineated and accredited body of "financial investigators" exists in the UK and the majority of UK police forces are moving away from the traditional 'fraud investigation' model towards specialist Economic Crime or Financial Investigation Units specifically tasked with an anti-money laundering remit. These units are the centre for each force in relation to expertise concentrating solely on confiscation and forfeiture of assets and the use of all POCA powers.

396. The Government has also set up five multi-agency Regional Asset Recovery Teams (RARTs) in England and Wales. A RART is a joint agency team with staff from the police, HMRC, SOCA, ARA, and CPS co-located in one team. The teams are dedicated to confiscating criminal assets, dismantling organised crime groups and tackling money laundering.

397. The possibility of entering into "Joint Investigation Teams" (JITS) with other EU jurisdictions exists under EU law. This allows officers from one jurisdiction to investigate offences with officers of another jurisdiction.

398. ML and FT methods, trends and techniques analysis is produced by and available within the UK FIU, and is circulated for review to UK law enforcement agencies and competent authorities.

399. Since the enactment of POCA, law enforcement agencies have had different experiences of prosecuting offences. The decisions of the courts have a huge significance for actual practice. These changes are circulated by a number of ad hoc "regional financial investigation working group" meetings; however there are also formalised structures including: (1) a CICFA newsletter (more on this at section 6.1 below); (2) the Financial Investigator Support System (FISS) website (www.fiss.gov.uk/ara - password restricted). This is open to all accredited financial investigators. It includes all stated cases, legislation, and contact details of law enforcement and financial institution personnel, and (3) the Regional and National Seminars hosted by ARA (known as the "Payback" initiative).

400. The Concerted Interagency Criminal Finances Authority (CICFA) is chaired by the relevant SOCA director and shares learning and performance information between senior officials, policy makers, and practitioners (see section 1.5 above). At an operational level, UK law enforcement agencies have a "Proceeds of Crime Working Group", led by a Deputy Chief Constable. This multi-agency body acts as a forum for developing and promulgating good operational practice.

Recommendation 28

401. Competent authorities in the UK have comprehensive authority to compel production of, search persons or premises for, and seize and obtain evidence. This includes transaction records, identification data obtained through the CDD process, account files and business correspondence, and other records, documents or information, held or maintained by financial institutions and other businesses or persons.

402. For a full description of powers available to law enforcement under POCA, refer to Recommendation 3 above. As an overview: POCA provides the following powers for law enforcement officers to obtain further information from a reporting party:

- Production Orders (Sections 345-351 POCA);

- Customer Information Orders (Sections 363-369 POCA);
- Account Monitoring Orders (Sections 370-375 POCA);
- Search and seizure warrants (Section 352 POCA);
- Disclosure orders (Section 357 POCA).

403. All of these powers are used routinely by UK law enforcement, including by SOCA officers working on proceeds of crime investigations such as proactive money laundering investigations or asset recovery cases.

404. Similar provisions are available in the SOCPA 2005 (Sections 62 and 66), and the Police and Criminal Evidence Act (PACE). If the "records" amount to evidence of an indictable offence, any one or more of the PACE powers could apply depending on the nature of the evidential material, whether it is held by the financial institution, whether the suspect was the customer or a representative of the institution or both and whether either or both have been arrested; for example:

(a) *The court order/search warrant powers re premises:* The particular option used would depend whether the "suspect" is a "customer", e.g. who knowingly provided false information to the financial institution or to whom transaction records relate, or is a representative of the financial institution e.g. one who has altered legitimate customer records or criminally deceived the customer, or both e.g. when customer & representative are jointly concerned in the commission of an indictable offence.

(b) Without warrant powers: Application would depend on when and where police exercised the powers concerned. For example,

- re s.18 & 32 PACE, it would depend on when & where a "suspect" customer and/or "suspect" representative of the financial institution was arrested;
- s.18 PACE would apply for a "suspect" representative who was deemed to occupy or control the financial institution's premises where the "evidence" of the indictable offence was to be found & s.32(2)(b) PACE would apply if the suspect was arrested in those premises or immediately after leaving those premises;
- Section 32(2)(a)(ii) PACE would apply to the search of any "suspect" for evidence of the offence for which arrested.

405. With regard to terrorism, any premises may be searched, and any information obtained if it relates to a terrorist or terrorist financing investigation under the Terrorism Act (TACT) 2000, now updated in the TACT 2006. Specific powers, include: power to obtain information (section 37); search of premises and persons (section 42-43); seizure (section 82-83), and examination of documents (section 87). The only exceptions are those items which might fall subject to legal professional privilege.

Power to take witness statements

406. *England, Wales & Northern Ireland:* Where a person so consents, investigators are able to take statements from anyone who they believe will be able to assist them. If a person is not willing to provide a statement, the prosecutor can apply to the court for a witness summons under Section 2 of the Criminal Procedure (Attendance of Witnesses) Act 1965 or in Northern Ireland section 51 of the Judicature (Northern Ireland) Act 1978. The court will issue a witness summons ordering a person to attend court where the court is satisfied that the person is likely to give material evidence and it is in the interests of justice to issue a summons. These powers are available in respect of ML, FT, and predicate offence investigations.

407. *Scotland:* Scottish authorities are also authorised to take voluntary witness statements. However, apart from a few statutory exceptions (e.g. Section 6, Official Secrets Act, 1920, as substituted by Section 1, Official Secrets Act, 1939; Section 232, Road Traffic Act, 1960; and Section

172, Road Traffic Act, 1988), the police cannot *compel* a witness to give a statement. The Procurator Fiscal can make an application to the court for a witness to be precognosced before a Sheriff. Failure to attend for such precognition can result in a warrant being issued for the witnesses' arrest.

408. Where a constable has reasonable grounds for suspecting that a person has committed or is committing an offence at any place, he may require any person whom the constable finds at that place or at any place where the constable is entitled to be and who the constable believes has information relating to the offence, to give their name, address, date of birth, place of birth and nationality under the terms of Section 13 (1)(b) of the Criminal Procedure (Scotland) Act 1995, as amended by the Police Public Order and Criminal Justice (Scotland) Act 2006.

Structure, resources, integrity standards and training for law enforcement and prosecution agencies[18]

Funding through the "incentivisation scheme"

409. Under the "incentivisation scheme" operating in 2004-05 and 2005-06 the Home Office allocated to police forces in England, Wales and Northern Ireland a total of £39m over 2 years in incentive shares from recovered assets. Under a new scheme which came into effect on 1 April 2006, 50% of recovered assets receipts will be paid back to all the agencies involved. The purpose of the scheme is to reward and drive up performance of front-line agencies in taking away the profits of drug dealers and other criminals.

Police

410. There are 43 regional police forces in England and Wales funded by and subject to Home Office oversight, 8 in Scotland funded by and subject to Scottish Executive oversight, and 1 in Northern Ireland funded by the Northern Ireland Office and answerable to the Northern Ireland Policing Board. Of the 43 forces in England & Wales the majority have specialist financial crime investigation units, accounting for approximately 2,700 trained financial investigators who meet the ARA accreditation standards.

411. The ***City Of London Police*** has a large Financial Investigation Unit, as part of the Economic Crime Department. It is currently divided into two parts: the Confiscation Team is responsible for conducting confiscation investigations for the cases dealt with by all force BCU's. The Money Laundering Investigation Unit (MLIU) was established in July 2005 and has lead responsibility for the SARs regime, with a heavy emphasis on intelligence development to identify asset recovery opportunities and the consent regime. Within the MLIU, there are two officers who are dedicated to deal with the consent regime. The consent regime is managed and supervised by the Detective Inspectors (Confiscation and MLIU) and the four Detective Sergeants. The MLIU also has lead responsibility for developing money laundering investigations from non-SAR sources.

412. The Home Office is providing the following additional £2.6m for an additional 88 Financial Investigators in police forces throughout England and Wales.

NTFIU

413. The NTFIU is a multi-agency body consisting of financial investigators dedicated to combating terrorist financing. It is part of a Special Branch (SO-15) of the Security Service. The Unit investigates to terrorist financing component of investigations in co-operation with terrorist investigations of other departments (e.g. Special Branches, the Security Service). NTFIU officials explained that every terrorism investigation would include investigations into the financial aspects of

[18] As related to Recommendation 30; see Section 7.1 for the compliance rating for this Recommendation.

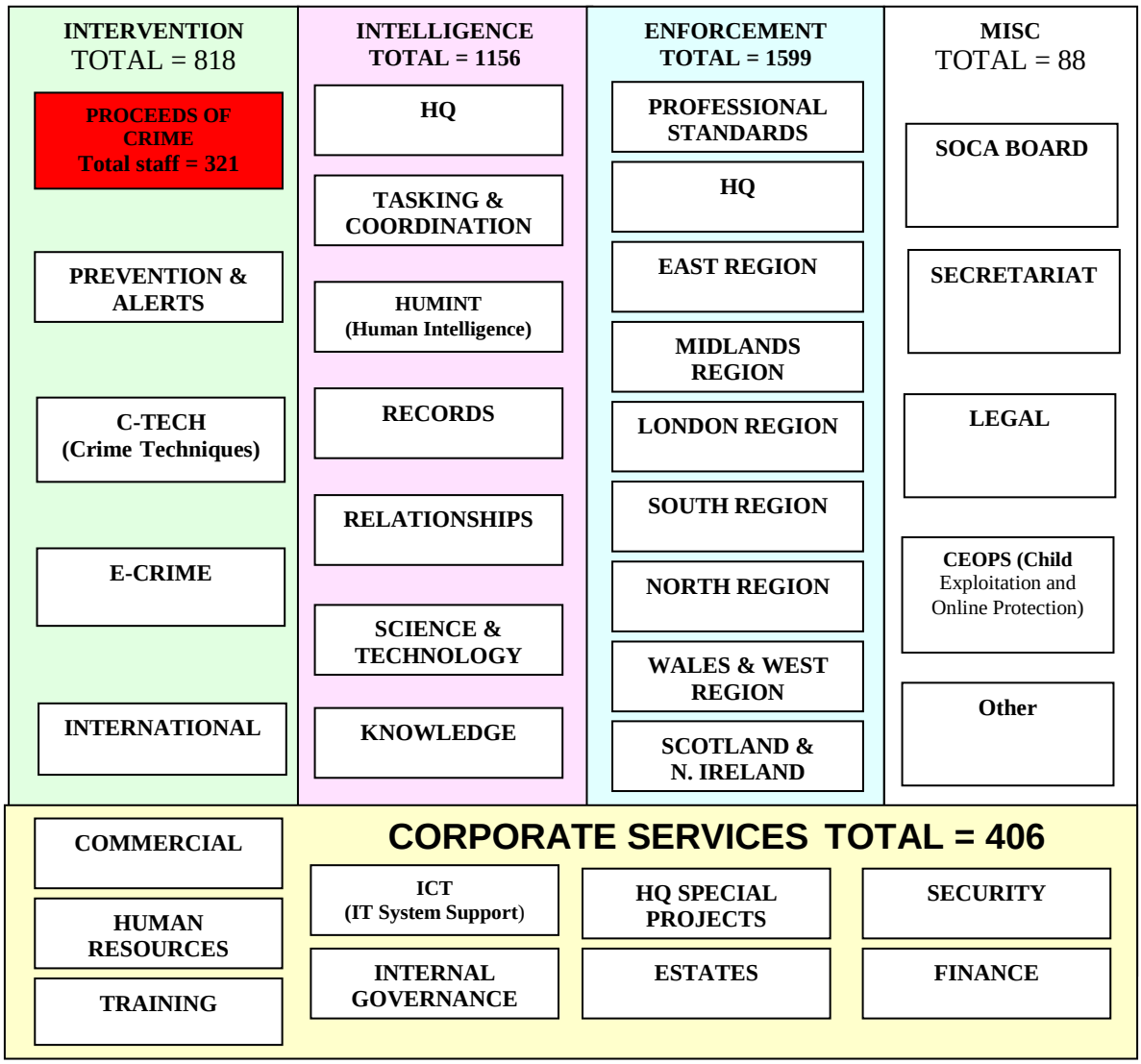
the case. The NTFIU undertakes or coordinates terrorist finance enquires to develop both intelligence and evidence. For example, the NTFIU receives and develops intelligence reports sent to it by the UK FIU's Terrorist Financing Team.

414. The NTFIU has grown from 10 officers in 2001 to its present strength of 35 core police officers and 10 police staff. The team is enhanced by attachments / secondments from regional forces and other law enforcement or government agencies, creating a total unit strength that varies between 60 and 70 staff (some attachments are case specific and not ongoing). NTFIU is supported by financial investigators attached to anti-terrorist teams within regional forces. These units have specialist arms staffed by financial investigators to combat terrorist financing. NTFIU officers undergo the same financial investigator training (i.e., accreditation by ARA as described below) as other investigators.

SOCA

415. SOCA's resource budget excluding pay is £210m (inc. pay £416m) and capital £41m. All Proceeds of Crime work in SOCA (including the UK FIU) had a resource budget for FY 06/07 that was £4.4m excluding pay. (In this case, pay is part of a separate, central budget. The organisational chart for SOCA is as follows.

SOCA Chart – total number of staff 4,067



416. SOCA has an enforcement capability specifically dedicated to tackling money laundering and asset recovery. There are approximately 250 financial investigators within SOCA, most of whom are embedded within SOCA Enforcement Teams across the UK. These financial investigators however remain part of the Proceeds of Crime Department (PoC) command structure to ensure operational independence and freedom from undue influence within the Enforcement Teams. In reality, this means that the financial investigators work alongside their Enforcement colleagues, providing the technical expertise on money laundering investigations; whilst PoC can influence the direction of their activities in support of its Strategic Priorities.

HMRC

Money laundering/Asset Recovery Chart

Product & Progress Group	**Operations**	**Corporate Functions**
Excise and Stamp Taxes	Intelligence (75) Criminal Investigations (*) Detection (100)	**Central Policy** – Criminal and Enforcement Policy (3) **Legal & Governance** - Criminal Finances, Customs and Excise Litigation Team (16)

417. Team definitions:

- **Intelligence** – provide national co-ordination, direction and control of intelligence to drive each of HMRC's strategies.
- **Special Civil Investigations** – investigating suspected cases of complex avoidance and tax evasion, tackling fraud and error in tax credits and child benefits, dealing with tax affairs of the Country's most wealthy and tackling serious non compliance.
- **Criminal Investigation** – provides HMRC with an effective investigation arm to enforce policies and deliver against strategic responsibilities across direct tax, indirect tax, criminal finance, excise regimes and frontiers.
- **Detection** – are accountable at the frontier and inland for the detection and disruption of smuggling, fiscal fraud and non-compliance with international trade procedures.

418. Where evidence of money laundering is uncovered during the course of a criminal investigation of a predicate offence, HMRC will ask the prosecutor to consider the addition of money laundering charges.

419. HMRC has approximately 274 Financial Investigators that meet ARA accreditation standards. There is a specialist Financial Investigation Division which comprises three distinct commands. The first is Restraint and Confiscation, which works in close partnership with investigators dealing with predicate offences and lawyers from the Revenue and Customs Prosecution Office. The second team is the Anti Money Laundering Unit, which reviews and conducts cases suitable for investigation as money laundering linked to Direct Tax fraud, other HMRC intelligence, and existing cases. The third team deals with disruption and training.

420. Spread over the UK territory, there are currently other 18 specialist criminal investigation branches across all disciplines of the Department as follows: Investigation South - Dover Branch 3a, Crawley Branch 3b, Staines Branch 5 Investigation Central - Birmingham 11a, Nottingham 11b, Ipswich 2, Bristol 15 Investigation North - North West 9, Branch 12, Glasgow 13a, Belfast 13b Investigation London - VAT 4, Financial / POCA 16, Commercial 18 National Teams - Branch 10, Forensics (HTCT/DocEx/NAFIS) 24 Criminal Investigation - Complex Business Crime, Business & Credits Criminal Investigation - Criminal appeals Bureau. These number approximately 1600 staff.

Additionally, there are various levels of civil investigation and compliance which may also deal with the proceeds of crime. A specialist Financial NIU (80 staff) exists to co-ordinate and manage intelligence activity across the Department in relation to the proceeds of crime. There are currently 571 FIs in the Department although a proportion of these work within intelligence.

Crown Prosecution Service (CPS)

421. The CPS is responsible for prosecuting criminal cases investigated by the police in England and Wales, including advising the police on cases for possible prosecution, and review, prepare and present cases in court. At the end of March 2006, the CPS employed 8,184 people. This includes 2,832 prosecutors and 4,731 caseworkers and administrators. All CPS prosecutors may deal with money laundering prosecutions, whether they are based in the CPS Areas, or Headquarters.

422. The CPS has 42 Areas across England and Wales. Each Area is headed by a Chief Crown Prosecutor (CCP) who is responsible for the delivery of a high quality prosecution service to his or her local community. A 'virtual' 43rd Area, CPS Direct, is also headed by a CCP and provides out-of-hours advice to the police. Three casework divisions, based in Headquarters, deal with the prosecution of serious organised crime, terrorism and other specialised prosecution cases.

423. The national lead on money laundering and confiscation issues is held by the Head of the ***Proceeds of Crime Delivery Unit (POCDU)***. POCDU is responsible for the performance management of asset recovery in Areas and for the lawyers within the ***Regional Asset Recovery Teams (RARTs)***. Within each of the 42 CPS Areas, local lawyer and caseworker POCA champions are responsible for training local CPS staff on money laundering and confiscation issues.

424. Money laundering investigations conducted by SOCA leading to CPS prosecutions are dealt with by lawyers within the Organised Crime Division (OCD). Level two money laundering investigations conducted by the five RARTs are dealt with initially by CPS lawyers based within the RARTs, but are then dealt with by Area CPS lawyers together with any level two money laundering investigations conducted by the local police forces.

425. The ***Confiscation Unit*** of the OCD at Headquarters deals with asset recovery issues on behalf of the OCD and also provides advice to CPS Area lawyers on POCA 2002 confiscation issues. The Unit also works to enforce high value confiscation orders made under the pre-POCA 2002 legislation and also executes requests for restraint and confiscation assistance on behalf of foreign jurisdictions. The Unit comprises 18 lawyers and 20 caseworkers and administrators. CPS Areas are responsible for obtaining POCA restraint, management receivership and confiscation orders in the Crown Court. They also apply for pre-POCA confiscation orders that fall below the threshold of the Confiscation Unit and enforce POCA confiscation orders requiring the appointment of an enforcement receiver.

426. CPS is centrally funded for its core work, and for the period 2006/07 and 2007/08, CPS benefits under the Home Office's incentive scheme (the Recovered Assets Incentive Fund (RAIF)); CPS receives one-sixth of the amount remitted to the Home Office in respect of enforced confiscation orders. Compensation and receivers' costs are deducted from the recovered amounts before remittance to the Home Office. RAIF funds five CPS prosecutors based within the RARTs; these prosecutors deal only with money laundering and confiscation issues. In addition, RAIF funding has been received for a national conference on money laundering and for the development of an e-learning package, which has a money laundering module.

427. The CPS net Request for Resources (RfR), as voted by Parliament, for the period to 31 March 2006 was £614 million. Outturn on expenditure as shown in the 2005-06 Accounts, Statement of Parliamentary Supply, was £602 million.

428. The Home Office is providing the following additional, ring-fenced resources to assist in the recovery of the proceeds of crime and the investigation of money laundering, including £10m for the 5 multi- agency RARTs, and £4.5m towards CPS costs in proceeds of crime work.

429. In 2002, the CPS produced a confiscation and money laundering training package in conjunction with the Nottingham Law School. This training is now available to all prosecutors and caseworkers as an e-learning package. The training was initially given to a minimum of two lawyers from each of the CPS 42 Areas. These lawyers formed a national network of POCA lawyer champions and each of them signed a training contract by which they agreed to cascade the training to the lawyers within their Areas. Subsequently, a training package was delivered to CPS caseworkers and a national network of POCA Caseworker champions was also formed. The training provided by the local Area POCA lawyer and caseworker champions has been coordinated and supplemented by the Regional Asset Recovery Team lawyers, who have provided training to CPS, the police and to the Bar. In addition, there have been a number of national conferences attended by CPS POCA lawyer and caseworker champions highlighting topics such as restraint, money laundering and the enforcement of confiscation orders. Workshops will shortly be delivered to nominated enforcement champions from each CPS Area, who will be responsible the enforcement of those confiscation orders requiring the appointment of a receiver. Training has also been delivered to Area personnel to enable CPS Areas to use the Joint Asset Recovery Database (JARD), so as to ensure that progress on asset recovery can be properly monitored by the Delivery Unit.

Scottish Crown Office and Procurator Fiscal Services (COPFS)

430. COPFS prosecutes all crime in Scotland; the decision on whether to start criminal proceedings rests with COPFS, whether or not a person has been arrested or charged by the police. The relationship between the COPFS and the police is a close one similar to the Crown Prosecution Service and police in England and Wales. But because the Fiscals have responsibility for the investigation and prosecution of crime, they have the power to direct the police in their investigation.

431. COPFS is headed by the Crown Agent & Chief Executive. COPFS is divided into 11 areas, each of which has an Area Procurator Fiscal. These areas normally coincide with the boundaries of the eight Scottish police forces. Within each area, apart from Glasgow, there is a network of local Procurator Fiscal offices and an Area Office. Within the headquarters, the Operations Group prepares cases for the High Court and Court of Appeal and also contains the Financial Crime Unit (33 staff), the Civil Recover Unit (11 staff) and the International Co-Operation Unit (8 staff).

432. Funding for COPFS and the Scottish Executive Civil Recovery Unit is provided by the Scottish Executive. COPFS had a statutory budget of £92.422m for 2005-2006, and £89.052m for 2004-2005.

Revenue and Customs Prosecution Office (RCPO)

433. RCPO is an independent government department responsible for prosecuting all HMRC criminal cases in England and Wales, (RCPO defers to the Crown Office for prosecutions in Scotland and the PPSNI in Northern Ireland). Its remit covers HMRC offences in England and Wales and prosecuting SOCA investigations into major drug importations (usually the large scale smuggling of Class A drugs and related money laundering). RCPO has 280 staff, of which 80 are lawyers, who are based in London and Manchester.

434. The Attorney General is the principal legal adviser to the government, as well as superintending minister for RCPO, the Crown Prosecution Service (CPS) and the Serious Fraud Office. The Attorney General's annual budget is just over £37 million.

435. There are five operational casework divisions. Each division has a lead activity, although divisions A–D are multifunctional and, therefore, all may handle money laundering prosecutions.

They are: Division A (Direct Tax Fraud); Division B: (Commercial Fraud) Including large-scale VAT fraud and more complex Missing Trader Intra-Community Fraud (MTIC); Division C (Border Detections, including drug smuggling through ports and airports, export controls and sanctions violations); Division D (Duty and Excise); Including alcohol, tobacco and hydrocarbon oils duty fraud; Division E (Serious Organised Crime—i.e., SOCA cases which covers large-scale drug importation and associated money laundering. RCPO lawyers work closely with investigators to ensure investigations and prosecutions are successful.

436. RCPO also has an expert Asset Forfeiture Unit, which is responsible for conducting restraint, confiscation and enforcement proceedings. It also responds to requests from overseas jurisdictions to preserve assets so that they may used to pay confiscation orders made in those jurisdictions and to enforce confiscation orders made in those jurisdictions against assets located in the UK. It deals with confiscation proceedings in serious and/or complex cases investigated by HMRC and in all cases investigated by SOCA. The Asset Forfeiture Unit is responsible for the enforcement of all confiscation orders obtained by RCPO.

437. RCPO provided internal training on confiscation hearings and proceedings in June 2005 dealing with the Criminal Justice Act 1998 and the Drug Trafficking Act 1994. RCPO is currently training all of its prosecutors on confiscation, restraint and enforcement under the Proceeds of Crime Act 2002. RCPO will supplement this with e-learning packages for new lawyers joining RCPO in early 2007.

Public Prosecution Service of Northern Ireland (PPSNI)

438. The PPSNI prosecutes criminal cases investigated by police, HMRC, and SOCA in Northern Ireland. It is headed by the Director of Public Prosecutions Northern Ireland, who is accountable to the Attorney General Northern Ireland.

439. The PPSNI is regionally based, with four regions in total. Each region is headed by a Regional Prosecutor who generally has overall responsibility for decision making on investigation files and for the conduct of prosecutions in that region. There are also a number of Sections, each headed by an Assistant Director, which deal largely with specialised or complex areas of work. These include: Central Prosecutions; Fraud and Departmental; Policy; and High Court, International and Restraint and Confiscation.

440. The funding for the PPSNI is provided by the Secretary of State for Northern Ireland and the Director is responsible for ensuring that public monies provided are used efficiently.

Scottish Crime and Drug Enforcement Agency (SCDEA)

441. The Scottish Crime and Drug Enforcement Agency (SCDEA) Money Laundering Unit ("SMLU") is led by a Detective Inspector backed up a 12-strong team, including one dedicated financial analyst. In addition to the SMLU, the SCDEA has 34 trained Financial Investigators available to work on proceeds of crime issues.

The Assets Recovery Agency (ARA)

442. ARA has offices in London and Belfast. The organisation's operational structure includes two intelligence units, one in each office to maintain a separation of intelligence from operational material. The ARA has in excess of 200 staff across the two offices with nearly 60% of staff located within Operations (either financial investigation or litigation).

443. In 2005/2006, the ARA undertook a strategic review of its approach which was informed by an analysis of successes to date and feedback from stakeholder partners. The review concluded that ARA should continue to put the majority of its resources into civil recovery and taxation work where the Agency has exclusive powers. As part of this approach ARA senior management also reviewed the

structure of the ARA to ensure that it was fit for purpose and that the maximum amount of resources were put into front-line investigation whilst reducing the management overhead.

444. All staff are subject to government security clearance to the appropriate level, which is determined by operational need. The sensitivity of ARA's work means that all paperwork is subject to at least a minimum level of security classification, using the government standard. ARA maintains an extensive security and professional standards framework together with regular security appraisals.

445. All operational financial investigators must complete the Centre of Excellence training programme (described below) but have delegated access to POCA powers from the Director and as such do not require formal accreditation.

Standards and Integrity

446. Individual agencies and police forces will have their own localised procedures and standards for staff (e.g. SOCA has its own unique standards guidelines). Also, the need for staff to be subject to any kind of government security clearance will vary with operational requirements. Other relevant standard setting and scrutiny issues include:

- minimum "fit and proper" recruitment standards apply for all officers and support staff;
- stringent vetting procedure for police officers prior to appointment, and higher levels of vetting on appointment to specialist departments. Internal police selection procedures for such posts emphasise discretion and experience. Serving police officers are subject to sanctions from both the relevant parts of the law e.g. Data Protection Act or The Official Secrets Act, as well as a comprehensive police discipline code;
- the handling and confidentiality of financial intelligence, specifically SARs, is part of the ARA training package for financial investigators;
- individual officers are subject to the scrutiny of the relevant professional standards unit;
- at agency / force level, there is scrutiny by a supervisory body such as HM Inspectorate of Constabulary for compliance with Government-approved law enforcement standards

Training for investigators

447. Under Section 3 of the Proceeds of Crime Act 2002, the Director of the Assets Recovery Agency (ARA) has a statutory duty to train, accredit and monitor the accreditation of financial investigators throughout England, Wales, and Northern Ireland. ARA accreditation is the only recognised accreditation for financial investigators in the UK.

448. This training is delivered by the ARA Centre of Excellence (CoE). The training covers all aspects of Asset Recovery including Money Laundering and the Suspicious Activity Reporting regime. Training courses include: Pre-Requisites course; Financial Investigation course; Money Laundering course; Confiscation course; Enhanced Financial Investigation Skills course; Senior Appropriate Officer course; Tutor Training course; and a Financial Investigation Management course. Currently there are almost 3000 financial investigators registered with ARA CoE.

449. Training is delivered to Police, SOCA, and HMRC officers and also to 18 other government departments and law enforcement organisations (such as DWP, Trading Standards, UK Passport Agency, etc: financial investigation techniques and POCA powers are useful for tackling a range of crimes, such as benefit fraud).

450. Once the training has been delivered, via a mixture of e-learning and classroom based courses, the investigators are assessed through the submission of a professional development portfolio (PDP) before becoming accredited as Financial Investigators. The ARA CoE is then responsible for the monitoring of all Financial Investigators' continuous professional development (CPD) through a series

of assessed activities and submissions via the CoE e-learning site and Financial Investigation Support System (FISS).

Centre of Excellence training data:

Year	New FIs attended training	FIs attended enhanced training*	Other courses**	New FIs accredited
2003/2004	431	205	---	131
2004/2005	607	544	---	334
2005/2006	644	749	494	489

*Includes confiscation and money laundering courses

** Includes financial investigation management, tutor training and pre-requisites' attended by non financial investigators

HMRC-specific training

451. All newly appointed operational staff undergo both Enforcement Awareness Core Skills (EACS) and National Anti-Smuggling Program (NASP) training. EACS is a gateway event for all staff appointed to law enforcement areas of HMRC and includes an awareness and training session on POCA. This is then developed further in the context of the NASP events to focus specifically on detection issues: this comprises more in-depth training, including operational deployment with a cash seizure team. The most senior official within HMRC dealing with cash detection has recently quality assured the financial element of EACS and is satisfied as to the depth and breadth of this training. In addition to EACS and NASP, officers who are deployed to specialist cash seizure teams receive further in-depth training. HMRC regional offices have recently rolled out refresher POCA awareness training to all front-line operational officers to ensure that cash detection and seizure is recognised as a mainstream rather than a specialist activity. An updated module will be rolled out in March 2007.

452. HMRC has its own Financial National Intelligence Unit (FNIU) to pool financial intelligence information from its offices across the UK. All HMRC FNIU staff receive training in intelligence analysis, and must pass the ARA Financial Investigators Course. Staff also attend the training course for Money Laundering Regulation (MLR) assurance officers (i.e. the training for HMRC officers involved in supervising of MSBs and HVDs for compliance with AML/CFT controls, cf Section 3 and Section 4) so they have a better understanding of their colleagues' supervisory responsibilities.

453. HMRC investigators receive financial awareness training as part of their basic course. In addition HMRC has developed a two-day 'financial up-skilling' course, which all investigators are required to attend. The purpose of the latter is to ensure that POCA issues are given prominence in all investigations and remain in the minds of all investigators. This supports a long-standing policy that all criminal cases should be accompanied by financial enquires with a view to confiscation. HMRC Criminal Investigation also has a three-person team dedicated to financial training matters that constantly monitor the training contents for accuracy and quality and upgrade the material as necessary. This team has also developed a one-day 'up-skilling' event for investigation managers. This includes an outline of the law, the procedures which are to be followed, and the role of the senior appropriate officer.

Additional elements

454. Under the new constitutional reforms the Lord Chief Justice (LCJ) is the head of the judiciary and this function includes responsibility for ensuring there is provision of training for judges and magistrates. This responsibility is exercised through the Judicial Studies Board (JSB), an independent body that reports directly to the LCJ. This is to ensure that there is no ministerial influence on judicial training, as part of the general commitment to maintaining judicial independence.

455. New legislation including that aimed at terrorist and money laundering offences is the subject of Criminal Continuation Seminars attended by all Crown Court judges in a rolling three-year programme. Any significant developments in the law and practice applying to such trials are covered during the seminars and are the subject of Criminal Appeal Office Bulletins published periodically.

456. The JSB, with the help of the Inns of Court School of Law, has produced a guide to the Proceeds of Crime Act 2002. This is in the form of a CD-Rom and is also accessible via a private (to judiciary) JSB training website. The guide contains a step-by-step guide on confiscation orders, and information on money laundering, receivership orders, restraint orders and help on cases with an overseas element. The material was made available as of February 2006.

2.6.2 Recommendations and Comments

457. The UK has taken a very pro-active approach to pursuing not only predicate offences but also the proceeds of crime and the financial aspects of terrorist cases. The UK has designated a number of competent authorities to investigate and prosecute money laundering offences, while the NTFIU actively pursues terrorist financing in conjunction with FT and terrorism investigations. The various agencies appear adequately structured, funded, and resourced to effectively carry out their functions. Integrity standards, including standards of confidentiality, are very high for investigators and prosecutors. Detailed training on AML/CFT, especially as regards financial investigations, is routinely provided and in fact required for all the relevant investigators.

458. In addition, UK authorities have sufficient and a wide range of powers to compel production of, search and seize, evidence including transaction, identification, and other records for financial institutions.

2.6.3 Compliance with Recommendations 27 & 28

	Rating	Summary of factors relevant to s.2.6 underlying overall rating
R.27	C	
R.28	C	

2.7 Cross Border Declaration or Disclosure (SR.IX)

2.7.1 Description and Analysis

Special Recommendation IX

Disclosure system

459. Under s78 of the Customs and Excise Management Act 1979 (CEMA) any person entering or leaving the UK is required to answer any questions that an HMRC officer may put to him about his baggage and anything contained therein or carried with him. In addition, he must produce such items for examination if requested to do so. These powers also apply to cash and bearer negotiable instruments. It is UK policy for HMRC officers to target travellers entering or leaving the UK on a risk assessment basis, taking account of risk profiles, trend data, and intelligence.

460. The UK does not currently operate a declaration system. However, the EU Council Regulation No 1889/2005: "the Cash Controls Regulation" will also apply in the UK as of 15 June 2007. Under Article 3, all persons entering or leaving the European Community (but not between the UK and another EU country) must declare any cash that they are carrying if it amounts to 10,000 euros or more (or the equivalent in other currencies). The cash controls regulation provides for the declaration to be made either orally, electronically or in writing. The UK will introduce a written declaration system.

461. Therefore, from 15 June 2007, the UK will have two systems operating simultaneously: the disclosure-based system for movements between the UK and any other country, plus the declaration system between the UK and non-EU states.

462. Upon discovery of a false disclosure of currency or bearer negotiable instruments or a failure to disclose them, designated competent authorities have the authority to request and obtain further information from the carrier with regard to the origin of the currency or bearer negotiable instruments and their intended use. Where a person is intercepted for questioning under CEMA s78, and admits to or is found to be carrying large quantities of cash, it is standard practice for the officer to ask about its origin and intended use.

Stop and seizure powers

463. UK authorities are able to stop or restrain currency or bearer negotiable instruments for a reasonable time in order to ascertain whether evidence of money laundering or terrorist financing may be found, where there is a suspicion of money laundering or terrorist financing. Schedule 1 to the Anti-Terrorism, Crime and Security Act 2001 (ACTS) provides for the seizure of any amounts of cash, however small, if there are reasonable grounds to suspect that it is linked to terrorism. Where terrorism is suspected, it is UK practice for HMRC officers to immediately refer the matter to the police.

464. Under civil powers in Section 294 POCA, HMRC/police may seize the "cash" and detain it up to 48 hours if it amounts to £1,000 or more and there are reasonable grounds to suspect that it is either the proceeds of or is intended for use in unlawful conduct, which would of course include money laundering. ("Cash" is defined as "notes and coins in any currency, postal orders, cheques of any kind, including travellers' cheques, bankers' drafts, bearer bonds and bearer shares.") On application by HMRC/police, a court may order seized cash to be further detained for periods of 3 months up to a maximum of two years whilst its origin and intended use are investigated, and may order its permanent forfeiture if as a result of the investigation it is satisfied to the civil standard of proof (i.e. balance of probabilities) that the cash is associated with criminal activity.

465. UK authorities do not have the specific authority to detain cash and bearer negotiable instruments purely for a false disclosure. If a person falsely disclosed to a customs officer, and this

false disclosure gave the officer reasonable grounds to suspect that the cash is associated with criminal activity, then he could seize the cash if it is £1,000 or more for money laundering or any amount for terrorist financing. UK authorities note that in practice the authorities would be able to seize the cash in most cases, since making a false declaration would arouse suspicion, and thus detention orders would be straightforward to obtain from the courts under the civil standard (i.e., the balance of probabilities). Article 4 of the EC cash controls regulation will explicitly establish a penalty for making a false declaration when carrying cash in and out of the European Economic Community.

System to record and make information available

466. Currently, there is no requirement to retain, at a minimum, the amount and identification the bearer in amount of disclosures where there is a false disclosure. Nor is there is a general requirement to maintain this data in the event of a suspicion of ML/FT; however, where there is a suspicion of terrorist financing, or a suspicion of money laundering and the amount is £1,000 or more, the cash concerned will be seized and a record made. Current practice is that identification data is currently retained in all cases where cash is seized, and for all unseized detections of £10,000 and over.

467. Article 5 of Reg. 1889/2005 will require identification data obtained from the declaration under Article 3 and/or from control measures under Article 4 to be recorded and processed by the authority in the Member State to whom the declaration is required to be made.

468. There is some detailed information on cross-border disclosures available to the FIU, either by way of notifying the FIU about suspicious cross-border transportation incidents or making comprehensive information on declarations available; however, the system is not fully comprehensive: the UK FIU has access to cash seizure data on the shared database JARD. Information is entered into JARD if there has been a seizure and the magistrates court has granted a continued detention order within 48 hours. In those cases, HMRC enters as much personal information as is provided by the investigator, usually name, address, date of birth, date, time, search provision, seizure circumstances, place of seizure, account given by subject and nature of the suspicion which led to the seizure (if known). But it should be noted that JARD does not include all information on all disclosures; money that has been disclosed but not seized is not put into the database; or if the money has been seized but no magistrate's order for continued detention has been issued within 48 hours.

Domestic and international co-operation

469. There is co-ordination between the various border agencies and related authorities (including port and airport security firms) with regard to the detection of criminal cash. Specifically, HMRC and the police are in the process of negotiating a formal MoU on the subject. It is standard practice for HMRC to refer any incidences of suspected terrorist cash to specialist police officers stationed at ports and airports. The HMRC also has officials working directly at the UK FIU. However, there could be more proactive communication to SOCA on these co-operation issues.

470. Within the framework of Mutual Administrative and Mutual Legal Assistance, the UK currently provides information and assistance to the enforcement authorities of other countries in relation to suspect cash movements and other aspects of financial crime insofar as it is within the limits of existing statutory gateways; this includes direct customs-to-customs interaction in some circumstances (for more on international co-operation arrangements, refer to Section 6).

471. In general, there are adequate co-operation arrangements with other countries which allow for bilateral customs-to-customs information exchanges between customs and other relevant agencies on cross-border transportation reports and cash seizures. For example, the HMRC has financial crime liaison officers posted abroad to work with about 50 customs administrations on these issues.

472. As from 15 June 2007, the UK will be required to comply with the requirements for exchanging information in relation to suspect cash movements with the relevant authorities in other Member

States, third countries and the Commission, as prescribed in Articles 5, 6, and 7 of Reg. No. 1889/2005.

Sanctions

473. The available sanctions are the civil powers in POCA, which are applied in relation to criminal cash (i.e., civil seizure powers in the event of a suspected crime. Under section 78 of CEMA a customs officer has the power to question a person travelling across the UK's borders about any items they are carrying, including cash and bearer negotiable instruments. Failure to answer these questions truthfully could result in criminal sanctions under section 167 of that Act. This would therefore provide for sanctions in the event of a false disclosure.

474. As required under Article 9 of Reg. 1889/2005 UK is introducing secondary legislation under which HMRC will have the option of imposing penalties up to a maximum of £5,000 for failure to comply with the obligation to declare under Article 3.

475. There are appropriate sanctions available for someone carrying out a physical cross-border transportation of currency or bearer negotiable instruments that are related to terrorist financing or money laundering contrary to the obligations under SR. IX. Where it is suspected that cash detections may be linked to money laundering or terrorist financing, the cash seizure powers under POCA or ATCS are normally applied.

476. HMRC may decide to deal with such a detection in the context of a criminal investigation of money laundering (sections 327-329 POCA); in respect of terrorist financing the police may decide to conduct a criminal investigation under Section 18 TACT. Either might involve the arrest on suspicion of such an offence any person associated with the cash, which could include the person found to be carrying it. Penalties are:

- under section 334 of POCA, a person guilty of a principal money laundering offence under section 327-329 POCA; or
- under section 22 TACT, a person guilty of a terrorist financing offence under section 18 TACT

is liable on conviction on indictment to a maximum term of imprisonment of 14 years, or to a fine, or both.

Other measures

477. Provisional and confiscation measures described under Recommendation 3 (in section 2 of this report) apply adequately for persons carrying out a physical cross-border transportation of currency or bearer negotiable instruments that are related to terrorist financing or money laundering. The measures to freeze terrorist-related funds as described under SR.III (in section 2 of this report) apply equally to persons who are carrying out a physical cross-border transportation of currency or bearer negotiable instruments that are related to terrorist financing.

478. If there were specific cases, HMRC would co-operate with the relevant authorities of other countries in respect of any investigations into the smuggling of gold, precious metal and precious stones, including those where money laundering is suspected, within the constraints of the existing legislation. To date, HMRC has not recorded an instance of this kind of smuggling linked to actual or suspected money laundering. UK authorities should be more pro-active in this area, since one would expect some cases of this type of smuggling through such a large and highly-transited country.

479. Systems will be put in place to ensure that as from 15 June 2007 information obtained under Articles 3 and 4 of Council Regulation 1889/2005 and recorded and processed under Article 5 will be made available as appropriate for the investigation of money laundering by the relevant authorities,

and will be safeguarded as required under national and Community legislation relating to data protection.

Recommendation 32

480. The UK does not maintain comprehensive statistics on cross-border disclosures concerning suspected ML/FT. The JARD database retains this information in the event of all seizures, however. (See the JARD statistics after the discussion of Recommendation 3 in this report.)

2.7.2 Recommendations and Comments

481. Overall, the UK has a disclosure system which appears to work in practice. However, authorities should have a more direct power to detain cash and bearer negotiable instruments purely for a false disclosure or declaration when transporting cash or monetary instruments into or out of the UK, and should retain, at a minimum, the amount and identification the bearer in amount of disclosures where there is a false disclosure, and in the event of a suspicion of ML/FT (even if there is not a seizure). Addressing these issues will also make the system for making all information on cross-border disclosures available to the FIU more comprehensive.

2.7.3 Compliance with Special Recommendation IX

	Rating	Summary of factors relevant to s.2.7 underlying overall rating
SR.IX	**LC**	• UK authorities do not have the authority to detain cash and bearer negotiable instruments purely for a false disclosure. • Currently, there is no requirement to retain, at a minimum, the amount and identification of the bearer where there is a false disclosure or maintain this data in the event of a suspicion of ML/FT, although this is be done in practice if the amount is £1,000 or more. • The system whereby detailed information on cross-border disclosures is available to the FIU is not fully comprehensive.

3. Preventative Measures – Financial Institutions

Overview of legal and regulatory framework

482. In line with its European commitments, the UK will finish implementing the Third Money Laundering Directive in December 2007, and this will substantially overhaul the regulatory and supervisory framework described below. At the time of the FATF on-site visit, however, the legal framework was provided by: Statutory Instrument 2003 No. 3075 (the Money Laundering Regulations 2003 or "MLRs"); EC Regulation No 1781/2006 of 15 November 2006 – information on the payer accompanying transfers of funds ("the wire transfers regulation"); the Terrorism Act 2000 (TACT) (as amended by the Anti-terrorism, Crime and Security Act 2001); Proceeds of Crime Act 2002 (POCA) (as amended by the Serious Organised Crime and Police Act 2005); and Financial Services and Markets Act 2000 (FSMA). The same legal framework applies to all financial institutions equally throughout the UK, including Scotland and Northern Ireland.

483. A large part of financial services business in the UK is conducted by financial institutions that are regulated by the UK's financial services regulator, the FSA. However, some relevant parts, such as MSBs, are not under FSA supervision. FSA-regulated financial institutions are required to comply with the FSA Handbook including its new AML Systems and Controls provisions which now focus on higher level obligations of adequate AML systems and controls and managerial responsibility. In addition, detailed guidance is provided to FSA-regulated institutions through the JMLSG Guidance (prepared by the industry and formally approved by the Treasury). In the view of the UK authorities, the three key constituent parts of its controls (the MLRs, the FSA Rules and Handbook, and the JMLSG Guidance) create an interlocking framework that should be understood as a whole.

484. Financial institutions that are not regulated by the FSA but provide a "money service business" (i.e. money value transmission, bureau de change, cheque casher) are regulated by HMRC and take account of guidance provided by HMRC.

485. Financial institutions that fall under the MLRs, but are not actively supervised for AML/CFT compliance, such as consumer credit providers, leasing, factoring, safe deposit keepers, and others, can be prosecuted for a breach of the legislation but do not have any comprehensive additional obligations or instructions to adhere to beyond the provisions of the legislation. However, the Finance and Leasing Association, which covers a substantial part of the leasing and consumer credit sectors, is a member of JMLSG and as such endorses the guidance therein.

Scope of the Money Laundering Regulations 2003

486. The Money Laundering Regulations 2003 were issued by the Treasury, in exercise of the powers conferred by: (i) section 2(2) of the European Communities Act 1972, and (ii) sections 168(4)(b), 402(1)(b), 417(1)(c) and 428(3) of the Financial Services and Markets Act 2000. The regulated sector is defined by the MLRs under Regulation 2(2). The table below indicates how all the financial activities within the with the FATF definition of financial institutions are covered by the MLRs.

FATF Financial Institution Definition	MLRs
Acceptance of deposits and other repayable funds from the public	MLRs Regulation 2(2)(a)(i)
Lending	MLRs Regulation 2(2)(e)
Financial leasing	MLRs Regulation 2(2)(e)
The transfer of money or value	MLRs Regulation 2(2)(d)
Issuing and managing means of payment (e.g. credit and debit cards, cheques, traveller's cheques, money orders and bankers' drafts, electronic money)	MLRs Regulation 2(2)(e) MLRs Regulation 2(2)(a)(x)
Financial guarantees and commitments.	MLRs Regulation 2(2)(e)

Trading in: - money market instruments (cheques, bills, CDs, derivatives etc.); - foreign exchange; - exchange, interest rate and index instruments; - transferable securities; - commodity futures trading	MLRs Regulation 2(2)(e)
Participation in securities issues and the provision of financial services related to such issues	MLRs Regulation 2(2)(e)
Individual and collective portfolio management	MLRs Regulation 2(2)(a)(iv) and (v) or 2(2)(e)
Safekeeping and administration of cash or liquid securities on behalf of other persons	MLRs Regulation 2(2)(a)(vi) or 2(2)(e)
Otherwise investing, administering or managing funds or money on behalf of other persons	MLRs Regulation 2(2)(a)(iii), (iv), (v), (viii)
Underwriting and placement of life insurance and other investment related insurance	MLRs Regulation 2(2)(a)(ii)
Money and currency changing	MLRs Regulation 2(2)(d)

FSA Handbook of Rules and Guidance

487. FSA's rule making power can be found at Part X, section 153 of the Financial Services and Markets Act 2000 ("FSMA"). FSMA also requires the FSA to exercise its rule-making powers in writing, in a document FSMA calls a 'rule-making instrument'. The FSA publishes all these instruments on its website. Furthermore, it also brings together the content of these instruments in a consolidated format in the "FSA Handbook of Rules and Guidance". The instruments indicated as "rules" in the FSA Handbook are thus considered secondary legislation or regulation.

488. There are three categories of provisions in the FSA Handbook:
   (i) The letter **R** is used to indicate general **rules** made under the Act. The rules in the Handbook create binding obligations on FSA regulated financial institutions.
   (ii) The letter **E** is used to identify **evidential** provisions with characteristics specified in FSMA. An evidential provision is a rule, but is not binding in its own right. It always relates to some other binding rule within the FSA Handbook referred to above. The evidential provision is used to assess whether the financial institution has complied with the rules it supports. Breach of an evidential provision creates a rebuttable presumption that there has been a breach of the rule to which it refers.
   (iii) The letter **G** is used to indicate **guidance**. Guidance is not binding on those to whom FSMA and the rules apply, nor does it have 'evidential' effect. Guidance is generally designed to throw light on a particular aspect of regulatory requirements, not to be an exhaustive description of how a financial institution should meet its obligations. While this FSA guidance creates "legitimate expectations" that the FSA will behave in a certain way (i.e., take the guidance into account when assessing compliance), the converse is not true in that this does not create direct obligations upon the financial institutions to follow the specific provisions in the JMLSG Guidance.

489. FSMA, Part X, section 146, gives the FSA powers to create money laundering rules that would be binding on FSA-regulated financial institutions: "The [FSA] may make rules in relation to the prevention and detection of money laundering in connection with the carrying on of regulated activities by authorised persons." The FSA rules on money laundering were until recently contained within a "Money Laundering Sourcebook", which formed one module of the FSA Handbook. In 2005/06 the FSA reviewed the FSA Handbook to identify areas where, according to UK authorities, "requirements were more restrictive than necessary to achieve the FSA's statutory objectives; or where they did not deliver benefits to justify their costs; or where they were not consistent with the FSA's focus on senior management responsibility." Thus, the Money Laundering Sourcebook was deleted

altogether on 31 August 2006 in favour of new provisions in the *Senior Management Arrangements Systems and Controls (SYSC)* sourcebook. These new rules, according to the FSA, are meant to:

- put a clearer focus on senior management responsibility for AML systems and controls and on the need for financial institutions to manage real money laundering risk;
- create a better fit with the relevant primary and secondary law by removing duplication;
- create a better fit with industry guidance by removing duplication with the JMLSG Guidance (described below); and
- give financial institutions and senior managers greater flexibility to implement systems and controls in the most appropriate way for their institutions, whilst remaining accountable to the FSA for the actions they take.

Joint Money Laundering Steering Group (JMLSG) Guidance

490. The industry has elaborated guidance on AML/CFT covering good practice application of the law, FSA rules and anti-money laundering controls. It is published by the "Joint Money Laundering Steering Group" (JMLSG), a privately owned company, composed of representatives of 17 financial sector trade bodies. It is formally "approved" by the Treasury under specific provisions of the AML/CFT legislation. The JMLSG guidance has been a significant part of the AML/CFT landscape for financial institutions since the 1990s; the current version of the guidance went live on 1 September 2006.

491. MLRs Regulation 3(1)(b) and FSA Handbook, SYSC 3.2.6 R are both intended to be high level obligations. The JMLSG Guidance provides detailed guidance to financial institutions on their high level legal and regulatory obligations. Many of the specific guidance areas flow from the general, high-level obligations in MLR Regulation 3(1)(b), which requires "establish such other procedures of internal control and communication as may be appropriate for the purposes of forestalling and preventing money laundering" and from the FSA Handbook, SYSC 3.2.6 R, which indicates that "A firm must take reasonable care to establish and maintain effective systems and controls for compliance with applicable requirements and standards under the regulatory system and for countering the risk that the firm might be used to further financial crime."

Scope of the JMLSG Guidance

492. JMLSG Guidance, Part I, Preface, paragraph 14 states that the guidance "is addressed to firms in the industry sectors represented by its member bodies, and to those firms regulated by the FSA. All such firms – which include those which are members of JMLSG trade associations but not regulated by the FSA, and those regulated by the FSA which are not members of JMLSG trade associations - should have regard to the contents of the guidance." JMLSG Guidance, Part I, Preface, paragraph 15 states: "Financial services firms which are neither members of JMLSG trade associations nor regulated by the FSA are encouraged to have regard to this guidance as industry good practice. Firms which are outside the financial sector, but subject to the ML Regulations, particularly where no specific guidance is issued to them by a body representing their industry, may also find this guidance helpful."

493. As stated by the UK authorities, the JMLSG Guidance gives firms a degree of discretion in how to comply with AML/CFT legislation and regulation; it is still possible to take other courses of action that may demonstrated as equivalent. As indicated by paragraph 19 in the Guidance, "When provisions of the statutory requirements and of FSA's regulatory requirements are directly described in the text of the guidance, it uses the term **must**, indicating that these provisions are mandatory. In other cases, the guidance uses the term **should** to indicate ways in which the statutory and regulatory requirements may be satisfied, but allowing for alternative means of meeting the requirements." Finally, large passages of the text, for example on PEPs, or beneficial ownership, ongoing monitoring, is mostly descriptive, or coached in terms such as "firms are encouraged to…", or "firms may feel it appropriate to…" which clearly demonstrates that these parts only give advice and ideas and do not

create an obligation on the part of the financial entity – this is also clearly stated in the Preface to the JMLSG Guidance itself, and recurs in the text, e.g. Part I, Chapter 6, para 6.1., states "there is no specific legal or regulatory requirement that… but there is an expectation that…."

494. This means that a reading of JMLSG Guidance itself clearly points towards a differentiated approach towards the various obligations, recommendations, descriptions and advice contained therein, and a general treatment of the whole of the text as "other enforceable means" is not possible, even leaving aside the status under FSA rules described below.

Drafting and approval of the Guidance

495. The JMLSG Board maintains an Editorial Panel which prepares the industry guidance. The drafting of the guidance is developed with the input of a wide range of industry specialists and practitioners. Once the Guidance has been agreed by the JMLSG Board, there is a formal consultation process which is open to all. The Editorial Panel and the Board considered all the comments received in finalising the Guidance, before submitting it for formal Treasury approval. The current version of the JMLSG Guidance was formally approved by the Chancellor of the Exchequer on 13 February 2006 for the purposes of Regulation 3 of the Money Laundering Regulations 2003, sections 330 and 331 of the Proceeds of Crime Act 2002 and section 21A of the Terrorism Act 2002.

Status before a court

496. The MLRs provide that a court must take account of relevant industry guidance i.e. guidance that has been approved by the Treasury in determining whether a person or institution within the regulated sector (i.e. persons & businesses in the UK which are obliged to operate AML/CFT controls) has committed an offence under the regulations. MLRs Regulation 3(3) requires:

> In deciding whether a person has committed an offence under this regulation [MLRs Regulation 3: Systems and training etc. to prevent money laundering], the court must consider whether he followed any relevant guidance which was at the time concerned –
> a. issued by a supervisory authority or any other appropriate body;
> b. approved by the Treasury; and
> c. published in a manner approved by the Treasury as appropriate in their opinion to bring the guidance to the attention of persons likely to be affected by it.

497. Identical provisions can be found in POCA (section 330(8)) and TACT (section 21A (6)) requiring the court to take the guidance into account when deciding whether an offence under those acts has been committed (provided the same three conditions above are met). Therefore, a court must take the JMLSG Guidance into account for money laundering and terrorist financing prosecutions involving persons or business to whom the JMLSG Guidance applies. Following the Guidance provides a defence in court, in the way of a safe haven from prosecution for having adequately applied the guidance and therefore provides a disincentive for a firm seeking to deviate from it.

Status under the FSA Rules

498. The JMLSG Guidance also has status under the FSA rules and provides a defence. When considering whether to take disciplinary action against a financial institution in respect of a breach of the relevant provisions of its rules (SYSC) and enforcement (ENF), the FSA may have regard to whether the institution has followed relevant provisions in the JMLSG Guidance.:

- FSA Handbook, SYSC 3.2.6E **G**:[19]

[19] The "G" indicates that this is guidance and therefore is not binding.

- The FSA, when considering whether a breach of its rules on systems and controls against money laundering has occurred, will have regard to whether a firm has followed relevant provisions in the guidance for the UK financial sector issued by the Joint Money Laundering Steering Group.

- FSA Handbook, ENF 11.9.1 **G**:
  - The FSA's money laundering rules are set out in SYSC 3.2. The FSA, when considering whether to take disciplinary action in respect of a breach of those rules, will have regard to whether a firm has followed relevant provisions in the Joint Money Laundering Steering Group's Guidance Notes for the Financial Sector".

- FSA Handbook, ENF 15.4.1 **G**:
  - The FSA's general policy is to pursue through the criminal justice system all those cases where criminal prosecution is appropriate. The principles the FSA will apply when it decides whether a case is appropriate for criminal prosecution are set out in ENF 15.5. When considering whether to prosecute a breach of the prescribed regulations in relation to money laundering ENF 15.2.2 G (2) the FSA will also have regard to whether the person concerned has complied with the (Guidance Notes for the Financial Sector) produced by the Joint Money Laundering Steering Group.

499. However, all these quotes are only Guidance in the FSA Handbook, as defined by the "**G"** at the end of each quote. Thus, when considering whether to take disciplinary action in respect of a breach of the FSA's rules or whether to prosecute a breach of the prescribed regulations in relation to money laundering or, the FSA policy is that it will have regard to whether the financial institution or individual has followed the relevant provisions in the JMLSG Guidance. However, while this FSA guidance creates "legitimate expectations" that the FSA will behave in a certain way (i.e., take the guidance into account when assessing compliance), the converse is not true in that this does not create direct obligations upon the financial institutions to follow the specific provisions in the JMLSG Guidance.

500. Guidance is used as a means to prove a failure to comply with the AML/CFT regulation (rather than to create legal obligations themselves) and a disciplinary action cannot be engaged on the sole basis of a breach of the industry guidance. This analysis is confirmed by the fact that all imposed sanctions are actually based on a breach of the FSA Rules. The whole body of enforcement actions by FSA that pertains to AML/CFT was reviewed by the assessment team: they are not very numerous, many still pertain to the regime where the AML Handbook of FSA existed, and while they demonstrate that in some limited instances the FSA takes account of the JMLSG Guidance in its supervisory and enforcement actions, they do not demonstrate that the FSA is necessarily bound to do so, and do not demonstrate the existence of any specific obligations beyond the existing legal framework (i.e., the MLRs and the mandatory aspects of the FSA Handbook). Thus, in this context, the JMLSG Guidance as a whole cannot be considered as "other enforceable means" as defined by the FATF standards. Parts of the Guidance are linked to certain Rules, and when those rules are read inclusively with the Guidance, the content of the Guidance on those particular points (i.e. not the Guidance as a whole) could be regarded as part of the enforceable means, namely the relevant Rules. Other parts of the Guidance are not linked to anything and are therefore only that - mere guidance.

HMRC Guidance for Money Service Businesses (MSBs)

501. The HMRC does not have the power to make binding rules on the sector that it regulates. It does however produce guidance for the MSB sector which is drawn up in consultation with sector experts and representatives. When considering disciplinary action, HMRC will take account of whether or not the MSB operator has followed the guidance; but this guidance has no status before a court.

502. The HMRC Guidance is written to target the central questions related to AML/CFT that would occur for an MSB. The guidance is brief and covers less ground that the JMLSG, which the UK authorities justify on the fact that the majority of MSB business is of an over-the-counter, one- off transaction variety. Ongoing business relationships are the exception and are more common in the cheque-cashers sector, which advances payment to the customer against monetary instruments payable to them. Since the financial institution bears the risk that the cheque / other monetary instrument is not stolen, forged, or otherwise worthless, it is in that institution's commercial interests to ensure that the customer is subject to robust identification checks.

Customer Due Diligence & Record Keeping

3.1 Risk of money laundering or terrorist financing

503. The MLRs, Proceeds of Crime Act 2002 and the Terrorism Act apply to all financial institutions carrying out financial activities as defined by the FATF. In addition, the requirements in the MLRs 2002 also apply to all activities (and as indicated above, to all financial institutions as required by the FATF recommendations.) No financial institutions or activities (as defined by FATF) are excluded from the MLRs on a risk-sensitive basis.

504. UK legislation does not explicitly refer to a risk-based approach, although certain provisions are based on risk-based principles. The consequence of this risk-based approach is a high-level and principle-based law, leaving the detail of implementation to industry and leading to a reduction in prescriptive rule making. (Once the Third EU Money Laundering Directive is implemented in the UK law, the risk-based approach will be explicitly written into UK law.) In general, the risk-based approach applies to two main areas:

(1) **JMLSG Guidance and the risk-based approach by firms:** The JMLSG Guidance notes generally indicate that those entities under its scope should apply the particular guidance to the extent that that is required, taking into account the firm's risk-based view on the need to do so in order to meet the regulatory obligations under the MLRs and FSA Handbooks (such as customer identification and maintaining effective internal systems and controls to prevent and combat money laundering). The JMLSG Guidance has for some time referred to *the need* to adopt a risk-based approach to customer due diligence, and to some general factors of risks to be taken in consideration by the firm but does not offer firms a road map, structure or guideline for types of firms or sectors on how such a risk based approach should be implemented in the specific firm..

(2) **FSA Supervision:** In its supervisory work, the FSA directs more resources towards those financial institutions which, through their size, nature of their operations or the standard of their controls, pose greater risks to the four regulatory objectives set out above (protection of consumers, market confidence, public awareness, and the reduction of financial crime). Therefore, the detailed regulatory requirements for the 29,000 authorised financial institutions that the FSA regulates vary, for example to take account of international obligations and the nature of the business. In general, the financial institutions are divided by the level of "impact" to the financial sector, and ratings are determined for the level of risk. Initial impact "scores" begin with the size of the financial institution. These impact "scores" can then be overridden by the supervisors, raising or lowering the category of impact. For those with a finalised impact rating above "low", a further assessment of the probability of risks at those firms is carried out. That combination of impact and probability determines the overall level of risk and therefore the overall level of supervision. Factors to raise or lower risk probability could involve the extent to which the firm is involved in payment systems, or if a firm is located in a country with higher ML/FT risk. Approximately 31% of original impact or probability "scores" are overridden; 29% of the overrides are for financial crimes issues. See the

discussion under Section 3.10, Recommendation 23 ("Ongoing supervision and monitoring") for more details and analysis of the effectiveness of the current regime.

3.2 Customer due diligence, including enhanced or reduced measures (R.5 to 8)

3.2.1 Description and Analysis

505. The customer identification obligation is set out in the MLRs, which require that new customers are identified satisfactorily, without specifying how financial institutions should do this; in general they simply require that new customers are identified satisfactorily. These obligations apply equally to all financial institutions (as defined by FATF).

506. The financial services sector has to be seen in three parts, which are each dealt with differently based on different approaches by the legislator and regulator. Some are overlapping:

- The FSA-regulated sector and some additional practitioners (leasing): Here, the industry itself considered how firms can best comply with that requirement; this is set out in the Treasury-approved JMLSG Guidance;
- The HMRC-supervised sector which is covered by the HMRC Guidance;
- and the rest, who have no further obligation and no supervision or oversight for AML/CFT.

507. For the FSA/regulated sector, the approach adopted to identify and verify a customer's identity using reliable, independent source documents, data or information has been part of the JMLSG Guidance for some time, as an integral part of the UK regime and is therefore well established in the practice of the FSA/regulated sector. The approach allows for a number of variations, which it explains in detail, and requires firms to adopt a risk based approach when choosing the appropriate variation of customer identification.

508. The JMLSG Guidance, in advising firms on the variations allowed, makes clear that one of its important stated goals is to foster an atmosphere of public/private partnership and to provide a regime which is accepted as proportionate, and therefore strives to command industry and consumer support while it is intended to deliver value to law enforcement. This has led to a strong emphasis on a risk based approach to identification and on alternative means, such as electronic methods, for verification of identity. Also, avoiding repeated identification has been seen as an important goal.

509. However, although the JMLSG Guidance refers to *the need* to adopt a risk-based approach to customer due diligence, it does not offer details on how risks should be assessed within a firm, i.e. how to create and maintain a sound risk analysis in a specific sector or entity. The JMLSG itself does not provide a general risk analysis for the financial sector, either. Many of the evaluators' interlocutors in the financial industry seem to focus primarily on elements such as proportionality and avoiding double effort, while not focusing sufficiently on risk analysis processes. In sum, this situation raises concerns about a sound application of the risk based approach in practice, especially in smaller, less sophisticated firms, who lack the expertise to understand and apply the risk-based approach to their operations. Consequently, a less robust basic identification might be used in cases which do not warrant this.

510. For MSBs, the approach to customer identification is set out in HMRC Guidance, MSB2.

Anonymous accounts

511. MLRs Regulation 4(3)(a) effectively ensures that anonymous, numbered and fictitious named accounts are not allowed to exist in the UK, by requiring that the customer "produce satisfactory

evidence of his identity; or that such measures specified in the procedures must be taken in order to produce satisfactory evidence of the customer's identity."

When CDD is required

512. MLRs Regulation 4(2) states that:

> This regulation [MLRs Regulation 4 - Identification procedures] applies if -
> (a) A [the financial institution] and B [the customer] form, or agree to form, a business relationship;
> (b) in respect of any one-off transaction -
> (i) A knows or suspects that the transaction involves money laundering; or
> (ii) payment of 15,000 euro or more is to be made by or to B; or
> (c) in respect of two or more one-off transactions, it appears to A (whether at the outset or subsequently) that the transactions are linked and involve, in total, the payment of 15,000 euro or more by or to B.

513. Thus, MLR 4(2) therefore requires identification when (1) establishing a business relationship; (2) for occasional transactions (whether single or when appear linked) above the threshold of EUR 15,000; and (3) in case of suspicion of money laundering. The MLRs define "business relationship" as: "any arrangement the purpose of which is to facilitate the carrying out of transactions on a frequent, habitual or regular basis where the total amount of any payments to be made by any person to any other in the course of the arrangement is not known or capable of being ascertained at the outset."

514. Additionally, MLRs Regulation 5 makes clear that any exemptions from the need to verify ID do not apply if there is a suspicion of money laundering.

515. For wire transfers, the measures in place for SR.VII will be implemented starting in January 2007 (with the national enforcement regime expected to come into effect in December 2007) as a result of EC Regulation No 1781/2006 of 15 November 2006, includes requirements to identify name, address, and account number (article 4) in accordance with SR.VII. The Regulation was been published on 8 December 2006. Draft JMLSG guidance was published on the BBA website on 13 December 2006 (http://www.bba.org.uk/bba/jsp/polopoly.jsp?d=131&a=8108).

516. Identification upon suspicion of terrorist financing is indirectly covered in the Regulation. MLRs Regulation 2(1) defines "money laundering" as an act which falls within section 340(11) of the Proceeds of Crime Act 2002, or an offence under section 18 of the Terrorism Act 2000. Section 18, makes it an offence for a person to enter into or become concerned in an arrangement which facilitates the retention or control, by or on behalf of, another person of terrorist property, where he had knowledge or grounds to suspect that it was terrorist property. "Terrorist property" is defined as (a) money or other property which is likely to be used for the purposes of terrorism (including any resources of a proscribed; (b) proceeds of the commission of acts of terrorism, and (c) proceeds of acts carried out for the purposes of terrorism. JMLSG Guidance, Part I, Chapter 5, paragraph 5.2.32 also states: "There is no exemption from the obligation to verify identity where the firm knows or suspects that a proposed relationship or one-off transaction involves money laundering or terrorist financing." This also means that it is only applicable to entities covered by JMLSG and does not extend to HMRC regulated firms such as MSBs or further to the non-supervised financial sector.

517. Further, JMLSG Guidance (Part I, Chapter 5, paragraphs 5.2.47, 5.2.48) only partly deals with identification where there are doubts regarding previously obtained customer identification data. In substance, financial institutions are required to have regard to the risk posed by customers who might not have been identified and to take steps to mitigate those risks. "Firms that do not seriously address risks (including the risk that they have not confirmed the identity of existing customers) are exposing themselves to the possibility of action for breach of FSA rules, or of the MLRs." However, this is not

laid out in law or regulation. In addition, as mentioned earlier, JMLSG guidance is not applicable to the whole financial sector.

Required CDD measures

518. MLRs Regulation 4(3)(a) requires (for natural and legal persons):

> A [the financial institution] must maintain identification procedures which -
> (a) require that as soon as is reasonably practicable after contact is first made between A [the financial institution]and B [the customer] -
> (i) B [the customer] must produce satisfactory evidence of his identity; or
> (ii) such measures specified in the procedures must be taken in order to produce satisfactory evidence of B's [the customer's] identity…

519. Additionally, the JMLSG Guidance (Part I, Chapter 5) provides extensive guidance how to identify and to verify the identity of customers using reliable, independent source documents, data or information for those who have regard to it. Paragraphs 5.4.14-5.4.60 provides detailed guidance on the identification of personal customers. The norm is that financial institutions should obtain the full name, residential address and date of birth for personal customers. Evidence of identity can be verified by using documents, electronic data or a combination of both.

520. The level of detailed guidance attached to the use of alternate methods of identification and verification in cases where the standard approach is not feasible is quite exhaustive, and seems to cover adequately the practical challenges connected to using commercial service providers and their electronic databases for background checks, or any other form of identification and verification not based on photo id documents.

521. The UK has made an effort to solve in Guidance the tension between allowing pragmatic solutions where full documentation is not available to a low risk personal customer who enters a business relationship for a limited product, and ensuring that in all other cases documentation is complete. Therefore, exemptions from verification using standard documents are regulated in JMLSG and by HMRC Guidance. While the evaluation team has had doubts as to whether such pragmatic solutions as electronic verification and "source of funds as evidence" are sufficient to fulfil the FATF standard, the safeguards attached to such verification options in the Guidance, such as only using registered providers of electronic identification, and limiting the instruments where source of funds can be seen as evidence, seem to be adequate. It would be important to regularly check on-site or through thematic work with firms whether the safeguards are applied in practice.

Legal persons

522. MLRs Regulation 4(3)(d) requires that: A [the financial institution] must maintain identification procedures which…require that where B [the customer] acts or appears to act for another person, reasonable measures must be taken for the purpose of establishing the identity of that person. This is the general requirement to *identify* the person acting on behalf of another person in all cases, covering both the case of acting for a legal person (criterion 5.4 (a)(ii)) and acting on behalf of any other customer as well (criterion 5.5.1).

523. There is no specific requirement to verify the identity of the person purporting to act on behalf of another person, although the regulation requires that "reasonable measures must be taken" to establish that person's identity. All further details are dealt with in Guidance, both JMLSG and MSB Guidance (criterion 5.4(b)). Further, it is not specifically required in law or regulation to verify that any person purporting to act on behalf of the customer is so authorised. But the JMLSG Guidance, Part I, Chapter 5, paragraph 5.4.72 states "Firms should take appropriate steps to be reasonably satisfied that the person the firm is dealing with is properly authorised by the customer and is who he says he is."

524. There is no requirement in law or regulation to determine who are the natural persons that ultimately own or control the customer, including those persons who exercise ultimate effective control over a legal person or arrangement (for example, for companies - identifying the natural persons with a controlling interest and the natural persons who comprise the mind and management of company; and for trusts, identifying the settlor, the trustee or person exercising effective control over the trust, and the beneficiaries).

525. JMLSG Guidance, Part I, Chapter 5, paragraphs 5.4.61-5.4.161 provide detailed guidance on identification requirements for non-personal customers and legal persons, covering a wide range of entities in detail, with a practical detailed list of ways to achieve identification. Paragraph 5.4.62 indicates that "the firm's objective must be to know who has control over the funds which form or otherwise relate to the relationship, and/or form the controlling mind and/or management of any legal entity involved in the funds." "Must", according to the JMLSG introduction, denotes an obligation.

526. In relation to corporates, the customer's full name, registered number, registered office in country of incorporation and business address should be obtained. In addition, for private companies, the name of all directors (or equivalent) and names of beneficial owners holding over 25% should be obtained. The Guidance states that a firm should verify the identity of the corporate from either a search of the relevant company registry, or confirmation of the company's listing on a regulated market or a copy of the company's Certificate of Incorporation. Provisions for further checks in higher risk scenarios are explicitly included.

527. Regarding directors, paragraph 5.4.70 states that the "name of all directors (or equivalent)" should be obtained. But paragraph 5.4.86 explains further that verifying directors should also be subject to the risk-based approach: "Following the firm's assessment of the money laundering or terrorist financing risk presented by the company it may decide to verify the identity of one or more directors, as appropriate in accordance with the guidance for personal customers (paragraphs 5.4.15 to 5.4.60). In that event, verification is likely to be appropriate for those who have authority to operate an account or to give the firm instructions concerning the use or transfer of funds or assets, but might be waived for other directors."

528. HMRC guidance, in contrast, is quite brief, it only covers the basic case of a limited company – the authorities explained that it should be noted that MSBs are rarely faced with an over the counter transaction that does not involve a natural person. Legal persons or arrangements rarely utilise MSB services. Many money transmitters, for example, are small ethnic enterprises that offer transmission services to members of their local community to remit funds to narrowly defined geographical areas of their former countries. Their customer base is mainly ex-patriot workers remitting money to family and friends. Cheque cashers charge a premium rate for their service as they take the risk should the cheque bounce. The high cost is, therefore, a disincentive to legal persons.

Beneficial ownership

529. There is no requirement in law or regulation to identify the beneficial owner or take reasonable measures to verify the identity of the beneficial owner, as required by the FATF standards. The guidance generally covers understanding the ownership and control structure of a legal person. The JMLSG Guidance, Part I, Chapter 5, paragraph 5.4.66 states that consistent with the risk assessment, the firm should fully understand "the company's legal structure and ownership, and should obtain sufficient additional information on the nature of the company's business, and the reasons for seeking the product or service." However, there is no requirement in law or regulation to determine who are the natural persons that ultimately own or control the customer, including those persons who exercise ultimate effective control over a legal person or arrangement (for example, for companies - identifying the natural persons with a controlling interest and the natural persons who comprise the mind and management of company; and for trusts, identifying the settlor, the trustee or person exercising effective control over the trust, and the beneficiaries).

530. The JMLSG Guidance (Part I, Chapter 5, paragraphs 5.4.87 – 5.4.91) provides some guidance on identifying beneficial owners. Paragraph 5.4.87 indicates that "as part of the standard evidence, the firm will know the names of the beneficial owners of private companies holding 25% or more even where these interests are held indirectly." However, the identification procedures for beneficial owners in the JMLSG Guidance does not cover all cases of beneficial ownership according to the FATF definition, since it applies only to the 25% threshold and does not refer to the natural person(s) who ultimately controls the customer.

531. The JMLSG Guidance distinguishes between information about a customer that must be obtained (identifying the customer) and information that must be verified. Guidance in JMLSG Guidance, Part I, Chapter 5, paragraph 5.4.88 adds: "Following the firm's assessment of the money laundering or terrorist financing risk presented by the company, the firm may feel it appropriate to verify the identity of appropriate beneficial owners holding 25% or more. Where a principal owner is another corporate entity or trust, the firm should take measures to look behind that company or trust and establish the identities of its beneficial owners or trustees, unless that company is publicly quoted. The firm will then judge which of the beneficial owners exercise effective control, and whose identities should therefore be verified."

532. The wording of the guidance "may feel it appropriate" does not create or refer to any kind of obligation to actually verify beneficial ownership in any situation. Financial institutions covered by JMLSG are only expected to identify all natural persons with a controlling interest of 25% or more and then using a risk-based approach determine which natural persons' identities need to be verified.

533. HMRC Guidance does not mention beneficial owners at all. While, HMRC Guidance, MSB2, paragraph 9.7 states: that "Normally, in instances where your customer is or appears to be acting on behalf of someone else you must obtain ID evidence of everyone in the chain." However, this does not constitute beneficial ownership.

534. When fully implemented later in 2007, the 3rd ML Directive will introduce explicit "beneficial ownership" verification requirements into law.

Purpose and intended nature of the business relationship

535. There is no explicit obligation to obtain information on the purpose and nature of the business relationship in the UK in all cases. The UK authorities explained that in order to comply with the reporting obligations under section 330 and 331 the Proceeds of Crime Act 2002 (POCA) and section 21A of the Terrorism Act 2000 (TACT) and for FSA firms the regulatory requirements under SYSC 3.2.6R and 3.2.6A R, financial institutions will need to have a clear understanding of their customer's business to be able to fulfil their duty to report suspicious activity. This may be accepted as valid in cases of higher risk, it does not cover the cases of low or normal risk customers, where such information should also be requested by the financial institution and which, under the UK approach of a risk based effort, would not be seen by institutions as necessary.

536. For higher risk cases, guidance offers important elements to orient, unfortunately, only those financial sector entities subject to it via JMLSG or HMRC. The JMLSG Guidance (Part I, Chapter 5, paragraph 5.1.5) states that in addition to verifying the identity of the customer, the risk-based approach adopted by a financial institution may require additional information to be collected. This is referred to as 'know your customer' (KYC) information, which is defined to include understanding the customer's circumstances and business – including, where appropriate, the source of funds, and in some cases the source of wealth and the purpose of specific transactions - and the expected nature and level of transactions; and keeping such information current and valid. JMLSG Guidance, Part I, Chapter 5, paragraph 5.6.9 ("Existing sources of additional customer information) also states: "The purpose and reason for opening the account or establishing the relationship should also be understood.

In many cases, of course, this will be self-evident, but in other cases, the firm may have to find this out."

537. HMRC Guidance indicates that businesses should identify the nature of any new relationship "including the amounts of money involved and the expected frequency of transactions" and to consider why the customer is using their services. HMRC Guidance, MSB 2, paragraph 4.3 defines "know your customer" as: "Asking your customers questions such as their reason for establishing business with you, the source of their funds and the anticipated level and nature of the activity to be undertaken can increase the likelihood that you will detect suspicious activity." However, these measures are not set out in "other enforceable means".

Ongoing due diligence

538. There is no specific requirement in law or regulation to conduct ongoing monitoring or ongoing due diligence. Nor is there a general requirement that ongoing due diligence should include scrutiny of transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the institution's knowledge of the customer, their business and risk profile, and where necessary, the source of funds. This is clearly indicated in paragraph 6.1 of the JMLSG guidance: "There is no specific legal or regulatory requirement that customers' activities be monitored…But having regard to the following obligations:

- the general requirement to establish appropriate procedures of internal control for the purposes of forestalling and preventing money laundering/terrorist financing
- the requirement to report knowledge or suspicion of possible money laundering/terrorist financing
- the 'reasonable grounds' test for making such reports under POCA and the Terrorism Act

there is an expectation that, where the situation so warrants (see paragraph 6.9), a firm will establish and maintain an appropriate approach to enable it to detect transactions or activity that may indicate money laundering or terrorist financing."

539. In the UK authorities' view, financial institutions will need to have an ongoing understanding of their customer's business.

540. For FSA regulated firms, the FSA Handbook, SYSC 3.2.6 R requires that "a firm must take reasonable care to establish and maintain effective systems and controls for compliance with applicable requirements and standards under the regulatory system and for countering the risk that the firm might be used to further financial crime," and SYSC 3.2.6A R requires "a firm must ensure that these systems and controls: (1) enable it to identify, assess, monitor and manage money laundering risk; and (2) are comprehensive and proportionate to the nature, scale and complexity of its activities." FSA interprets this as meaning that a financial institution which does not take steps to conduct ongoing due diligence on the business relationship, will be leaving itself open to breaches of the MLRs or of the requirements in the FSA's Handbook. However, this has not been tested through enforcement action by FSA and it remains questionable whether this interpretation would stand the test of a legal challenge.

541. These high-level legal and regulatory obligations are echoed in the JMLSG Guidance, which explains the practices financial institutions could adopt to keep its KYC information current and valid. However, no mention is ever made of "ongoing monitoring", and this is left entirely up to the firm purely on its own risk-based approach. For example (JMLSG Part I, Chapter 6, paragraph 6.2 states) that "In addition to carrying out customer due diligence, therefore, a firm may need to monitor customer activity to identify, during the course of a continuing relationship, unusual activity. If unusual events cannot be rationally explained, they may involve money laundering or terrorist financing. Monitoring customer activity and transactions throughout a relationship helps give greater

assurance that the firm is not being used for the purposes of financial crime." Similarly, (Part I, Chapter 4, paragraph 4.29): "Firms should…ensure that their risk management processes…are kept under regular review"; and (Part I Chapter 4 paragraph 4.30): "There is a need to monitor the environment within which the firm operates…if customer behaviour is changing, the firm should be considering what it should be doing to take account of these changes".

542. The JMLSG Guidance explains that "monitoring may be by reference to specific types of transactions, the profile of the customer, or by comparing their activity or profile with that of similar, peer group of customers, or through a combination of these approaches"(paragraph 6.5). "The nature of the monitoring in any given case will therefore depend on the business of the firm, the frequency of customer activity, and the types of customer that are involved"(paragraph 6.9). Again, this only covers higher risk situations, and not normal or low risk customers.

543. There is no general obligation that documents, data or information collected under the CDD process be kept up-to-date and relevant by undertaking reviews of existing records. However, the general record keeping requirements would ensure that any information, if collected, would also be adequately kept – see record keeping in general.

544. The JMLSG Guidance states financial institutions should keep customer ID and KYC information up to date to ensure continued compliance with their legal and regulatory obligations. The following sections in Part I highlight this point: Paragraph 5.1.6 states that appropriate additional information to customer ID should be collected and that such information should be kept up-to-date:

KYC - obtaining appropriate additional information…

- understanding the customer's circumstances and business – including, where appropriate, the source of funds, and in some cases the source of wealth and the purpose of specific transactions - and the expected nature and level of transactions; and
- keeping such information current and valid.

545. Paragraph 5.4.12 states: "Where information is held about customers, it should, as far as reasonably possible, be kept up to date. Once the identity of a customer has been satisfactorily verified, there is no obligation to re-verify identity; as risk dictates, however, firms are recommended to take steps to ensure that they hold appropriate up-to-date information on their customers."

546. The majority of MSB transactions are one – off cash transactions and do not involve a business relationship. The bulk of guidance is steered appropriately. Business relationships are dealt with in paragraph 9.20 in the guidance by mentioning "regularly review the relationship and consider reporting any suspicion".

Risk

Enhanced due diligence

547. The MLRs and other legislation do not explicitly address the issue of enhanced due diligence, and there is no general requirement to take additional steps when there is a higher risk scenario, whatever that higher risk scenario may be. Thus, situations which emerge as higher risk, or specific higher risk transactions, are potentially not addressed adequately by all financial sector firms.

548. The FSA Handbook, SYSC 3.2.6A R requires of FSA regulated firms must ensure that these systems and controls: (1) enable it to identify, assess, monitor and manage money laundering risk; and (2) are comprehensive and proportionate to the nature, scale and complexity of its activities.

549. This along with the guidance provided within the JMLSG Guidance addresses the need for financial institutions to undertake a risk assessment for its general money laundering and terrorist

financing risk and higher risk categories of customer, business relationship or transaction. At the general level, enhanced due diligence as a general consequence of higher risk is developed in the JMLSG in part 5.6. There is, additionally, at the level of individual high risk situations, a lot of detailed guidance related to dealing with the individual risk, but no general requirement.

550. Many aspects of enhanced due diligence actions financial institutions need to take is addressed in the JMLSG Guidance. JMLSG Guidance provides a framework of factors/risks which should determine the due diligence measures that the financial institutions should adopt in relation to the different money laundering or terrorist financing risk posed by its customers.

551. JMLSG Guidance, does recommend enhanced due diligence when the firm determines it to be necessary. Part I, Chapter 4, paragraph 4.23 states: "Where a customer is assessed as carrying a higher risk, then depending on the product sought, it may be appropriate to seek additional information in respect of the customer, to be better able to judge whether or not the higher risk that the customer is perceived to present is likely to materialise."

552. As related to the specific cases of enhanced due diligence indicated as examples by FATF:

- **Non–resident customers:** JMLSG Guidance (Paragraphs 5.4.33-5.4.35) states that financial institutions should consider whether further verification of identity is required based on their risk assessment which will include the location of the customer. For higher risk customers, the need to have additional information needs to be balanced against the possibility of instituting enhanced monitoring.

- **Private banking:** The JMLSG Guidance, Part II includes a specific chapter (sector 5: Wealth Management) on recommended additional measures for financial institutions in respect of private banking. This chapter recognises the increased vulnerability of private banking to money laundering.

- **Legal persons or arrangements such as trusts that are personal assets holding vehicles:** JMLSG Guidance, Part I, Chapter 5, paragraphs 5.4.111 – 5.4.123 provides extensive and clearly laid out guidance in relation to due diligence measures for both individuals and corporates, churches, charities, including trusts, foundations and similar entities. For trusts representing a higher risk of money laundering or terrorist financing states that the financial institution should carry out a higher level of verification either by searching an appropriate register maintained in the country of establishment, or by obtaining a summary of the instrument establishing the trust.

- **Companies that have nominee shareholders or shares in bearer form** are mentioned in JMLSG Guidance as requiring extra care; "Firms should adopt procedures to establish the identities of the holders and material beneficial owners of such shares and to ensure that they are notified whenever there is a change of holder and/or beneficial owner" (paragraph 5.4.90). Bearer shares also seem to be very rare in practice – see description in Recommendation 34.

<u>Reduced due diligence</u>

553. MLRs Regulation 5 includes a number of exemptions from the identification requirements for low risk situations mentioned by FATF. These are total exemptions; they are not applicable only in cases of low risk. They cover financial institutions in the UK, the EEA, and other "comparable" jurisdictions; small life insurance policies where total payments in a year to not exceed EUR 1,000; and pension schemes in certain circumstances. This is in line with the First and Second EU Money Laundering Directives which reflect previous EU work to determine what constitutes "low risk", and has not yet taken into account the 3rd ML Directive.

Other exemptions in the MLRs:

554. Under the MLR Regulation 5(5), verification of the customer identification is not required when the proceeds of a one-off transaction are re-invested for the benefit of the customer of which a record is kept, and which can only result in another reinvestment made on the customer's behalf or in a payment made directly to the customer.

Further examples of simplified due diligence are found in JMLSG guidance:

555. **Pension superannuation or similar schemes:** Financial institutions do not have to verify the identity of those to whom pension payments are made—where a pension scheme has HMRC approval, a firm's identification obligation may be met by confirming the scheme's approval.

556. **Beneficial owners of pooled accounts held by DNFBPs: "**Where professional firms that are subject to the ML Regulations hold client money, they are obliged to verify the identities of their clients. Under client confidentiality rules, it may not be possible for the firm holding the client account to establish the identity of the person(s) for whom a solicitor or accountant is acting… "

557. **Source of funds as evidence of identity:** The JMLSG Guidance sets out how the source of funds can be used as evidence of identity where the ML/TF risk in a given scenario (covering customer and product) is considered to be at its lowest. In such a situation a payment drawn on an account with a UK or EU regulated credit institution, or one from a comparable jurisdiction, and where the account is in the sole or joint name of the customer may satisfy the standard ID requirement. The JMLSG Guidance, Part I, Chapter 5, paragraph 5.4.38 elaborates on the conditions under which this approach can be used. For example:

> One of the restrictions that will apply to a product that qualifies for using the source of funds as evidence will be an inability to make payments direct to, or to receive payments direct from, third parties. If, subsequent to using the source of funds to verify the customer's identity, the firm decides to allow such a payment or receipt to proceed, it should verify the identity of the third party. A further restriction would be that cash withdrawals should not be permitted, other than by the investors themselves, on a face-to-face basis where identity can be confirmed.

558. Relying on the source of funds as evidence of identity is used extensively in relation to lowest ML/TF risk business. It allows firms to make significant cost savings with products such as Individual Savings Accounts (ISAs), various insurance and pensions products, new share issues, certain lump sum and regular contribution savings and investment products, certain asset finance business and certain e-money products. It also reduces the inconvenience to the customer, in that with such products there does not automatically have to be a separate ID check process.

559. Some cases of simplified due diligence are contained in the MLRs. They are, however, full exemptions from CDD, and not just cases of reduced due diligence, for example financial institutions in 5(2). These cases seem to be applicable based on the Regulation, independently of any risk assessment, i.e. they do not require proven low risk, which is not in line with the FATF Recommendations.

560. In MLR 5, the exemption for applying customer due diligence for other financial institutions covers all EU and FATF countries, based on an underlying assumption of lower risk for these countries. This exemption is not based on an actual assessment, either by the UK itself or by the financial institution, which would confirm the assumption of low risk. The JMLSG has provided further guidance in their note "The assessment of AML/CFT standards in other countries," which provides a list and guidance on comparable jurisdictions. In practice, smaller financial institutions confirmed that they use the list, and based on this they treat all FATF countries as countries of proven low risk when applying CDD.

561. MLR 5 (i) indicates that the exemptions do not apply in the cases of Regulation (4)(2)(b)(i), which refers to cases of one-off transactions where money laundering is suspected (and indirectly terrorist financing, since this is included in the definition of money laundering). This could be a potential loophole, as it does not cover transactions carried out in the course of a business relationship. However, this may not be a problem in practice. The regulation does not indicate that the exemptions are not allowed where specific higher risk scenarios apply. However, the JMLSG Guidance, Part I, Chapter 5, paragraph 5.2.32 states that: "There is no exemption from the obligation to verify identity where the firm knows or suspects that a proposed relationship or one-off transaction involves money laundering or terrorist financing."

562. Where financial institutions are permitted to determine the extent of CDD measures on a risk-sensitive basis, this is consistent with guidelines issued. The JMLSG Guidance provides extensive guidance on the CDD measures—including reduced CDD—that financial institutions are required to undertake and is consistent with guidelines issued by the FSA. The drafting of the current JMLSG Guidance involved extensive consultation with Treasury, FSA, NCIS/SOCA (and wider law enforcement) to ensure that the guidance on CDD measures is consistent with the view of the competent authorities. For example, the FSA's initiative on customer identification and the outcome of this work fed into the revision of the JMLSG Guidance.

Timing of verification

563. MLRs Regulation 4(3)(a) requires:

> A [the financial institution] must maintain identification procedures which -
>
> (a) require that as soon as is reasonably practicable after contact is first made between A [the financial institution]and B [the customer] -
>
> (i) B [the customer] must produce satisfactory evidence of his identity; or (ii) such measures specified in the procedures must be taken in order to produce satisfactory evidence of B's [the customer's] identity…

564. This obligation applies to verifying the identity of the customer and applies to all financial institutions. However, as there is no obligation in law or regulation to verify beneficial ownership, there is no obligation to verify the beneficial owner before or during the course of establishing a business relationship or conducting transactions for occasional customers.

565. The JMLSG Guidance (Part I, Chapter 5, paragraph 5.4.7) provides guidance on the commencement of a business relationship before verification of customer ID has taken place, both at a general level, and underpinned by specific sectoral guidance. Where there is flexibility in the timing to complete the verification of identity of the customer, financial institutions are required to manage the risk of money laundering and terrorist financing effectively.

566. The specific nature of MSBs' business model means that these criteria are less applicable to MSB AML/CFT controls: in almost all instances the business will be able to undertake verification prior to doing business, therefore, there is no additional guidance beyond the MLRs.

Failure to satisfactorily complete CDD

567. Where the financial institution is unable to comply with core CDD requirements, it is not permitted to open the account, commence business relations or perform the transaction. MLRs Regulation 4(3)(c) states: "A [the financial institution] must maintain identification procedures which …require that where satisfactory evidence of identity is not obtained, the business relationship or one-off transaction must not proceed any further." In addition, JMLSG Guidance states that in these circumstances: "The firm should consider…. whether the circumstances give grounds for making a report to [SOCA]. In addition, paragraph 5.4.11 states that: If the firm concludes that the

circumstances do give reasonable grounds for knowledge or suspicion of money laundering or terrorist financing, a report must be made to [SOCA]. The firm must then retain the funds until consent has been given to return the funds to the source from which they came."

568. HMRC Guidance, MSB2 Guidance, paragraph 9.14 states: "If you are… not entirely satisfied with the identification presented you should refuse the business and report to your Nominated Officer who will decide whether to pass it on to (the FIU)."

569. With regard to an obligation to terminate a business relationship in the event a business relationship has already commenced (Criterion 5.16), there is no such requirement. The JMLSG Guidance states that "whether to terminate a relationship is essentially a commercial decision, and firms must be free to make such judgements." "Financial institutions should consider liaising with law enforcement to consider whether it is likely that termination would alert the customer or prejudice an investigation;" therefore, some provision is made which indicates that termination is at least an option that is used by the financial sector.

Existing customers

570. There is no enforceable obligation to apply CDD to existing customers. However, in a policy statement by the FSA in July 2003, the FSA clearly explains its expectation that it requires financial institutions to address the ML/TF risks associated with long-standing customers whose identities have not been adequately verified, and which thereby leaves them vulnerable to FSA enforcement action (or ultimately prosecution) if they do not have adequate systems and controls in place. The policy is strongly risk-sensitive, recognising that risk should drive these checks and that a less discriminating approach would lead to additional cost and customer irritation without sufficient countervailing AML/CFT benefit. It also recognises that a firm has to prioritise how it should spend its AML/CFT budget, and needs to weigh up the AML/CFT benefit from retrospective ID against the benefit from the same spend in other areas (e.g. extra monitoring).

571. This policy is summarised in the JMLSG Guidance: "The FSA reminded firms that, when carrying out risk assessment and mitigation, the FSA would expect them – as part of their overall approach to AML/CFT – to have considered the risk posed by existing customers who have not been identified." Thus while the MLRs, reflecting the First and Second EU Money Laundering Directives, do not require financial institutions to conduct ID checks retrospectively, such checks are seen by the FSA as an important part of institutions' more general legal and regulatory obligations to manage their ML/TF risks effectively (including their obligations under SYSC 3.2.6 R).

572. In practice, the largest nine retail banks have conducted an extensive "Current Customer Review" exercise. They have risk-assessed all their long-standing customers, using risk "filters" (developed in consultation with the FSA) to reduce the number of customers whose identities have proactively to be checked. Where a long-standing customer falls into a higher risk category (i.e. has not been filtered out), the bank will check what proof of identity it holds (including for reasons other than AML) and, if this does not give sufficient comfort, take other specific action to verify identity.

573. In the estimation of the UK authorities, other financial institutions have fewer long-standing customers, so the remedial work necessary is not so great. Many financial institutions have no pre-1994 customers, or no long-standing customers presenting a significant ML risk, according to UK authorities. In such circumstances, conducting a risk assessment and form an informed judgement as to whether any action is needed would be sufficient, in the FSA's view.

574. In addition, JMLSG Guidance states that "Where information is held about customers, it should, as far as reasonably possible, be kept up to date. Once the identity of a customer has been satisfactorily verified, there is no obligation to re-verify identity; as risk dictates, however, firms are

recommended to take steps to ensure that they hold appropriate up-to-date information on their customers."

575. HMRC Guidance states in general terms that do not distinguish between new and existing customers: "You should regularly review the (business) relationship and consider reporting any suspicion."

Recommendation 6

576. There is currently no enforceable requirement for financial institutions to conduct additional measures regarding PEPs as required by FATF Recommendation 6. There are only some specific references in the JMLSG Guidance Notes, paragraph 5.6.15—5.6.18, which indicates:

> Under the Basel CDD paper, firms are encouraged to have in place additional due diligence measures in respect of PEPs. The Third EU Money Laundering Directive will require firms, on a risk-sensitive basis, to:
>
> - have appropriate risk-based procedures to determine whether a customer is a PEP;
> - obtain appropriate senior management approval for establishing or maintaining business relationships with such customers;
> - take reasonable measures to establish the source of wealth and source of funds of such customers; and
> - conduct enhanced ongoing monitoring of the business relationship.

577. It appears in practice, however, that most financial institutions take the issue seriously and are already implementing PEP-related procedures. This is due, to a great extent, to FSA outreach in this field: PEPs and high net worth individuals are flagged as one of the priority issues for FSA supervision to focus on in respect of 'Private Client Investment Managers' (a sub-sector of the financial services sector that includes private banks). The FSA has also carried out PEP-related thematic work which confirmed that the majority of firms had systems and controls in place that were fully in line with JMLSG Guidance. Similarly, work underway by the authorities to prepare for the implementation of the 3rd Money Laundering Directive has been conducted in the public eye and in consultation with industry, so firms are aware of the forthcoming changes to the law that will create a legal obligation to conduct enhanced CDD in respect of PEPs.

578. The JMLSG Guidance states what could constitute "appropriate" procedures in the context of a risk-based approach to PEPs and gives examples of measures financial institutions with different levels of PEP exposure should take. The approach adopted by financial institutions will depend on their initial risk assessment and ongoing due diligence of the customer. This PEP section refers to paragraph 44 of the 3rd EU Money Laundering Directive, which is not yet applicable in the UK. The language is not mandatory; the guidance only "encourages" the additional CDD measures and says explicitly that the new legislation, when implemented "will require" the various measures. Financial institutions clearly indicated that, while aware of the problem, they are dealing with it according to their risk assessment. One institution visited explicitly indicated that it does nothing as PEPs are not a risk for its business.

579. The PEPs team within the UK FIU receives on average 2,800 SARs per year in relation to suspicious activity involving PEPs, which according to UK authorities indicates that the concept behind this Recommendation is well known within the financial sector, even if there is scope for improvement in the actual controls.

Additional elements

580. The UK has ratified the United Nations Convention Against Corruption in February 2006. According to UK authorities, all provisions have been fully implemented.

Recommendation 7

581. Only FSA-regulated institutions are in a position to offer correspondent banking services; however, there are no specific requirements on correspondent banking in the MLRs or the FSA Handbook. Under MLRs Regulations (3)(1)(b) and FSA Handbook, SYSC 3.2.6 R financial institutions must have in place measures commensurate with their AML/CFT risks. Enhanced due diligence in respect of correspondent banking relationships will become a legal obligation once the Third EU Money Laundering Directive is implemented in December 2007.

582. The JMLSG Guidance includes a specific chapter on Correspondent banking in Part II, Sectoral Guidance 16. This chapter sets out: activities associated with correspondent banking; the corresponding money laundering risks; how to assess the elements of risk in correspondent banking; key elements of CDD and enhanced due diligence that should be undertaken in correspondent banking relationships; and advice on the level and type of monitoring activity that should be undertaken by a Correspondent on its Respondent's activity.

583. The JMLSG Guidance on correspondent banking states that financial institutions should undertake customer due diligence on a respondent institution using a risk-based approach based on the following risk indicators: the respondent's domicile, the respondent's ownership and management structures, the respondent's business and customer base, and downstream correspondent clearing.

584. Further, paragraphs 16.10-16.17 state that financial institutions should gather sufficient information on the respondent institutions. This includes publicly available information, the quality of its supervision and whether it has been subject to any negative regulatory pronouncements. It explicitly also covers the issue of not providing banking services to shell banks.

> All correspondent banking relationships should be subject to an appropriate level of due diligence that will ensure that a Correspondent is comfortable conducting business with/for a particular Respondent (and hence its underlying clients) given the Respondent's risk profile. It may be appropriate for a Correspondent to place greater reliance upon a Respondent being domiciled in or operating in a regulatory environment that is recognised internationally as adequate in the fight against money laundering/terrorist financing. In these instances, a bank may choose to rely on publicly available information obtained either from the Respondent itself, another reputable existing Respondent, from other credible sources (e.g. regulators, exchanges), or from reputable information sources, to satisfy its due diligence requirements.

585. There is no specific requirement for the financial institution to assess the respondent institution's AML/CFT controls and ascertain that they are adequate and effective. However, Paragraph 16.15 of the JMLSG Guidance states that financial institutions should "establish whether the Respondent is itself regulated for money laundering/terrorist financing prevention and, if so, whether the Respondent is required to verify the identity of its customers and apply other AML/CFT controls to FATF standards."

586. While there is not a direct requirement for senior management approval, JMLSG Guidance, paragraph 16.16 states that senior management approval should be obtained: "A person senior to, or independent from, the officer sponsoring the relationship should be required to approve the setting up of the relationship. For higher risk relationships, the Correspondent's compliance (or MLRO) function should also satisfy itself that the risks are acceptable."

587. Both the Correspondent and the Respondent bank must have a clear understanding of their respective responsibilities following the establishment of the relationship in line with the JMLSG Guidance, although nothing specifically mentions that financial institution should document the respective AML/CFT responsibilities of each institution.

588. There are no specific requirements regarding payable through accounts, and the guidance does not refer to being satisfied that the CDD for customers with direct access to the account has actually been performed or being satisfied that the respondent financial institution is able to provide relevant CDD data upon request. However, the FSA indicates that its research shows that payable through accounts do not exist in the UK. UK authorities emphasise that financial institutions' risk-based approach to due diligence should take the following factors into account: (a) JMLSG Guidance, Part II, sector 16, paragraph 16.15, which states that a correspondent should establish whether the respondent is required to verify the identity of its customers and apply other controls to FATF standards; and (b) JMLSG Guidance, Part II, sector 16, paragraph 16.22 states that financial institutions: "Should consider terminating the accounts of Respondents, and consider their obligation to report suspicious activity, for Respondents who fail to provide satisfactory answers to reasonable questions regarding transactions/activity passing through the correspondent relationship, including, where appropriate, the identity of their customers featuring in unusual or suspicious transactions or activities."

589. Overall, there are currently no enforceable obligations pertaining to correspondent banking in the UK. This will be covered in the 3rd ML Directive implementation. However, for the time being, the JMLSG Guidance constitutes a helpful tool for financial institutions and seems to prepare them well for future requirements.

Recommendation 8

590. Under MLRs Regulations (3)(1)(b) financial institutions should have in place effective systems and controls to mitigate the ML/TF risks faced by their business. The FSA Handbook, SYSC 3.2.6 C explicitly refers to the necessity to carry out regular assessments of the adequacy of these systems to ensure continued compliance. In addition, FSA Handbook, SYSC 3.2.6G G (4) indicates that:

> A firm should ensure that the systems and controls include…appropriate measures to ensure that money laundering risk is taken into account in its day-to-day operation, including in relation to:
> (a) the development of new products;
> (b) the taking-on of new customers; and
> (c) changes in its business profile…

591. Therefore, this obligation appears broad enough to cover measures to prevent the misuse of technological developments, at least FSA-regulated firms. Additionally, outreach and thematic work by FSA underpins these rules in practice, by drawing industry resources and attention to emerging new trends and methods.

592. MLRs Regulation 4(3)(b) indicates that: "A [the financial institution] must maintain identification procedures which…take into account the greater potential for money laundering which arises when B [the customer] is not physically present when being identified…"

593. Additional pertinent details is provided in Guidance, both JMLSG and HMRC. The JMLSG Guidance Part 1, Chapter 5, paragraphs 5.4.26-5.4.31 specifically addresses the risks posed by non face-to-face identification and verification. It establishes different types of non face-to-face activity and sets out ways to mitigate impersonation risk. It explains that the extent of verification in respect of non face-to-face customers will depend on the nature and characteristics of the product or service requested and the assessed money laundering risk presented by the customer and acknowledges that non face-to-face identification and verification carries an inherent risk of impersonation fraud and financial institutions are required to mitigate this risk. Guidance on the mitigation of impersonation risk is provided in detail in a clear and easily applicable form allowing for many solutions. Additional checks might include, for example:

- requiring the first payment to be carried out through an account in the customer's name with a UK or EU regulated credit institution or one from a comparable jurisdiction;
- verifying additional aspects of the customer's identity, or of his electronic 'footprint';
- telephone contact with the customer prior to opening the account on a home or business number which has been verified (electronically or otherwise), or a "welcome call" to the customer before transactions are permitted, using it to verify additional aspects of personal identity information that have been previously provided during the setting up of the account;
- communicating with the customer at an address that has been verified (such communication may take the form of a direct mailing of account opening documentation to him, which, in full or in part, might be required to be returned completed or acknowledged without alteration);
- internet sign-on following verification procedures where the customer uses security codes, tokens, and/or other passwords which have been set up during account opening and provided by mail (or secure delivery) to the named individual at an independently verified address;
- requiring copy documents to be certified by an appropriate person.

594. HMRC Guidance considers the risk from non face-to-face customers. It requires MSBs to examine certified copies of original documents when carrying out CDD: this requires a certified hardcopy of some kind and specifically excludes faxes. This reduces the risk of relying on a document that may have been tampered with, such as an unsigned electronic version.

3.2.2 Recommendations and Comments

595. Overall, UK's compliance with the FATF standards on CDD requirements shows a number of essential gaps (beneficial owner, PEPs, ongoing monitoring, etc.) Further, certain elements are not addressed in either law, regulation, or other enforceable means, which further weakens the UK compliance with the FATF standards. The UK authorities indicate that all the identified gaps will be addressed in the implementation of the Third Money Laundering Directive.

596. In practice, the awareness of the requirements and the application of due diligence measures seems very high and goes sometimes beyond the actual requirements in those parts of the financial industry which are regulated, or otherwise strongly exposed to dialogue and outreach by the authorities. However, this compliance level is:

- Dependent on the stance of the regulators and their ability to continue to transmit the message of high-level requirements;
- Does not cover the financial sector as a whole, since significant parts are not sufficiently integrated into the AML/CFT regime;
- And may be open to legal challenge as other means of ensuring adequate systems and controls to safeguard against ML/FT might also successfully fulfil the high-level requirements, thus exposing the authorities to risk of challenge in a court of law on some of the guidance which is now applied.

597. It is strongly recommended to embed the missing elements clearly in law and regulation where necessary, and to clarify the status of the existing guidance either by making it enforceable or by transferring some of its main content into a more mandatory instrument (such as the FSA Handbook). This approach should encompass all financial sectors; the current system leaves significant gaps in several important financial sectors or activities which are not justified, as they present recognisable ML/FT risks.

598. Regarding Recommendation 5, the UK should put the following obligations into law or regulation: (i) to identify the beneficial owner and take reasonable measures to verify the identity of the beneficial owner (for all customers); (ii) for legal persons, to determine who are the natural persons that ultimately own or control the customer; (iii) to verify that any person purporting to act on

behalf of a customer is so authorised; and (iv) a general requirement for conducting ongoing due diligence.

599. The UK authorities should also clarify that CDD is still required in the context of an on-going business relationship if money laundering/FT are suspected (rather than just for "one-off" transactions.) Also, any reduction or exemption of CDD requirements should be based on a specific analysis and identification of a proven low risk.

600. It should also be specifically required by law, regulation, or other directly enforceable means: (i) to verify the beneficial owner before or during the course of establishing the business relationship; (ii) once the business relationship has commenced, to terminate the business relationship if proper CDD cannot be conducted; and (iii) to apply CDD to existing customers on the basis of materiality and risk.

601. Other issues are currently encouraged on a risk-based approach in the guidance and are not directly mandatory. UK authorities should make more clearly enforceable obligations: to obtain information on the intended purpose and nature of the business relationship; to specify the procedures for on-going due diligence in compliance with the FATF Recommendations; to require that financial institutions maintain documents and other CDD data up-to-date and relevant by undertaking regular reviews.

602. Regarding PEPs, the UK authorities should create enforceable obligations in this regard as soon as possible.

603. On correspondent banking, while current language in the JMLSG guidance is generally comprehensive and appears to cover the main areas of Recommendation 7, it does not constitute an enforceable requirement; the UK authorities should make it a more enforceable obligation.

3.2.3 Compliance with Recommendations 5 to 8

	Rating	Summary of factors underlying rating
R.5	**PC**	• JMLSG Guidance only partly deals with identification where there are doubts regarding previously obtained customer identification data. There is no requirement in law or regulation. • It is not specifically required by law or regulation to verify that any person purporting to act on behalf of the customer is so authorised. • There is no requirement in law or regulation to: identify the beneficial owner or take reasonable measures to verify the identity of the beneficial owner, or to determine who are the natural persons that ultimately own or control the customer, including those persons who exercise ultimate effective control over a legal person or arrangement. • The wording of the guidance does not create an obligation to *verify* beneficial ownership in any situation; there is no obligation to verify the beneficial owner before or during the course of establishing a business relationship or conducting transactions for occasional customers. • There is no explicit obligation to obtain information on the purpose and nature of the business relationship in the UK in all cases. • A requirement to conduct ongoing monitoring does not exist in law and regulation. Nor is there a general requirement that ongoing due diligence should include scrutiny of transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the institution's knowledge of the customer, their business and risk profile, and where necessary, the source of funds. The limited procedures for on-going due diligence in the guidance only apply for higher-risk scenarios. • There is no general obligation that documents, data or information collected under the CDD process be kept up-to-date and relevant by undertaking reviews of existing records. • There is no general requirement to take additional steps when there is a higher risk scenario, whatever that higher risk scenario may be, although the Guidance makes it clear that this is expected. • Provisions for reduced/simplified CDD are overly broad—providing a full exemption from CDD

		in respect of financial institutions from certain countries (not just reduced); this is not based on an actual risk assessment, either by the UK itself or by the financial institution, which would confirm the assumption of low risk. • The exemption from CDD within the context of a business relationship could still apply when money laundering is suspected. • Once the business relationship has commenced, it is not a specific requirement to terminate the business relationship if proper CDD cannot be conducted. • There is no enforceable obligation to apply CDD to existing customers on the basis of materiality and risk. • A number of measures are mentioned only in JMLSG guidance and have no significance in respect of MSBs or the non-supervised sector other than as guidance.
R.6	**NC**	• No currently enforceable obligations with regards to PEPs.
R.7	**NC**	• No currently enforceable obligations pertaining to correspondent banking.
R.8	**C**	

3.3 Third parties and introduced business (R.9)

3.3.1 Description and Analysis

Recommendation 9

604. The principle of using the verification work carried out by intermediaries or other third parties to meet a financial institution's identity verification obligations in respect of introduced business is an established UK practice *inter alia* between product providers (e.g. life insurers and collective investment scheme operators), independent intermediaries (including stockbrokers) and in the derivative sector between executing and clearing brokers.

605. The legal basis for introduced business is MLR 5(3). This allows for an exemption from the obligation to take steps to obtain evidence of any person's identity when: "A [the financial institution] carries out a one-off transaction with or for a third party pursuant to an introduction effected by a person who has provided a written assurance that evidence of the identity of all third parties introduced by him will have been obtained." The financial institution must have reasonable grounds for believing that the introducer is a "financial institution" (i.e. covering the whole range of financial activities under MLR 2(2) a-e except money service operators) in the UK or in comparable jurisdictions covered by the 2nd Money Laundering Directive (i.e. the EEA), or are supervised by an overseas regulatory authority outside the EEA for AML/CFT rules comparable to the 2nd MLD.

606. For financial institutions subject to JMLSG Guidance (paragraph 5.5.26), this is further expanded: "Confirmations may only be accepted from another regulated firm carrying on appropriately regulated business. The assessment as to whether or not a firm should accept confirmation from an intermediary that a customer's identity has been verified will be risk-based, and cannot be based simply on a single factor." Where financial institutions use the verification work carried out by a third party, the confirmation is provided at the time the application is made for the customer to enter into the transaction or arrangement. These confirmations have been widely standardised – example forms of a certificate that confirms the identification are shown as Annexes to the JMLSG guidance. The pro-forma certificates for corporate and other non-personal entities require the provision for the following ID data:

- Full name of customer
- Type of entity
- Location of business (full operating address)
- Registered office in country of incorporation
- Registered number if any (or appropriate)

- Relevant company registry or regulated market listing authority
- Names of directors (or equivalent)
- Names of principal beneficial owners (over 25%)

607. The information provided only makes limited references to beneficial owners (i.e. for certain businesses and not all customers). There is no current enforceable requirement that the financial institutions be satisfied that the introducer will make ID and other relevant documentation available upon request. (This fact is also repeated in the JMLSG Guidance.) But JMLSG Guidance makes clear that it would be good practice on the part of an intermediary to accede to a request, if, exceptionally, one is made as part of a firm's risk-based customer acceptance procedures. Where a firm makes such a request, and it is not met, it will need to take account of that fact in its assessment of the intermediary in question, and of the acceptability of the intermediary's confirmations. The JMLSG Guidance explicitly directs firms to only accept third party confirmation where their own risk analysis procedures have been satisfied (para 5.5.26) – and recommends that firms factor into that analysis the willingness of the third party to disclose relevant documentation (para 5.5.33).

608. Under the Third Money Laundering Directive, when implemented in the UK, there will be a legal requirement on an intermediary to make identification data available on request to a firm relying on its confirmation.

609. Therefore, financial institutions are not required to satisfy themselves that the third party is regulated and supervised (in accordance with Recommendation 23, 24 and 29), and has measures in place to comply with, the CDD requirements. The financial institution itself can rely on all the introducers mentioned (e.g. authorised in the UK, or from another EAA or comparable jurisdiction) without making any specific AML/CFT risk assessment.

610. In determining in which countries the third party that meets the conditions can be based, competent authorities only to some extent take into account information available on whether those countries adequately apply the FATF Recommendations. Treasury under Regulation 28 of the MLRs can issue specific advisory notices to direct financial institutions not to undertake relevant business with customers from a specific jurisdiction. It has also issued advisories about jurisdictions of concern, the last example being advice about Nauru in 2001 (see http://www.hm-treasury.gov.uk./newsroom_and_speeches/press/2001/press_145_01.cfm). The Regulation 28 power would only exclude countries which are subject to FATF countermeasures. For all other countries, the general rules from the MLRs would apply.

611. The JMLSG Guidance states:

> An MLRO should ensure that the firm obtains, and makes appropriate use of, any government or FATF findings concerning the approach to money laundering prevention in particular countries or jurisdictions. This is especially relevant where the approach has been found to be materially deficient by FATF. Reports on the mutual evaluations carried out by the FATF can be found at www.fatf-gafi.org. FATF-style regional bodies also evaluate their members. Not all evaluation reports are published (although there is a presumption that those in respect of FATF members will be). Where an evaluation has been carried out and the findings are not published, firms will take this fact into account in assessing the money laundering and terrorist financing risks posed by the jurisdiction in question. Depending on the firm's area of operation, it may be appropriate to take account of other international findings, such as those by the IMF or World Bank.

612. The JMLSG provides additional guidance, *"The assessment of AML/CFT standards in other countries"*, which explains what constitutes a comparable jurisdiction; sets out different categories of countries which are comparable jurisdictions; provides guidance on how to assess AML/CFT standards in countries which are comparable jurisdictions; sets out the current status of NCCTs; and provides details of UK prohibition notices in respect of countries with material deficiencies. Financial

institutions should take account of this guidance when considering using the verification work carried out by third parties.

613. On occasions, the FSA has communicated to the financial sector counter-measures taken in international jurisdictions against specific financial institutions. In practice, financial institutions have indicated that they would tend to be either extremely restrictive and only accept introducers within the UK, or accept all EU and FATF countries as comparable jurisdictions, but would check on their individual introducers themselves to ensure a certain degree of reliability or quality to allow for a smooth working relationship. They would also be reluctant to work with an introducer who has shown itself in any way unreliable.

614. The UK arrangements for using the verification work carried out by third parties are established on the principle that ultimate responsibility for customer ID and verification remains with the relying institution, although there is nothing explicit in this regard.

3.3.2 Recommendations and Comments

615. The UK system legally allows for a very wide use of introducers. A number of requirements called for by FATF Recommendation 9 are not implemented in enforceable documents: identification data is not passed on in the standardized introduction certificates, there is no requirement to make ID data available, and no requirement to assess the regime of another country before allowing for introductions from other FATF or EEA member countries. In practice, financial institutions seem to carefully choose their introducers and cooperate – based on the legal possibilities – only with those they find reliable.

616. Nevertheless, UK authorities should make more explicit requirements for financial institutions to immediately obtain from the third party all the necessary information concerning certain elements of the CDD process, to take adequate steps to satisfy themselves that copies of identification data and other relevant documentation relating to CDD requirements will be made available from the third party upon request without delay, and for financial institutions to accept introducers pursuant to its assessment of AML/CFT adequacy. Much of this will be achieved by the implementation of the 3rd EU Money Laundering Directive.

3.3.3 Compliance with Recommendation 9

	Rating	Summary of factors underlying rating
R.9	**PC**	• The information provided concerning the CDD process makes only a limited reference to beneficial owners (i.e. for certain businesses and not all customers. • There is no enforceable requirement that the financial institutions be satisfied that the introducer will make ID and other relevant documentation available upon request. • Financial institutions are not required to satisfy themselves that the third party is regulated and supervised (in accordance with Recommendation 23, 24 and 29), and has measures in place to comply with, the CDD requirements. • In determining in which countries the third party that meets the conditions can be based, competent authorities only to some extent take into account information available on whether those countries adequately apply the FATF Recommendations.

3.4 Financial institution secrecy or confidentiality (R.4)

3.4.1 Description and Analysis

Recommendation 4

617. There are no financial institution secrecy laws in the UK that inhibit the implementation of the FATF Recommendations. MLRs Regulation 26(5) specifically provides that where a supervisory authority reports evidence of money laundering to the police then this is not taken to breach any restriction on the disclosure of information. MLRs Regulation 26(5) states that "A disclosure made under this regulation is not to be taken to breach any restriction on the disclosure of information (however imposed)."

Duty of banking confidentiality

618. A bank's duty of confidentiality under English law was laid down by the Court of Appeal in Tournier v. National Provincial and Union Bank of England ([1924] 1KB 461). Tournier affirmed the legal duty of a bank not to disclose client information but specified four exemptions to the duty. The first of these is relevant in this instance being where disclosure is under exemption by law. This exception to client confidentiality may be exercised where a bank is subject to a court order, or a statutory requirement to provide information.

Ability of competent authorities to access information

619. The FSA has comprehensive powers to require the production of information and documents from persons, including from persons outside of the regulated community. Its wide range of powers includes the power to compel, from any person, (i.e. not just regulated financial institutions or individuals) such information and documents as the investigator may require for the purposes of the investigation and also to attend before the investigator at a specified time and place to answer questions.

Sharing of information with other competent authorities internationally and domestically

620. The FSA has adequate authority to share information when appropriate. See the description under Recommendation 31, which sets out the regime under FSMA for the disclosure of confidential information and Recommendation 40, which sets out the FSA's duty to co-operate with overseas regulators.

621. The confidentiality regime set up under FSMA, Part XXII, section 348 (and regulations made under section 349) includes a number of exceptions or "gateways" allowing the FSA to disclose to other UK bodies with financial crime interests information it has obtained, whether voluntarily or using compulsory powers..

Sharing of information between financial institutions

622. There are no restrictions on the sharing of information between financial institutions where this is required by R.7 (correspondent banking) and R.9 (third parties and introduced business). Regarding wire transfers, EC Regulation No 1781/2006 came into force in December 2006, and includes requirements for wire transfers to contain information on customer's name, address, and account number.

Data Protection Act (DPA)

623. The DPA implements the Data Protection Directive into UK law. One of its requirements is that all personal data processing (which includes sharing of information) be conducted fairly and

lawfully. For any personal data to be shared, one of a list of conditions in Schedule 2 of the Act must be met. If information is 'sensitive' personal data, one of a further set of conditions in Schedule 3 of the Act must be met. Among the conditions for processing listed in Schedules 2 and 3 is the requirement that the processing is necessary for the exercise of any functions conferred on any person (such as the FSA or the police) by or under an enactment.

624. The DPA also imposes a restriction on transferring personal data outside the European Economic Area unless that state ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data. Schedule 4 of the DPA identifies a number of cases in which personal data may be transferred outside the EEA. These include situations in which the transfer is necessary for reasons of substantial public interest. The FSA ensures an adequate level of protection in non-EEA states by putting in place 'Memorandum of Understanding' with organisations in the country of destination.

HMRC

625. HMRC has a statutory authority to obtain information from MSBs under MLRs Regulation 15(2)(a) and (b) and HMRC also has coercive powers under Regulation 16 to obtain a court order to access any recorded information. HM Revenue & Customs officials may not disclose information they obtain in the course of carrying out their duties unless there is a lawful authority for that disclosure. There are various forms of lawful authority that permit disclosure to other competent authorities in the furtherance of HMRC's AML and CTF activities. For example, HMRC may make disclosures if it is necessary in order to perform a function of HMRC. In certain circumstances this may include disclosure of information to the other supervisory bodies.

3.4.2 Recommendations and Comments

626. The recommendation is fully met.

3.4.3 Compliance with Recommendation 4

	Rating	Summary of factors underlying rating
R.4	C	

3.5 Record keeping and wire transfer rules (R.10 & SR.VII)

3.5.1 Description and Analysis

Recommendation 10

627. Under MLRs Regulation 6(4) records on transactions must be kept for a period of 5 years from the date of the transaction. MLRs Regulation 6(4) requires that: "In relation to the records mentioned in paragraph (2)(b), the period is at least five years commencing with the date on which all activities taking place in the course of the transaction in question were completed." MLRs Regulation 6(2)(b) requires: "A record containing details relating to all transactions carried out by A [the financial institution] in the course of relevant business.

628. HMRC Guidance, MSB2, section 10 deals with record keeping. Paragraph 10.3 states that "the records that you keep must be sufficient to form a complete audit trail… Photographic evidence is particularly valuable; legible copies of the forms of identification presented or details of where the copies of identification can be found, which should be filed and easily recoverable. You must keep these records for at least five years from the date when the relationship with your customer finishes."

Regarding business records, "You must keep a record of all transactions, regardless of whether the ID of the customer or client needed to be verified, for five years. All records of your disclosures. Letters received from [SOCA] or any other correspondence with a law enforcement agency, should be retained for at least five years.

629. It is generally required that transaction records be sufficient to permit reconstruction of individual transactions so as to provide, if necessary, evidence for prosecution of criminal activity. The FSA Handbook (SYSC 3.2.20 R) requires financial institutions to take reasonable care to make and retain adequate records: (1) A firm must take reasonable care to make and retain adequate records of matters and dealings (including accounting records) which are the subject of requirements and standards under the regulatory system…"

630. JMLSG Guidance, Part I, Chapter 9, paragraph 9.14 states that: "All transactions carried out on behalf of or with a customer in the course of relevant business must be recorded within the firm's records. Transaction records in support of entries in the accounts, in whatever form they are used, e.g. credit/debit slips, cheques, should be maintained in a form from which a satisfactory audit trail may be compiled where necessary, and which may establish a financial profile of any suspect account or customer."

631. HMRC Guidance, MSB2, section 10.1 states: "The purpose of keeping records is to enable law enforcement to reconstruct business transactions; often well after the original business has been concluded. In making and retaining records you should have in mind the need to provide a clear audit trail of the business you have conducted."

632. MLRs Regulation 6(2)(a) and 6(3) require that evidence of identity for at least five years after the end of the end of the business relationship or five years after a one-off transaction has been completed. Furthermore, the FSA Handbook, SYSC 3.2.20 R requires financial institutions to take reasonable care to make and retain adequate records: "(1) A firm must take reasonable care to make and retain adequate records of matters and dealings (including accounting records) which are the subject of requirements and standards under the regulatory system." Therefore, the requirement to maintain accounting records appears adequately covered.

633. With regard to a requirement to maintain business correspondence, this appears adequately covered through tax legislation and in practice. The VAT Act 1994 sets out the VAT records that should be kept and specifies a six-year retention period. The regulations to the Act allow the Commissioners to expand up the definition of "records" by means of public notices; HMRC Notice 700/21 includes a wide range of business records to be kept, including "relevant business correspondence." In addition, the JMLSG Guidance, Part I, Chapter 9, paragraph 9.9 states that a financial institution may hold additional information in respect of a customer for the purposes of wider customer due diligence: "A firm may often hold additional information in respect of a customer for the purposes of wider customer due diligence." Additional information could be interpreted as business files and correspondence in relation to a particular customer.

634. Production orders under POCA will require information including customer and transaction records to be made available to competent authorities where appropriate. Law enforcement agencies claim that their experience is that a very broad range of information, including business correspondence, can normally be accessed through production orders, indicating that substantial records are kept. Also, JMLSG Guidance, Part I, Chapter 9, paragraph 9.24 acknowledges that the overriding objective is for financial institutions to be able to retrieve relevant information without undue delay: "The ML Regulations do not state where relevant records should be kept, but the overriding objective is for firms to be able to retrieve relevant information without undue delay."

635. JMLSG Guidance, Part I, Chapter 9, paragraph 9.25 addresses identification records held outside the UK, and highlights the fact that UK records have to meet UK requirements.

Special Recommendation VII

636. As member of the European Union, the UK is bound by the "Regulation (EC) No. 1781/2006 of the European Parliament and of the Council of 15 November 2006 on information on the payer accompanying transfers" in force since 1 January 2007. As an EC Regulation, this instrument is directly applicable in the UK and further implementation is therefore limited mainly to the establishment of an appropriate monitoring regime, and an enforcement and penalties regime applying from 15 December 2007 (see Articles 15 and 20 of the Regulation) and to clarifying the position in relation to derogations.

Scope and exemptions

637. The EU Regulation applies to transfers of funds, in any currency, which are sent or received by a payment service provider established in the European Community. In line with the exemptions set out in SR.VII, the Regulation is not intended to apply to the following types of payment (Article 3.2):

- any transfer of funds carried out using a credit or debit card provided that a unique identifier20, allowing the transaction to be traced back to the payer21, accompanies the transfer. Where credit or debit cards are used as a payment system to effect a transfer of funds, this exemption does not apply because it is also subject to the proviso that the payee22 must have an agreement with the payment service provider permitting payment for the provision of goods or services.
- any transfers of funds where both the payer and the payee are payment service providers acting on their own behalf.

Threshold

638. The EU Regulation uses a threshold of EUR 1,000. This threshold applies in relation to: (i) the derogation for transfers of funds using electronic money (Article 3.3); (ii) the disapplication of the Regulation to transfers of funds within a Member State in certain prescribed circumstances (Article 3.6); (iii) transfers not from an account (Article 5.4, see below).

Obtaining originator information

639. Article 5(1) of the EU Regulation requires that payment service providers must ensure that transfers of funds are accompanied by complete information on the payer. The payment service provider shall verify the complete information on the payer on the basis of documents, data or information obtained from a reliable and independent source (Article 5(2). Complete information for this purpose is defined in Article 4 as the payer's: name; address (which may be substituted with the date and place of birth, customer identification number / national identity number); and account number or, where this does not exist, his unique identifier which allows the transaction to be traced back to the payer.

Verifying originator information

---

[20] In the EU Regulation, "*unique identifier*" means a "combination of letters, numbers or symbols, determined by the payment service provider, in accordance with the protocols of the payment and settlement system or messaging system used to effect the transfer of funds."

[21] In the EU Regulation, "*payer*" means either the natural or legal person who holds an account and allows a transfer of funds from that account, or, when there is no account, a natural or legal person who places an order for a transfer of funds.

[22] In the EU Regulation, "*payee*" means a natural or legal person who is the intended final recipient of transferred funds.

640. Article 5(2) of the EU Regulation requires the payment service provider of the payer, before transferring the funds, to verify the complete information on the payer on the basis of documents, data or information obtained from a reliable and independent source. This requirement is subject to Article 5(3) and (4).

641. Article 5(3) provides for circumstances in which, in the case of transfers from an account, verification may be deemed to have taken place. These are where:

- a payer's identity has been verified in connection with the opening of the account and the information gained by this verification has been stored in accordance with certain customer due diligence and storage obligations prescribed in the 3rd Money Laundering Directive (Article 8.223 and 30.a)24; or
- the payer falls within the scope of the Article in the 3rd Money Laundering Directive (Article 9.6) which provides that Member States must require institutions and persons covered by the Directive to apply customer due diligence procedures to all new customers and at appropriate times to existing customers on a risk-sensitive basis.

642. Article 5(4) provides for circumstances in which, in the case of transfers not from an account, verification of information on the payer is not required – where: (i) the amount does not exceed EUR 1,000; or (ii) the transaction is not carried out in several operations that appear to be linked and together exceed EUR 1,000.

Transfers of funds within the Community

643. By way of derogation from Article 5(1), where both the payment service provider of the payer and the payment service provider of the payee are situated in the Community, transfers of funds shall be required to be accompanied only by the account number of the payer or a unique identifier allowing the transaction to be traced back to the payer (Article 6 of the Regulation). However, if so requested by the payment service provider of the payee, the payment service provider of the payer shall make available to the payment service provider of the payee complete information on the payer, within three working days of receiving that request.

Maintaining originator information

644. Article 5(5) of the EU Regulation requires the payment service provider of the payer to keep records for five years of complete information on the payer which accompanies transfers of funds.

Cross-border wire transfers

645. Article 7(1) of the EU Regulation requires that transfers of funds where the payment service provider of the payee is situated outside the Community must be accompanied by complete information on the payer. Article 7(2) provides an exception to the requirement in Article 7(1) in relation to cross-border batch file transfers but only where these are from a single payer. The effect of this exception is that the cross-border transfer requirement in Article 7(1) does not apply to the

[23] Article 8.2 sets out : "*the institutions and persons covered by this Directive shall apply each of the customer due diligence requirements set out in paragraph 1, but may determine the extent of such measures on a risk-sensitive basis depending on the type of customer, business relationship, product or transaction. The institutions and persons covered by this Directive shall be able to demonstrate to the competent authorities mentioned in Article 37, including self-regulatory bodies, that the extent of the measures is appropriate in view of the risks of money laundering and terrorist financing.*"

[24] Article 30.a sets out: "*Member States shall require the institutions and persons covered by this Directive to keep the following documents and information for use in any investigation into, or analysis of, possible money laundering or terrorist financing by the FIU or by other competent authorities in accordance with national law: (a) in the case of the customer due diligence, a copy or the references of the evidence required, for a period of at least five years after the business relationship with their customer has ended*".

individual transfers bundled together within the batch file provided that (i) the batch file contains the complete information; and (ii) the individual transfers carry the account number of the payer or a unique identifier. Therefore, where this exception applies, the requirements for domestic wire transfers must still be met (see below).

Domestic wire transfers

646. Article 6 of the EU Regulation provides for derogation for domestic wire transfers from the requirement for payment service providers to ensure that transfers of funds are accompanied by complete information on the payer. Such transfers are only required to be accompanied by the account number of the payer or where the account number does not exist, a unique identifier allowing the transaction to be traced back to the payer. Article 6 also provides that if so requested by the payment service provider of the payee, the payment service provider of the payer must make available to the payment service provider of the payee complete information on the payer within three working days of receiving that request.

647. In addition, Article 14 provides that payment service providers must respond fully and without delay, in accordance with the procedural requirements established in the national law of their Member State, to enquiries from the competent authorities responsible for combating money laundering or terrorist financing concerning the information on the payer accompanying transfers of funds and corresponding records.

Transmission of information by intermediaries

648. Article 12 of the EU Regulation requires intermediary payment service providers to ensure that all received information is kept with the transfer.

Technical limitations

649. Article 13(5) requires the intermediary payment service provider to keep records for five years of all information received where technical limitations prevent information on the payer from accompanying the transfer of funds.

Wire transfers not accompanied by complete originator information

650. Article 8 of the EU Regulation requires the payment service provider of the payee to detect that fields within the messaging or payment and settlement system used to effect the transfer in respect of the information on the payer have been completed in accordance with the characters or inputs admissible within the conventions of that messaging system. Under this Article, the payment service provider of the payee is required to have effective procedures in place to detect a lack of presence of the required information on the payer.

651. Article 9 sets out the obligations of the payment service provider of a payee who becomes aware that the required information on the payer is missing or incomplete and provides that it must either reject the transfer or ask for complete information on the payer and comply with any applicable law, administrative provisions and national implementing measures. Where a payment service provider regularly fails to supply the required information on the payer, this Article also requires the payment service provider of a payee (i) to take steps which may include restricting or terminating the business relationship, and (ii) to report that fact to the authorities.

652. In addition, Article 10 ("Risk-based assessment") requires the payment service provider of the payer to consider incomplete information on the payer as a factor in assessing whether the transfer of funds, or any related transaction is suspicious, and whether it must be reported, in accordance with the reporting obligations set out in Chapter 3 of the 3rd Money Laundering Directive, to authorities responsible for combating money laundering or terrorist financing.

Compliance monitoring and sanctions

653. In line with the second paragraph of Article 15, the UK must require competent authorities to effectively monitor and take necessary measures with a view to ensuring compliance with the Regulation. The first paragraph of Article 15 provides that the UK must lay down the rules on penalties applicable to infringements of the provisions of the Regulation and take all measures necessary to ensure that they are implemented. It also provides that the penalties must apply from 15th December 2007.

654. The FSA has been in discussions with HMT on the development of an enforcement regime in relation to the EU Regulation on information on the payer accompanying transfers of funds. This has included consideration of how sanctions and penalties can be applied to non-compliant FSA-regulated financial institutions. The FSA will be assessing and adapting its internal procedures for applying enforcement measures, and the corresponding accountability mechanisms that will allow the FSA's decisions to be subject to appropriate review should this be necessary. The sanctions regime will come into effect as per the date set by the Regulation: 15 December 2007. Therefore, currently there is no effective and dissuasive sanctions regime in place, and since no sanctions can currently be applied it is doubtful as to whether any "enforceable obligations" are in place before 15 December 2007.

655. The FSA's approach to assessing firms' compliance with the EU Regulation will be considered as part of business-as-usual supervision of firms. Formal training for FSA staff will begin in autumn 2007. The authorisation process by which firms can apply to be regulated by the FSA has been amended so that applicants must inform the FSA if they will be subject to the Regulation.

3.5.2 Recommendations and Comments

656. *SR VII*. The UK fully relies on the implementation of the EU Regulation on the payer accompanying transfers of funds that is in force since 1 January 2007. The Regulation meets the technical requirements as set out in SR.VII (obtaining and verifying originator information; maintaining full originator information for cross-border transfers; accompanying domestic wire transfers with more limited originator information and made full originator information available within three days; adopting specific procedures for identifying and handling wire transfers not accompanied by full originator information; compliance monitoring and sanctions).

657. However, the EU Regulation classifies wire transfers within the EU as domestic and therefore subjects those transfers to the domestic regime under SR.VII. The FATF defines domestic transfers as "any wire transfers where the originator and beneficiary institutions are located in the same jurisdiction. This term therefore refers to any chain of wire transfers that takes place entirely within the borders of a single jurisdiction, even though the system used to effect the wire transfer may be located in another jurisdiction". On the contrary, cross-border wire transfers means "any wire transfer where the originator and beneficiary institutions are located in different jurisdictions. This term also refers to any chain of wire transfers that has at least one cross-border element".

658. The derogation set out in the EU regulation is not in compliance with the FATF requirement applicable to domestic wire transfers in that Article 6.1 of the EU regulation does not meet the objectives of the FATF standards in relation to SR.VII. The intention in SR.VII is clearly to establish a distinct regime for the transfers operated nationally (under C.VII.3) where obtaining full originator information (either by the beneficiary institution of by law enforcement authorities) can be done on a timely basis. The cross-border element in a non-domestic wire transfer is as an obstacle for timely access to the full originator information. There are doubts about the practicality of the three working days rule in the EU context (it is not certain that the exchange of full originator information between a law enforcement authority in country A with a financial institution in a country B could be systematically timely).

659. The BBA has already published guidelines in this area on its website; the JMLSG website has drawn the attention of all JMLSG users to this guidance. Credit institutions should adopt effective risk-based procedures for identifying and handling wire transfers that are not accompanied by complete originator information. In the absence of an effective AML/CFT supervision, the assessors have doubts about the existence of a proper compliance monitoring of financial institutions with the requirements set out in the EU Regulation. Finally and by December 2007, the UK authorities should adopt effective, proportionate and dissuasive sanctions applicable to infringements of the provision laid down on the EU Regulation.

3.5.3 Compliance with Recommendation 10 and Special Recommendation VII

	Rating	Summary of factors underlying rating
R.10	**C**	
SR.VII	**PC**	• The derogation set out in the EU regulation for wire transfers within the EU (classified as domestic transfers) is not in compliance with the FATF requirements under SR.VII. [25] • The sanctions regime is not effective or dissuasive; since no sanctions can currently be applied it is doubtful as to whether any "enforceable obligations" are in place before 15 December 2007. • In terms of effectiveness, there are doubts about the current implementation of the very recent EU requirements, including the requirement to have in place effective risk-based procedures for identifying and handling wire transfers that are not accompanied by complete originator information, and about the existence of an effective compliance monitoring of financial institutions.

[25] The FATF decided at the June 2007 Plenary to further consider this subject.

Unusual, Suspicious and other Transactions

3.6 Monitoring of transactions and relationships (R.11 & 21)

3.6.1 Description and Analysis

Recommendation 11

660. As mentioned above in paragraphs 538 to 542, the UK authorities derive from the requirements for monitoring though MLRs Regulation 3(1)(b); the reporting obligations under the POCA sections 330 and 331; the reporting obligations under section 21A of the TACT; and the FSA Handbook, SYSC 3.2.6 R that financial institutions will establish and maintain an appropriate approach to enable them to detect transactions and activity that may indicate money laundering or terrorist financing. The JMLSG Guidance, Part I, Chapter 6, includes guidance on monitoring customer activity and treats it as an essential component of anti-money laundering controls; however, the Guidance itself makes clear in para 6.1. that "there is no specific legal or regulatory requirement that customers' activities be monitored… but having regard to the following obligations:

- the general requirement to establish appropriate procedures of internal control for the purposes of forestalling and preventing money laundering/terrorist financing
- the requirement to report knowledge or suspicion of possible money laundering/terrorist financing
- the 'reasonable grounds' test for making such reports under POCA and the Terrorism Act

there is an expectation that, where the situation so warrants (see paragraph 6.9), a firm will establish and maintain an appropriate approach to enable it to detect transactions or activity that may indicate money laundering or terrorist financing."

661. Thus, there is no specific obligation to pay special attention to all complex, unusual large transactions, or unusual patterns of transactions, that have no apparent or visible economic or lawful purpose. However, JMLSG Guidance encourages financial institutions, in the context of the risk-based approach and the requirements to have adequate systems and controls to combat ML, to have monitoring systems and provides examples of situations where staff should pay special attention and ask further questions. UK authorities also point out that under the FSA Rules, SYSC 3.2.6 R and 3.2.6A R financial institutions are required to have adequate systems and controls in order to counter the risk that the firms might be used to further financial crime, and that the firm must ensure that these systems and controls "enable it to identify, assess, monitor, and manage money laundering risk."

662. The JMLSG Guidance states that financial institutions should monitor customer activity and transactions, including certain areas mentioned as examples in FATF Recommendation 11. It states in paragraph 6.10:

Effective monitoring is likely to be based on a considered identification of transaction characteristics, such as:

- the unusual nature of a transaction: e.g., abnormal size or frequency for that customer or peer group; the early surrender of an insurance policy;
- the nature of a series of transactions: for example, a number of cash credits;
- the geographic destination or origin of a payment: for example, to or from a high-risk country; and
- the parties concerned: for example, a request to make a payment to or from a person on a sanctions list.

663. Paragraph 5.6.2 (in section 5.6: "KYC Additional customer information") of the JMLSG Guidance states:

As a part of a risk-based approach, therefore, firms may need to hold sufficient information about the circumstances and business of their customers for two principal reasons:

- to inform its risk assessment process, and thus manage its money laundering/terrorist financing risks effectively; and
- to provide a basis for monitoring customer activity and transactions, thus increasing the likelihood that they will detect the use of their products and services for money laundering and terrorist financing.

664. According to the UK authorities, it is clear from the SARs received by the UK FIU that financial institutions understand their responsibilities under POCA and indicate that there is on-going monitoring of customer activity and transactions.

665. There is no specific requirement to examine as far as possible the background and purpose of such transactions and to set forth findings in writing. UK authorities point out that SYSC 3.2.20 R, requires firms to "take reasonable care to make and retain adequate records of matters and dealings which are the subject of requirements and standards under the regulatory system." The JMLSG Guidance, Part I, Chapter 9, paragraphs 9.17-9.19 states financial institutions should retain internal and external reports as well as information or material concerning possible money laundering even where a report has not been made to [UK FIU]. A firm should make and retain: (1) records of actions taken under the internal and external reporting requirements; and (2) when the nominated officer has considered information or other material concerning possible money laundering, but has not made a report to [UK FIU], a record of the other material that was considered. In addition, copies of any SARs made to [UK FIU] should be retained. UK FIU analysis of SARs received suggests that the majority of the financial institutions that submit SARs are conducting at least a basic level of research and analysis prior to submission, and in some cases undertake quite substantial pre-submission examination. UK law enforcement experience is that, when investigating money laundering, a useful source of data is a firm's archive material on undisclosed SARs.

666. Financial institutions are not specifically required to keep such findings available for competent authorities and auditors for at least five years. JMLSG Guidance, Part I, Chapter 9, paragraph 9.19 states that "Records of all internal and external reports should be retained for five years from the date the report was made." HMRC Guidance, MSB2 Guidance, paragraph 10.3 states that "All records of your disclosures: letters from [SOCA] or any other correspondence with a law enforcement agency should be retained for at least five years."

Recommendation 21

667. There are no provisions which direct UK entities to act in a certain way against certain countries below the threshold of FATF counter-measures, and there is no legal requirement for financial institutions to give special attention to business with countries which do not sufficiently apply FATF Recommendations.

668. The separate JMLSG Guidance on: "*The assessment of AML/CFT standards in other countries*" sets out:

- which countries can be regarded as comparable jurisdictions, i.e. where simplified due diligence and exemptions are allowed, and to which extent this can be used. The UK considers all FATF member states as comparable jurisdictions.
- which countries cannot be regarded as comparable jurisdictions. This includes FATF's current and past list of Non Co-operative Countries and Territories (this guidance was last updated in January 2006), and information about those countries with material deficiencies in AML procedures that have been the subject of advisory notices from the FATF and UK Government in recent years.

669. The guidance indicates that financial institutions should have in place additional monitoring procedures for transactions from countries that remain NCCT classified and correspondent relationships with financial institutions from countries on the NCCT list. When considering what additional procedures are required, financial institutions will take into account FATF assessments of the progress that has been made.

670. The JMLSG Guidance states that: "Firms considering business relations and transactions with individuals and firms – whether direct or through correspondents - located in higher risk jurisdictions, or jurisdictions against which the UK has outstanding advisory notices, should take account of the background against which the assessment, or the specific recommendations contained in the advisory notices, have been made." The JMLSG guidance states, at paragraph 3.23, that an MLRO should ensure that the firm obtains, and makes appropriate use of, any government or FATF findings concerning the approach to money laundering prevention in particular countries or jurisdictions.

671. The guidance is regularly updated via the JMLSG's website: http://www.bba.org.uk/bba/jsp/polopoly.jsp?d=362&a=7644. Given this guidance, it appears that there are measures in place to help financial institutions to be advised of concerns about weaknesses in the AML/CFT systems of other countries.

672. As with Recommendation 11, there is no specific requirement to examine as far as possible the background and purpose of such transactions, and make written findings available for authorities. However, for the FSA regulated sector, there is guidance in JMLSG which seems to be well received by larger firms. The JMLSG Guidance states that financial institutions should monitor customer activity and transactions in a way that is appropriate to their business. One characteristic which is pointed out to firms is the geographic destination or origin of a payment.

673. The UK authorities are able to apply appropriate counter-measures where a country continues not to apply or insufficiently applies the FATF Recommendations. Under MLRs Regulation 28, the Treasury may direct that a financial institution not enter a business relationship or carry out a one-off transaction in relation to a person who is based or incorporated in a country (other than an EEA state) to which the FATF has decided to apply countermeasures. The Treasury has not utilised this power to date; UK authorities indicate that the FATF NCCT list has been sufficiently effective so as to render UK enforcement redundant. The Treasury has also issued press releases / advisory notices drawing attention to the NCCT list and other issues of particular concern. According to the UK authorities, this power could also apply to any other jurisdiction designated by the FATF as inadequately applying the FATF Recommendations.

3.6.2 Recommendations and Comments

674. *Recommendation 11:* There is no explicit legal or regulatory obligation to monitor transactions. UK authorities should adopt more specific requirements to monitor all complex, unusual large transactions, etc, and to make out findings in writing. The intention of the UK authorities is to include such obligation in the future, when the 3rd ML Directive of the EU is implemented.

675. However, the JMLSG Guidance – which does not connect back to a high level obligation related to this requirement – covers much of the substance of monitoring, and the FSA regulated institutions which are at higher risk seem to follow the guidance quite effectively. This is the effect of good cooperation with the authorities, good outreach by SOCA which seems to explain well what type of transactions and activities should be a subject of concern for financial institutions, and a generally high standard of observance in the larger financial sector players. However, the sectors not covered by JMLSG Guidance are not under any obligation related to ongoing monitoring, as is the case for instance for MSBs.

676. *Recommendation 21:* The UK authorities should adopt more specific requirements dealing with monitoring transactions involving certain countries and making findings in writing. While this is

encouraged through comprehensive guidance, guidance only applies to JMSLG covered entities, not to the whole financial sector. As with Recommendation 11, the UK authorities plan to address this through implementation of the 3rd EU Directive.

3.6.3 Compliance with Recommendations 11 & 21

	Rating	Summary of factors underlying rating
R.11	**PC**	• There is no specific obligation to pay special attention to all complex, unusual large transactions, or unusual patterns of transactions, that have no apparent or visible economic or lawful purpose. The expectation in guidance only covers the JMLSG covered part of the financial sector. • There is no specific requirement to examine as far as possible the background and purpose of such transactions and to set forth findings in writing.
R.21	**PC**	• There is no requirement for financial institutions to give special attention to business with countries which do not sufficiently apply FATF Recommendations. MLR 28 only covers FATF countermeasures, and the guidance of JMLSG only covers part of the financial sector. • No specific requirement to examine as far as possible the background and purpose of such transactions, and make written findings available for authorities.

3.7 Suspicious transaction and other reporting (R.13-14, 19, 25 & SR.IV)

3.7.1 Description and Analysis

Recommendation 13 & Special Recommendation IV

677. The legal obligation on the regulated sector to submit suspicious activity reports is set out in sections 330-331 of POCA (as amended by SOCPA). There is no *de minimis* limit; nor is there a specification for transaction data: the report can be on suspicious activity, thus ensuring the widest possible scope for reporting. Section 330 POCA makes it an offence for someone working in the regulated sector who knows or suspects or has reasonable grounds for knowing or suspecting that another person is engaged in money laundering, not to disclose this either to their institution's "nominated officer" or directly to the UK FIU. The "nominated officer" (often referred to as the Money Laundering Reporting Officer, or MLRO) is the person designated by the institution to receive internal money laundering reports and to forward those to the UK FIU.

678. Section 331 of POCA makes it an offence for the nominated officer of a firm undertaking business in the regulated sector not to make a disclosure to SOCA where the officer receives an internal disclosure and knows or suspects or has reasonable grounds for knowing or suspecting that another person is engaged in money laundering. Schedule 9 of POCA defines business in the regulated sector and covers the full range of activities that would be expected to be undertaken by a "financial institution" in the FATF definition.

679. As indicated under the discussion of Recommendation 26, where firms have the opportunity to delay or stop a transaction they suspect of being involved in money laundering/terrorist financing, they must do so and seek "consent" from the UK FIU. The FIU then has seven days to determine (usually after liaising with law enforcement) whether or not to grant consent for the transaction to continue. (For a more thorough discussion of the consent process, see section 2.6.) A request for "consent" under POCA is also a form of suspicious activity report, since it is made by a financial institution to the UK FIU, and the UK FIU keeps a record of the issue (whether or not the consent is granted or refused). As indicated under Recommendation 26, overall the consent system is useful. However, there are some concerns regarding its current set up and implementation: the fact that, after a SAR has been filed, banks are currently obliged to seek consent on every subsequent transaction (over 250 pounds) for that same customer is difficult for the private sector to implement fully.

680. The legal obligation on the regulated sector to submit suspicious activity reports in relation to terrorism and terrorist financing is set out at Section 21A of TACT. (Section 21A was added to the TACT by way of the Anti Terrorism Crime and Security Act, Schedule 2, Part 3.) This makes in an offence for someone working in the regulated sector who knows or suspects or has reasonable grounds for knowing or suspecting that another person has committed an offence under sections 15-18 of TACT (i.e., terrorist financing offences), not to disclose this either to their institution's "nominated officer" or a constable. Section 20 of TACT also covers the non-regulated sector, in that any person "may disclose a suspicion or belief ….that arises in the course of trade, profession, business or employment….." Schedule 4, paragraph 126 of the Serious Organised Crime and Police Act 2005, amends TACT so that the nominating officer must now report to SOCA. For a full description of TACT and its scope, including the principal terrorist financing offences applicable in the UK, please refer to Section 2 above.

681. There are consent provisions within TACT very similar to those within POCA (although consent MUST be determined by a "Constable"), so the point about consent being a form of SAR in relation to money laundering also applies here.

682. SARs on terrorist financing suspicions are analysed by a specialist team within the UK FIU to assess whether further action is required. This analysis is based on intelligence shared with the UK FIU by both the police and the UK intelligence services. If the review reveals that further action is

required, an intelligence package based upon the SAR is put together and disseminated to specialist police unit the NTFIU. International requests from FIUs for CFT assistance are dealt with by the appropriate team within the UKFIU. There were eight requests for assistance on FT issues during 2005.

683. For both reporting money laundering and terrorist financing, the legislation is based on reporting suspicious activity and is not constrained by a 'transaction amount', or any *de minimis* limit. While the legislation does not specifically say that attempted transactions must be reported, the consent system clearly shows that attempted transactions are included as part of the reporting requirement. SOCPA Section 103 has amended POCA such that, in circumstances where the amount under consideration is less than £250, there is not an automatic duty to seek consent.

684. The obligation to report (whether for money laundering or terrorist financing) is not constrained by those activities which might involve tax matters. The money laundering offence covers all crime, including tax evasion; and all types of 'property' including real or personal, heritable or moveable; things in action and other intangible or incorporeal property.

Additional elements

685. The money laundering offence and corresponding reporting obligation are based on an "all crimes" approach. Financial institutions are required to report to the FIU when they suspect or have reasonable grounds to suspect that funds are the proceeds of all criminal acts that would constitute a predicate offence for money laundering domestically.

Recommendation 14

686. Sections 337 and 338 of POCA provide immunity from prosecution for those persons report suspicion of criminal conduct or criminal proceeds to the UK FIU in good faith, when identified through the course of their business, trade or profession. This covers both the regulated and non-regulated sectors. Section 21B of TACT similarly provides that any disclosure under section 21A does not breach any restriction on the disclosure of information (however imposed). This allows the regulated sector to disclose without breaching any other legal restriction that would normally apply.

687. In addition, Tournier Principles apply (see 3.4 above), in that banks have an overriding public duty to assist Police, and can legally disclose information about their customers if: compelled by law; it has a public duty; and the bank's own interests require disclosure and the customer agrees to that disclosure

688. SARs are governed by "tipping off" provisions (Section 333 of POCA) which make it an offence, having made a disclosure, to reveal information which is likely to prejudice any resulting law enforcement investigation.

Additional elements

689. The UK FIU enforces the confidentiality of SAR originator details. All persons involved in the use of SAR intelligence receive appropriate training. The UK FIU has also set up a confidential reporting "hot-line" whereby SAR originators can report suspicions or concerns regarding potential breaches of confidentiality and any such breaches are pursued by the UK FIU with the SAR user in order to mitigate the effects of that breach and to improve systems, all are then reported to the national body responsible for inspecting the performance of the law enforcement end-users (Her Majesty's Inspectorate of Constabularies). Annual statistics of reported breaches of confidentiality will be included in the FIU's Annual Report.

Recommendation 25 (guidance and feedback related to STRs)

690. UK FIU has posted guidance on the internet on how to complete a SAR and when a SAR should be considered. See http://www.soca.gov.uk/financialIntel/suspectActivity.html. The SOCA website also has a preferred form for electronic submission of suspicious activity reports and guidance on completion and submission, including SARs seeking consent.

691. The Lander Review of SARs also recommended that the existing UK FIU feedback programme should be overhauled and enhanced. This has resulted in the development of:

- a SARs Committee with sector representation to oversee the strategic direction of the SARs regime;
- a "vetted group" of public and private sector representatives with government security clearance to discuss confidential or sensitive issues in a closed forum;
- assorted sector-specific groups to discuss particular problems; and
- regulator forums where the UK FIU shares performance management data (i.e. volume of reporting) and guidance and feedback (quality of reporting) with regulators and regulatory bodies on a quarterly basis.

692. This feedback also makes use of sanitised case examples from closed investigations particularly where they have been instrumental in obtaining a successful conviction. Other examples of mechanisms of feedback utilised by the UK FIU include:

- **Seminars** conducted with regulators, government, and law enforcement.
- **Ongoing dialogue** with the Association of Chief Police Officers.
- **Meetings** with individual reporting sector institutions to provide generic advice in a one-to-one context.
- **Informal consultation** with public, private, and law enforcement representatives particularly on the impact of new policy or legislation.
- **Programme of presentations** to reporting sector to shape best practice.
- **Direct and published e-mail address** for ease of contact.
- **SAR quality assurance reviews**, conducted with individual financial institutions; including a detailed breakdown of number and quality of SARs submitted by the institution. Demand for these sessions has increased fourfold since 1 April 2006 and provide a platform for further dialogue.

693. The UK FIU endeavours to provide the private sector with timely indicators of potential terrorist related financial activity to ensure that the SARs filed with the UK FIU are of maximum usefulness. These are provided through periodic bulletins which are presented to the financial sector at meetings, conferences, seminars, and electronically, through the extranet system, Money Web. In 2005, UK FIU produced four profiles on CFT typologies, two of which were placed on the Egmont Secure Web (ESW).

694. Specific seminars and feedback from the seminars indicates that regime participants have welcomed SOCA's willingness for co-operation, and feedback has been positive. To date, 15 seminars have been held; of these, 9 seminars have been held in London, 6 mixed sector seminars (Banking, Law and Accountancy) have been held, 3 in Scotland and 3 in Leeds. Delegates focussed on SOCA's open and frank approach, with a clear willingness to listen and engage; and the good use of case studies. 91% of respondents rated the seminars as good to excellent and a delegate comment stated it "makes it all seem worthwhile".

695. General feedback and typologies provided to the reporting sectors therefore appears generally comprehensive; private sector representatives across the board noted a welcomed increase of outreach and feedback from the UK FIU since it was transferred to SOCA in April 2006.

696. The volume of SARs received by the UK FIU (200,000 per year) precludes specific case by case feedback in all cases; however, The UK FIU provides automatic acknowledgements of all SARs submitted by electronic means (85%). Additionally, SOCA replies to, and thereby acknowledges, all consent SARs submitted either electronically or on paper. Where a SAR has led to an investigation, it is likely that the reporting institution will indirectly receive feedback, in the form of requests for further information from law enforcement. SOCA does not routinely acknowledge the receipt of SARs that are submitted on paper (15%) and that do not require consent. In any case, the number of paper submissions are falling as electronic submission via SAR Online increases.

Recommendation 19

697. The UK has taken a policy decision not to apply a currency transaction reporting system. However, the UK has *considered* the feasibility and utility of implementing a system where financial institutions report all transactions in currency above a fixed threshold to a national central agency with a computerised database. Consultations on threshold–based reporting took place prior to the introduction of the Proceeds of Crime Act 2002. Key law enforcement agencies as well as financial institutions and regulators contributed to the consultation exercise. No evidence was found of support at that time for the introduction of a system which required the automatic reporting of transactions above a specified threshold.

698. More thorough consideration took place in December 2006, when the Home Office led a policy review on the feasibility and utility of implementing such a system. The review considered the impact on the FIU, law enforcement and financial institutions, and took into account the views of the financial services regulatory body (the FSA). The UKFIU also consulted informally with FIUs in other jurisdictions where a threshold based reporting system operates. The input from the departments and agencies consulted raised the following concerns:

- Awareness of AML controls amongst serious and organised criminals and the likelihood of smurfing below a given threshold to avoid detection;
- The likely decline in SARs that would result from financial institutions refocusing their risk models to incorporate a threshold that would be perceived as a Government statement of what constitutes high AML risk;
- Cost implications; both the financial institutions, who might split existing compliance functions to process the automatic reporting rather than take on more staff; and for UK FIU, and law enforcement agencies, in terms of the cost of establishing the new (IT) architecture handling the additional data;
- There would need to be criminal sanctions for non-compliance which could be disproportionate if the non reported transaction proved genuine;
- Absence of evidence that such a system would add benefit or improvement to the current SAR regime and difficulties over how a threshold amount would be determined.

699. In light of the above concerns there was agreement that:

- the UK money laundering reporting regime should be suspicion based, not value based (i.e. the concept that there is no one typology for money laundering);
- The suspicion based approach fits very well with the United Kingdom structures and those of its reporting sectors, who take a risk based approach. It is also compatible with law enforcement's intelligence-led approach to tackling crime, including money laundering;
- That the UK should not introduce threshold reporting as either a replacement or an addition to a suspicion based system.

700. The key findings of this review have been that: (i) the suspicion-based regime currently in place is widely considered to be more effective than any other option in the context of the UK anti-money

laundering strategy; and (ii) there is limited justification for the implementation of a fixed-threshold reporting regime on operational, financial, or policy grounds. In light of this recent review, the Home Office has concluded that the current policy regarding this issue should remain unchanged. The matter will be kept under review.

Statistics

701. The UK FIU, maintains an electronic database of all SARs ("ELMER", see section 2.5 above). Since not all SARs will cover specific transactions (e.g. a SAR might be generated by an attempt to open an account or retain the services of a legal adviser) it is not possible or necessary to interrogate ELMER by "value of SAR". Between the periods 1 June 2005 and 21 May 2006, a total of 207,555 SARs were submitted to the UK FIU from across the regulated sector.

Total number of SARs reported by sector and year

	2002	2003	2004	2005	2006	Total	% Total
Accountant	155	692	7,521	14,567	9,896	32,831	4.58%
Anonymous	15	43	266	303	145	772	0.11%
Asset mgt	200	241	353	1411	1,347	3,552	0.50%
Auction House	11	23	30	21	14	99	0.01%
Banks	37,871	67,094	96,799	127,918	142,140	471,822	65.85%
Barristers		172	82	67	33	354	0.05%
Bookmaker	30	24	17	26	48	145	0.02%
Building Society	3,788	5,393	6,770	11,758	10,841	38,550	5.38%
Bureaux de change	8,220	6,370	5,467	3346	3,045	26,448	3.69%
Capital Markets					12	12	0.00%
Charities	2	10	4	6	12	34	0.00%
Cheque Casher	98	581	360	474	2,134	3,647	0.51%
Company Formation Agents	8	5	19	88	335	455	0.06%
Consolidated Credit		1	1	1	5	8	0.00%
Credit Card	9	16	46	144	181	396	0.06%
Credit Union	32	32	64	122	149	399	0.06%
Education		3	5	5	4	17	0.00%
Electronic Payments	2	2	5		17,186	17,195	2.40%
Estate Agents	7	5	104	209	129	454	0.06%
FFIU (Jersey/Guernsey/IOM etc)	1	2	587		3	593	0.08%
Finance Companies	674	820	678	1,452	1,869	5,493	0.77%
Foreign entities		1		1	23	25	0.00%
Friendly Societies Commission	15	23	24	18	109	189	0.03%
FSA others					337	337	0.05%
Gaming	590	516	525	742	520	2,893	0.40%
Government		4	21	59	102	186	0.03%
High Value Dealers	277	275	143	107	42	844	0.12%
Independent Financial Advisors	117	221	267	320	227	1,152	0.16%
Insurance	1,077	1,202	1,276	1,727	1,452	6,734	0.94%
Invst Exchange			10	12	16	38	0.01%
IT/ Software companies		5	2	6	3	16	0.00%
Law enforcement agencies	4,236	1,183	3,845	35	154	9,453	1.32%
Legal other (non-barrister or solicitor)					2	2	0.00%
Leisure	3	3	19		179	204	0.03%
Licensed Conveyancers				3	20	23	0.00%
Local Authorities	5	2	22	54	76	159	0.02%
Manufacturing	6	1	10	7	8	32	0.00%
Money Transmission Service	1,232	6,754	4,431	9,140	6,732	28,289	3.95%

Mortgage Providers	589	1,147	1,436	2,848	2,588	8,608	1.20%
Motoring Organisations		11	6	238	140	395	0.06%
Markets & Exchanges (non-FSA)	33	33	40	76	35	217	0.03%
Other	33	71	567	6,940	1,953	9,564	1.33%
Other Legal	10	22	134	126	82	374	0.05%
Pension Provider		14	88	136	128	366	0.05%
Private Individuals	7	11	18	22	13	71	0.01%
Regulator	83	115	101	104	132	535	0.07%
Retail Intermediaries					86	86	0.01%
Security Firms	201	205	247	305	76	1,034	0.14%
Solicitors	605	3,718	9,576	10,525	7,296	31,720	4.43%
Specialist financial services		2	10	7	18	37	0.01%
Spread Betting			1		87	88	0.01%
Stockbrokers	8	32	25	109	176	350	0.05%
Tax Advisors					35	35	0.00%
Tied Financial Adviser	9	13	14	5		41	0.01%
Crown Dependency FIUs (Jersey/Guernsey/IOM)	3,783	2,818	1,540		725	8,866	1.24%
Unknown		2	62	112	102	278	0.04%
Total	64,042	99,933	143,638	195,702	213,202	716,517	100.00%

Terrorist Finance SARs Reported to UK FIU

Year	Terrorist Finance SARs Reported to UK FIU	SARs Disseminated to NTFIU
2002	4775	512
2003	2783	568
2004	2248	672
2005	2091	649

702. In general, the statistics show a wide range of reporting from the various regulated sectors. Statistics have also increased over time, indicating an ongoing, increased awareness of reporting obligations, and the ability to recognise and report suspicious activity.

3.7.2 Recommendations and Comments

703. The UK has a generally comprehensive system for reporting suspected money laundering and terrorist financing. Legal provisions are comprehensive and the system seems to be implemented effectively. However, the UK should continue to work with the private sector to make the consent process more efficient and effective.

3.7.3 Compliance with Recommendations 13, 14, 19 and 25 (criteria 25.2), and Special Recommendation IV

	Rating	Summary of factors underlying rating
R.13	**C**	
R.14	**C**	
R.19	**C**	
R.25	**C**	
SR.IV	**C**	

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

Internal AML/CFT controls

704. The MLRs 3 and 7 require financial institutions to implement appropriate internal controls in order to comply with their AML/CFT obligations. These measures have been in effect since the 1st April 1994 when the First EU Money Laundering Directive was implemented into UK law. MLRs Regulation 3(1) requires that:

> Every person must in the course of relevant business carried on by him in the United Kingdom…
> (b) establish such other procedures of internal control and communication as may be appropriate for the purposes of forestalling and preventing money laundering.

705. MLRs Regulation 3(1)(c) requires financial institutions to make their staff aware of the provisions under the Regulations, Part 7 of POCA, and sections 18-21A of the TACT and to provide training on how to recognise and deal with transactions which may be related to money laundering. Failure to take these steps leaves the firm open to prosecution for having inadequate training and awareness arrangements. Under POCA (sections 327-329 and 334(2)) and TACT (section 18 and 21A) individual members of staff face criminal penalties if they are involved in money laundering or terrorist financing or if they do not report their knowledge or suspicion of money laundering or terrorist financing where there are reasonable grounds for their knowing or suspecting such activity.

706. The FSA Handbook, SYSC 3.2.6 **R** requires that "A firm must take reasonable care to establish and maintain effective systems and controls for compliance with applicable requirements and standards under the regulatory system and for countering the risk that the firm might be used to further financial crime." The nature and extent of systems and controls will depend on a variety of factors, including:

- the nature, scale and complexity of the firm's business;
- the diversity of its operations, including geographical diversity;
- its customer, product and activity profile;
- its distribution channels;
- the volume and size of its transactions; and
- the degree of risk associated with each area of its operation.

707. JMLSG Guidance provides guidance on internal controls that financial institutions will require in order to meet their legal and regulatory obligations. In addition, it includes guidance on each of the requirements under the MLRs: customer identification, record keeping, reporting of suspicions, staff awareness and training.

708. The format of the HMRC MSB2 Guidance is constructed around the mnemonic CATCH, focusing on internal controls:

- **C**ontrol your business by having anti-money laundering systems in place (Section 4).
- **A**ppoint a nominated officer (Section 7).
- **T**rain your staff (Section 8).
- **C**onfirm the identity of your customers (Section 9).

- **H**old all records for at least 5 years (Section 10).

Compliance management arrangements

709. The MLRs require financial institutions to appoint a 'nominated officer' who is responsible for receiving internal money laundering disclosures and making external reports to SOCA where appropriate. MLRs Regulation 7(1)(a) states that "A [financial institution] must maintain internal reporting procedures which require that...a person in A's organisation is nominated to receive disclosures under this regulation ("the nominated officer")…"The 'nominated officer' is also responsible for receiving internal reports under POCA, section 331 (9) and the TACT, section 21A (7)(a)

710. Financial institutions are required to have arrangements in place for senior management accountability. SYSC 3.2.6H R requires that "A firm must allocate to a director or senior manager (who may also be the money laundering reporting officer) overall responsibility within the firm for the establishment and maintenance of effective anti-money laundering systems and controls." This emphasises senior management responsibility which flows from SYSC generally to ensure that senior individuals in the firm carry responsibility for ensuring that the FSA's requirements in relation to AML are met.

711. In addition, SYSC 3.2.6I R requires that a firm must "(1) appoint an individual as MLRO, with responsibility for oversight of its compliance with the FSA's rules on systems and controls against money laundering; and (2) ensure that its MLRO has a level of authority and independence within the firm and access to resources and information sufficient to enable him to carry out that responsibility." This means that he/she will have timely access to all relevant information such as customer identification data and other CDD information transaction records.

712. The FSA requires the MLRO to have a sufficient level of seniority within the financial institution to enable him to carry out his function effectively. To emphasise the importance and standing of the MLRO within the financial institution the role of the MLRO has been designated a "controlled function" under FSMA, Part V, section 59 by the FSA. This applies to UK, EEA, and non-EEA financial institutions: meaning that the FSA may only grant approval when it is satisfied that the candidate is "fit and proper". As a result, the MLRO must be individually approved by the FSA before performing the function. The MLRO's failure to discharge the responsibilities imposed on him by SYSC 3.2.6I R is conduct that is likely to be considered to be in breach of "Statement of Principle No. 7" for Approved Persons which states that: "An approved person performing a significant influence function must take reasonable steps to ensure that the business of the firm for which he is responsible in his controlled function complies with the relevant requirements and standards of the regulatory system." The MLRO is responsible for oversight of compliance with the FSA's rules on systems and controls against money laundering and is the "focal point" of all the firm's AML/CFT activity. In addition, a firm must allocate a director or senior manager (who may also be the money laundering reporting officer) overall responsibility within the firm for the establishment and maintenance of effective AML/CFT systems and controls

713. The legal obligation covers all financial sector firms; however, in the MLR Regulation 7 there is no obligation for the MLRO to be in charge of the whole AML/CFT regime within a company, only the necessity to have a person who is responsible for receiving all information necessary for reporting SARs is definitely required. There is no mention of CDD, training, and general internal controls.

714. HMRC Guidance, MSB2, paragraph 6.3 states "You (the nominated officer), must consider the report in the light of all the other relevant information…You will need to balance the requirement to make a timely disclosure with the need to obtain enough information to confirm your decision that the transaction is suspicious." In addition, MSB2 Guidance, paragraph 7.4 states: "…The nominated officer must have reasonable access to all the information that could help them when considering disclosures received from staff."

Independent audit function

715. FSA Handbook, SYSC 3.1.1 R requires that "A firm must take reasonable care to establish and maintain such systems and controls as are appropriate to its business." FSA Handbook, SYSC 3.2.16 G expands on how financial institutions may meet this obligation:

> Depending on the nature, scale and complexity of its business, it may be appropriate for a firm to delegate much of the task of monitoring the appropriateness and effectiveness of its systems and controls to an internal audit function. An internal audit function should have clear responsibilities and reporting lines to an audit committee or appropriate senior manager, be adequately resourced and staffed by competent individuals, be independent of the day-to-day activities of the firm and have appropriate access to a firm's records.

716. However, it should be noted that the FSA Handbook indicates this is guidance ("G") and not a requirement. Nevertheless, the FSA expects a firm to consider having an independent audit function, where that is an appropriate way of establishing and maintaining adequate systems and controls. However, the FSA believes that a firm and its senior management should have sufficient flexibility to determine whether having this function is appropriate, taking into account the nature, scale and complexity of that firm's business. Having the function, for example, to monitor the appropriateness and effectiveness of their controls may be disproportionate for some firms though they would still be expected to have effective internal control mechanisms for that monitoring. In practice, large and medium-sized firms will usually have an internal audit function. For smaller firms, which in many cases can mean a sole trader, it is not reasonable for them to assess the adequacy of their own controls and, therefore, they will usually get external auditors to provide an independent audit where appropriate.

717. In addition, the role of internal audit is a controlled function for which the individual holding the post will require approval from the FSA under its "approved persons" regime. Internal audit and compliance monitoring will typically be an essential aspect of financial institutions assessing the adequacy of their controls. The structure and resource of internal audit will reflect the size and complexity of the financial institution's business. However, since this is only encouraged through guidance ("G") in the FSA Handbook, there is not a direct requirement for firms to maintain an independent audit function.

718. There is no explicit requirement on MSBs to maintain an independent audit function given that they are small business with limited resources. While this might be generally adequate for the smaller MSBs, there is a concern that there is not a stronger internal audit requirement for the larger MSBs such as Western Union and MoneyGram, although some of these might have head offices subject to internal audit requirements in their countries of origin (for example, the US).

Training requirements

719. MLRs Regulation 3(1)(c) requires financial institutions to:

> take appropriate measures so that relevant employees are -
> (i) made aware of the provisions of these Regulations, Part 7 of the Proceeds of Crime Act 2002 (money laundering) and sections 18 and 21A of the Terrorism Act 2000; and
> (ii) given training in how to recognise and deal with transactions which may be related to money laundering.

720. For FSA regulated firms, this general rule is extensively expanded upon in the FSA Handbook, beginning with SYSC 3.2.6G (1) **G** which further states that "A firm should ensure that the systems and controls include…appropriate training for its employees in relation to money laundering…" The JMLSG Guidance, provides guidance on staff awareness, training and alertness. Further, ongoing

training should be given at appropriate intervals to all relevant employees. The JMLSG Guidance covers clearly all the training requirements, including all legal material and guidance and all elements of an AML/CFT regime, such as CDD, the role of the MLRO, and a firm's specific vulnerabilities and the internal policies and procedures in place.

721. Financial institutions will typically adopt a rolling programme to ensure that relevant staff receive training on a regular basis. The frequency and approach to staff training will be determined by the financial institution's risk-based approach.

722. HMRC Guidance, MSB2, Part 8, paragraph 8.1 states:

> All your managers and anyone who deals with money service business must be trained:
> - In the law regarding money laundering offences including MLR 2003, Part 7 of the Proceeds of Crime Act 2002 and sections 18 and 21A of the Terrorism Act 2000:
> - In policies and procedures relating to the prevention of money laundering:
> - In identification and "know your customer" procedures:
> - In recognition and handling of suspicious transactions which may be related to money laundering; and:
> - About record keeping.

723. In addition, MSB2, paragraph, 8.2 states that "You should give training to all new staff before they start MSB work and repeat the training regularly (at least every 2 years)." Further detail is included in MSB2 Guidance.

724. For FSA regulated firms, the requirement is covered well, for the HMRC regulated sector, it seems fairly complete; however, there might be a gap related to the other financial sector entities, as the MLR only mentions "training in how to recognise and deal with transactions which may be related to money laundering", which leaves out specifically CDD requirements. Further, financing of terrorism is not mentioned.

Screening procedures

725. Under the FSA Handbook, Threshold Condition 5: Suitability: financial institutions are required to operate adequate employee vetting procedures when recruiting certain new staff. COND 2.5.3 G states:

> (1) The emphasis of this threshold condition is on the suitability of the firm itself. The suitability of each person who performs a controlled function will be assessed by the FSA under the approved persons regime... In certain circumstances, however, the FSA may consider that the firm is not suitable because of doubts over the individual or collective suitability of persons connected with the *firm.*
> (2) When assessing this threshold condition in relation to a firm, the FSA may have regard to any person appearing to it to be, or likely to be, in a relevant relationship with the firm, as permitted by section 49 of the Act (Persons connected with an applicant)...

726. A further aspect of the satisfaction of Threshold Condition 5 in terms of the employment of individuals, is that those employees who will be undertaking "controlled functions" must be assessed as "fit and proper" by the FSA before they can undertake that controlled function. In making this assessment of fitness and propriety, FSA will have regard to the 'honesty, integrity and reputation; competence and capability; and financial soundness' of the person (Handbook, FIT 1.3.1 G). MLROs are required to undergo the "fit and proper" test. In addition, under SYSC 3.2.14 G, this includes that in "…assessing an individual's honesty and competence. This assessment should normally be made at the point of recruitment." The requirements under SYSC 3.2.14 G apply to all staff and not just controlled persons; however, it should be noted that this is guidance ("G") and not a requirement.

727. The assessment of an individual's suitability will take into account the level of responsibility that the individual will assume within the firm. The nature of the assessment will generally vary depending upon whether it takes place when the individual is recruited, at the end of the probationary period (if there is one) or subsequently. The effect of this is that all staff should be competent for their role and remain competent.

728. The majority of MSBs are small businesses with limited means. Given that they are cash based there is an obvious incentive for business owners to vet their staff as a simple commercial precaution, but there is no requirement for MSBs to put in place "fit and proper" screening procedures as this would impose an undue burden on them. According to the UK authorities, implementation of the Third Money Laundering Directive will introduce a fit and proper person test for senior management of MSBs.

729. While guidance regarding screening procedures is comprehensive for those operating "control functions" (e.g. managers, directors, MLROs), as well as other employees, there is no general requirement to have screening procedures for all employees.

Additional elements

730. The MLRO is able to act independently and to report to senior management directly. SYSC 3.2.6G (2) G states that a firm's governing body and senior management should receive appropriate information including a report at least annually by the MLRO on the operation and effectiveness of their AML systems and controls.

731. In addition, the JMLSG Guidance, Part I, Chapter 3, paragraph 3.11 states:

> The MLRO must have the authority to act independently in carrying out his responsibilities. The MLRO must be free to have direct access to the FSA and (where he is the nominated officer) appropriate law enforcement agencies, including [SOCA], in order that any suspicious activity may be reported to the right quarter as soon as is practicable. He must be free to liaise with [SOCA] on any question of whether to proceed with a transaction in the circumstances.

732. In practice, many MLROs do not consult with the management before making a report to SOCA, or have internal rules explicitly discouraging information on the details of a report to management; this is a positive feature which argues for a very high degree of factual independence.

Recommendation 22

733. There is no explicit requirement that foreign branches and subsidiaries observe AML/CFT measures consistent with home country requirements and the FATF Recommendations, to the extent that local (i.e. host country) laws and regulations permit. However, this is encouraged, on a risk-based approach, through guidance and in practice.

734. Generally, the FSA's SYSC provisions on money laundering apply with respect to activities carried on by an establishment maintained by authorised financial institutions in the UK. Therefore, the FSA's focus is on UK head office and its senior management who are responsible for ensuring that their foreign branches and subsidiaries are complying with Group AML/CFT standards. In considering whether to take regulatory action under SYSC 2 (Senior management arrangements) and SYSC 3 (Systems and controls) outside the United Kingdom, the FSA will take into account the standards expected in the market in which the firm is operating (SYSC 1.11.1(1) G).

735. The FSA requires financial institutions to take reasonable care to establish and maintain effective systems and controls for compliance with applicable requirements and standards under the regulatory system and for countering the risk that the firm might be used to further financial crime

(SYSC 3.2.6 R). This would also apply in a "prudential context" to a UK domestic financial institution or an overseas financial institution as regards activities wherever they are carried on (FSA Handbook, SYSC 1.1.9 R and SYSC 1.1.10 R). "Prudential context" broadly means the context in which the activities might be expected to have a negative effect on confidence in the financial system, the financial institution's fitness and propriety or the institution's solvency.

736. In most cases, Group standards are based on FATF Recommendations. The FSA expects senior management at the head office to resolve breaches at a local level with the relevant regulator where appropriate. It would also expect to be updated and notified of significant breaches or issues. Where the FSA is not satisfied with the financial institution's measures to mitigate the risk it will use its "close and continuous" supervisory model or if it is particularly significant through the supervisory risk mitigation programme (see section 3.10 below). FSA supervisors will also periodically talk to Group MLROs about AML issues/developments around the Group.

737. In addition, the JMLSG Guidance, Part I, Chapter 1, paragraphs 1.41-1.42 deal with group AML policies. Paragraph 1.41 states:

> The UK legal and regulatory regime is primarily concerned with preventing money laundering which is connected with the UK. Where a UK financial institution has overseas branches, subsidiaries or associates, where control can be exercised over business carried on outside the United Kingdom, or where elements of its UK business have been outsourced to offshore locations (see paragraphs 2.6-2.10), the firm should consider putting in place a group AML/CFT strategy. It is, however, for the firm to decide how to address AML/CFT outside the UK, taking into account the various obligations which it has to meet in these countries.

738. In addition, paragraph 1.42 states:

> A group policy may wish to ensure that all overseas branches and subsidiaries undertake identification and record-keeping procedures at least to the standards required under UK law or, if the standards in the host country are more rigorous, to those higher standards. Reporting processes must nevertheless follow local laws and procedures.

739. While this encourages the financial institutions to apply the higher standard, to the extent that the host country laws and regulations permit, this is not required. In practice, UK firms with large international activities have informed the team that they will take the foreign AML/CFT risk into account where the activities might be expected to have a negative effect on confidence in the financial institution's fitness and propriety or the institution's solvency, or where there is strong regulatory pressure from a supervisor, based on a solid requirement, either in their home or host jurisdiction.

740. There is no explicit requirement to pay particular attention that this principle is observed with respect to their branches and subsidiaries in countries which do not or insufficiently apply the FATF Recommendation. However, the principles above could help to ensure that financial institutions' foreign branches and subsidiaries are applying standards consistent with the FATF Recommendations.

741. There is not a requirement to inform the FSA if the foreign branch or subsidiary is unable to observe appropriate AML/CFT measures, although at least for those firms where FSA supervision is intense and active, this appears to be met in practice.

Additional elements

742. UK financial institutions are regulated in compliance with the Basel Core Principles, the IOSCO objectives and principles of securities regulation and IAIS supervisory principles.

3.8.2 Recommendations and Comments

743. Overall, the system of internal controls is generally strong and complete. The FSA's supervisory approach, in its strong core area related to AML/CFT, focuses on the internal controls and compliance arrangements financial institutions have in place to prevent money laundering and terrorist financing as part of wider systems and controls issues. FSA-regulated financial institutions will need to have effective compliance arrangements in place because the role of the MLRO will need approval from the FSA.

744. However, there should be a more direct requirement for firms to maintain an independent audit function. The UK should also address other minor legal issues (coverage of all MLRO duties under MLR 7), coverage of the full range of training requirements under MLR 3 (1)(c); particularly related to those financial sector entities who are only subject to the MLRs, without further rules or guidance. The UK should also consider a general requirement to screen all employees.

745. The UK should also adopt more specific rules relating to foreign branches and subsidiaries in relation to the requirements of Recommendation 22.

3.8.3 Compliance with Recommendations 15 & 22

	Rating	Summary of factors underlying rating
R.15	**LC**	• There is not a direct requirement for firms to maintain an independent audit function. • Some minor legal issues (coverage of all MLRO duties under MLR 7, coverage of the full range of training requirements under MLR 3 (1)(c)) are of concern; particularly related to those financial sector entities who are only subject to the MLRs, without further rules or guidance. • No requirement for screening procedures for all employees.
R.22	**NC**	• There are currently no requirements relating to foreign branches and subsidiaries.

3.9 Shell banks (R.18)

3.9.1 Description and Analysis

Recommendation 18

746. Shell banks are not permitted to establish or continue to operate in the UK. The FSA's authorisation process helps to ensure that shell banks do not operate in the UK. All applications to carry out FSMA-regulated activities must be submitted to the FSA for approval, and the FSA will only authorise financial institutions if it is satisfied that they meet and will continue to meet the "threshold conditions."

747. The guidance in the FSA Handbook, COND 2.2 identifies the head office of a firm as the location of its central management and control. Although the FSA will judge each application on a case-by-case basis, the key issue in identifying the head office of a firm is the location of its central management and control, that is, the location of the directors and other senior management, who make decisions relating to the financial institution's central direction, and the material management decisions of the institution on a day-to-day basis; and the central administrative functions of the financial institution (for example, central compliance, internal audit). COND 2.2.3 G states:

> Neither the Post BCCI Directive, the Insurance Mediation Directive nor the Act define what is meant by a firm's "head office". This is not necessarily the firm's place of incorporation or the place where its business is wholly or mainly carried on. Although the FSA will judge each

application on a case-by-case basis, the key issue in identifying the head office of a firm is the location of its central management and control, that is, the location of:

(1) the directors and other senior management, who make decisions relating to the firm's central direction, and the material management decisions of the firm on a day-to-day basis; and
(2) the central administrative functions of the firm (for example, central compliance, internal audit).

748. The guidance in COND 2.4 & 2.5 expands upon the requirement for the applicant to have adequate and suitable resources including personnel, premises and finances.

749. Once authorised FSMA, Part IV, section 45 also allows the FSA to exercise its power to vary or cancel a financial institution's permission if it appears that the authorised entity: (a) is failing, or is likely to fail, to satisfy the threshold conditions; (b) has failed, during a period of at least 12 months, to carry on a FSMA-regulated activity for which it has a Part IV permission; or (c) it is desirable to exercise that power in order to protect the interests of consumers or potential consumers. The FSA's power under this section is referred to in this as its "own-initiative power."

750. There is no enforceable obligation for financial institutions not to enter into, or continue, correspondent banking relationships with shell banks or to require them to satisfy themselves that respondent financial institutions in a foreign country do not permit their accounts to be used by shell banks. However, there is guidance in this area. The JMLSG Guidance, Part II, sector 16: Correspondent banking, paragraph 16.8 states that "Correspondents must not maintain relationships with shell banks" and that "Correspondent banks must not maintain relationships with shell banks nor any respondent which itself provides banking services to shell banks."

3.9.2 Recommendations and Comments

751. The UK does not approve or accept the creation or continued operation of shell banks. In this respect, it is fully compliant with FATF Recommendations. However, as pertains to correspondent banking relationships, there are no requirements prohibiting business with shell banks by UK counterparts. The JMLSG Guidance is useful, but it does not establish an enforceable obligation. More enforceable obligations combined with the JMLSG Guidance should be adopted to address this problem; UK authorities will include this in the revised MLRs when implementing the 3rd ML Directive.

3.9.3 Compliance with Recommendation 18

	Rating	Summary of factors underlying rating
R.18	PC	• There is no enforceable obligation for financial institutions not to enter into, or continue, correspondent banking relationships with shell banks. • No obligation to require financial institutions to satisfy themselves that respondent financial institutions in a foreign country do not permit their accounts to be used by shell banks.

Regulation, supervision, guidance, monitoring and sanctions

3.10 The supervisory and oversight system - competent authorities and SROs; Role, functions, duties and powers (including sanctions) (R.23, 29, 17 & 25)

General Background

752. The FSA is the UK's single financial services regulator. It is an independent non-governmental body, established as a company limited by guarantee. It has statutory powers conferred on it by the Financial Services and Markets Act (FSMA) 2000, and is funded through fees imposed on regulated financial institutions.

753. The FSA has four regulatory objectives which are: **market confidence, public awareness, the protection of consumers** and **the reduction of financial crime**. FSMA, Part I, section 6(3) defines financial crime to include fraud or dishonesty, market misconduct and money laundering. The FSMA definition is not meant to be an inclusive list and as such the FSA interprets its financial crime objective to include 'other financial crime' such as terrorist financing. The FSA's primary focus and activities are designed to ensure that the financial institutions it regulates have adequate systems and controls including in relation to preventing financial crime, which includes AML and CFT.

754. Financial institutions carrying out activities under FSMA are regulated by the FSA. However, financial institutions subject to FSA regulation will also undertake activities where specific permission or authorisation is not required. This will include financial activities such as credit cards or money service business. While the FSA's focus is on the regulated parts of the business, its approach to supervision ensures that the financial institution is looked at as a whole and this would include its FSA-authorised and non FSA-authorised activities. Consistent with the FSA's risk-based approach, the supervisory attention allocated to non-authorised activities will depend on how significant it is to the institution's overall business and the regulatory risks associated with that business.

3.10.1 Description and Analysis

Authorities/SROs roles and duties & Structure and resources - R.23, 30

Recommendation 23 (overall supervisory framework: Criteria 23.1, 23.2)

755. The FSA is the prudential and designated AML/CFT regulator for FATF-defined financial institutions that are authorised to carry out FSMA-regulated activities – this covers both their regulated and unregulated activities. FSMA, Part I, section 6 indicates that:

> (1) The reduction of financial crime objective is: reducing the extent to which it is possible for a business carried on-
> (a) by a regulated person, or
> (b) in contravention of the general prohibition,
> to be used for a purpose connected with financial crime.
>
> (2) In considering that objective the [FSA] must, in particular, have regard to the desirability of-
> (a) regulated persons being aware of the risk of their businesses being used in connection with the commission of financial crime;
> (b) regulated persons taking appropriate measures (in relation to their administration and employment practices, the conduct of transactions by them and otherwise) to prevent financial crime, facilitate its detection and monitor its incidence;

(c) regulated persons devoting adequate resources to the matters mentioned in paragraph (b).

756. HMRC is responsible for financial institutions undertaking the transfer of money or value and currency changing unless they are already authorised and regulated by the FSA for carrying out FSMA-regulated activities. (MLRs Part III). HMRC also has a program for monitoring MSBs (as well as HVDs) for AML compliance.

757. All types of financial institution as defined in the FATF methodology are subject to the Money Laundering Regulations 2003. The supervisory system is risk-based. It deploys a relatively intensive regime involving regular on-site assessments for the larger (high impact firms), and a less intensive approach for medium impact firms relying on less frequent on-site visits and targeted thematic work for smaller entities. In the view of the evaluation team, there was not adequate regulation for the smaller firms subject to FSA supervision and which fit into the FATF definition of "financial institution." In addition, there are activities that come under the FATF definition which are neither supervised nor obliged to comply with FSA rules and industry guidance (consumer credit, financial leasing, guarantees and commitments, brokers, factoring, safe-keeping and administration); for these activities there is lack of AML/CFT regulation and supervision. There are currently 110,000 active consumer credit licenses; and this cannot be considered as an insignificant AML/CFT risk. UK authorities plan to address this latter point when implementing the 3rd EU Money Laundering Directive. Finally, HMRC supervision of MSBs could be more comprehensive.

Recommendation 30 (Structure, funding, staffing, resources, standards and training)

FSA: *Structure, funding, staffing, resources*

758. The FSA as a whole seems adequately funded, staffed and has sufficient technical and other resources to fully and effectively perform its functions. The FSA is accountable to Treasury Ministers, and through them to Parliament. It is operationally independent of Government. The FSA's powers to authorise and take enforcement action against financial institutions is independent of any involvement or influence from the UK Government.

759. The Treasury appoints the FSA Board, which currently consists of a Chairman, a Chief Executive Officer, three Managing Directors, and 10 non-executive directors (including a lead non-executive member, the Deputy Chairman). This Board sets the overall policy, but day-to-day decisions and management of the staff are the responsibility of the FSA's Executive Committee.

760. The FSA does not receive any funding from the Government. To fund its work, it charges fees to all authorised financial institutions that carry out activities that it regulates, as well as other bodies such as recognised exchanges. The general powers to charge fees are set out in FSMA and associated legislation, which are reflected in FSA's Handbook. FSMA, Part VI, Schedule 1, Part I, paragraph 17.

761. The FSA's fees policy aims to recover the costs of its ongoing regulatory activities, and is therefore not intended to provide incentives to financial institutions to be well managed, or as a practical supervisory tool. In the year ended 31 March 2006, the FSA received £270.6m in fees, its funding requirement for 2006/07 is £281m.

762. A number of areas within the FSA are involved in AML/CTF issues including a number of specialist areas:

763. *Financial Crime Sector Leader/ Financial Crime Sector Team:* The FSA has created nine "Sector Leader" roles one of which is financial crime. The Financial Crime Sector Leader, supported by the Financial Crime Sector Team, is responsible for co-ordinating and supporting the work of the whole organisation to deliver the FSA's financial crime objective. The Sector Leader and Sector team are responsible for:

- risk identification and mitigation: helping the FSA become better at identifying financial crime risks early on and taking pre-emptive action to manage issues swiftly and decisively;
- representing the FSA on financial crime issues: building and maintaining strong relationships with external stakeholders to achieve common goals in the fight against financial crime; making public statements about FSA strategy and policies and how it is proposed to deliver them;
- overview of the coherence of the FSA's approach to financial crime issues: devising the financial crime strategy referred to, for the approval of the FSA's Executive Committee, and ensuring it is rolled out across the FSA so that the financial crime objectives and priorities are understood by the whole organisation and that they achieve them in the most efficient way possible; and
- staff development: developing the skills and knowledge of financial crime issues among FSA staff so that they can to do their job well and with confidence.

764. *Financial Crime Policy Unit (FCPU):* The FCPU leads the FSA's development of anti-money laundering and fraud policy within FSA financial crime strategy, working in partnership with other areas of the FSA, the Government, the industry and law enforcement agencies. Its activities include providing advice on AML compliance issues and guidance on the requirements of the SYSC provisions. The team has also led on policy issues such as the "defusing the ID issue" initiative, a discussion paper on "Reducing money laundering risk: know your customer", and AML monitoring issues as part of the "Current Customer Review (CCR)" project.

765. *Authorisation (financial institutions) and Individuals, CIS and Mutuals (individuals)*: These Departments are responsible for all corporate and individual applications. Applicants must satisfy the FSA that they can meet and continue to meet the FSA's criteria including any matters relating to financial crime. Both departments are responsible for reviewing applications and conducting any background checks that are necessary. If concerns are raised by any of these checks, or the review of the application, further enquiries will be made which could lead to the application being refused for failing to meet the FSA's criteria. In addition, both departments work closely with other areas within the FSA including the Intelligence Team and Enforcement Divisions as well as other regulatory agencies.

766. *Supervision:* The FSA's supervisory areas are responsible for the day to day relationship with the financial institutions regulated by the FSA. See description to section 3.10.1 below.

767. *Enforcement:* The Enforcement Division is responsible for investigating cases, including AML/CFT issues, where it is suspected that financial institutions have breached the FSA's rules or principles or the provisions of FSMA. FSMA also gives the FSA powers to take action under the insider dealing provisions of the Criminal Justice Act 1993 and the MLRs. The Enforcement division works with other regulatory bodies and law enforcement agencies to ensure that appropriate action is taken by the correct authority.

768. *Risk Review Department (RRD):* RRD's core function is to provide specialist assistance to supervisors. One team in RRD assists supervisors who have concerns about financial crime risk in their institutions. Typically, where a risk assessment has highlighted potential AML weaknesses, RRD experts are commissioned to undertake an assessment of the firm's AML controls and to recommend remedial action within a specified time frame. RRD also carries out thematic project work, assessing fraud and money laundering risk across a number of financial institutions and sectors. Recent examples include reviews of money laundering risk in UK hedge fund management and of automated AML transaction monitoring in retail banking.

769. *Intelligence:* The Intelligence Team's is responsible for the collection of intelligence from external partners in law enforcement, the wider intelligence community, other regulatory bodies and other sources (including internal ones), and making that intelligence available for use by the FSA in its regulatory activity as well as to law enforcement for criminal investigations. The Intelligence Team

supports the regulatory functions both tactically (case specific) and strategically (identifying areas of risk to FSA objectives). Tactically, it provides intelligence on applications for Authorisations (and other regulatory decisions); identifying financial institutions with weak controls for Supervision and specific cases that may require referral to Enforcement. On a strategic level, the Intelligence Team provides thematic products to FSA staff (such as international financial crime centres, or the financial crime risks in particular sectors). Support for external agencies includes the provision of the Shared Intelligence Service, intelligence sharing with law enforcement bodies on criminal investigations and the provision of financial crime knowledge/intelligence for external thematic products.

770. *Firm Contact Centre:* The Firm Contact Centre provides a direct point of contact for smaller, non-relationship managed financial institutions to help them to understand and comply with the FSA's regulatory requirements, including its money laundering rules. Telephone queries are handled by an appropriate advisor who may point to a relevant section of the FSA Handbook or website, where detailed information can be found to answer the query. If the query relates to a more complex issue, the FSA would normally aim to provide a substantive response to the firm.

771. At the end of May 2006 the FSA had over 2,800 full time equivalent staff members. This table is split into 4 sections:

- Number of supervisors within the FSA who will cover AML/CTF issues in the context of day to day supervision of their financial institutions (the actual number of supervisors has been separated from other staff in the main supervisory areas).
- Specialist financial crime areas who deal with financial crime, policy and intelligence issues on a full time basis.
- Other areas within the FSA who would deal with financial crime issues on a regular basis.
- Other areas of the FSA.

FSA Staff numbers (as of end May 2006)			
Supervisory Areas	**Supervisors**	**Senior Mgt.**	**Support**
Major Retail Groups	107.3	6	25.6
Retail Firms	145.6	5	24.6
Small Firms	157.1	5	16.6
Wholesale Firms	122.8	7	29.8
CRIM*	125.7	3	31.9
Markets	94.6	5	27.2
Total Supervisors	**753.1**		
Specialist Financial Crime Areas	**Total Staff**		
Financial Crime Policy Unit	10.0		
Financial Crime Sector Team	6.0		
Intelligence Team	29.0		
Other FSA Areas with FC focus			
General Counsel Division	82.5		
Enforcement	258.8		
Risk Review Department (RRD)	42.2		
Regulatory Transactions (including Authorisations & Individuals, CIS and Mutuals)	199.7		
Retail Themes	133.2		
Other FSA Areas			
CEO Office	7.0		
Chairman's Office	4.8		
Company Secretary	26.7		
Business Review & Audit	10.0		
Finance, Strategy & Risk	117.9		

People (HR)	76.8		
Communications	32.8		
Retail Policy	83.4		
Retail Management	38.4		
Basel Team	29.9		
Wholesale Policy	109.9		
Wholesale Services	57.6		
Sectors	42.8		
IS	261.6		
FSA Services	98.8		
Regulatory Management Services	43.6		
Other	91.6		
Total FSA Staff	**2834.8**		

*****Contact Revenue & Information Management – this represents the FSA's Firm Contact Centre (FCC).

772. The FSA appears to have enough staff and resources. The FSA is funded by the firms it regulates. It is possible that staff can leave to go to the private sector or elsewhere but all FSA staff are subject to a three month notice period (for senior staff it is six months) once they have resigned and staff are normally expected to work their notice period. The quality of the team dedicated to AML/CFT assessment (the RRD) can also be highlighted.

773. As of 1 January 2007, the reorganisation of the Financial Crime and Intelligence Division concentrates all Financial Crime resources into one area of the FSA (this includes the Financial Crime Sector Team, Financial Crime Policy Unit, Intelligence, and the financial crime specialist function in the Risk Review Department). It aims to strengthen effectiveness by establishing a centre of expertise and adding new operations teams to increase thematic and case work on financial crime issues, and prepare for the new supervisory responsibilities which the FSA will take on when the Third EU Money Laundering Directive is implemented into UK law. Work on the risk based approach will also be expanded. Additionally, the departments mentioned above will continue to cover financial crime issues in their work, as described above, including it in their processes of authorisation, supervision, enforcement etc. where appropriate.

Professional standards, confidentiality, integrity, and skills

774. FSA staff are generally required to maintain high professional standards, including standards concerning confidentiality, and be of high integrity and appropriately skilled. In relation to FSA staff, FSMA, Part XXIII, section 348 requires that confidential information not be improperly disclosed. "Confidential information" refers to information related to the business is applicable.

775. The FSA's Staff Handbook states that, except as required to enable staff to perform normal duties, they must observe absolute confidentiality concerning the affairs of the FSA. This includes all aspects of the FSA's business, its committees, tribunals, panels and working groups as well as the financial institutions and individuals which it regulates. Information must be kept confidential even if it is favourable, and not adverse, to the firm or individual concerned. Disclosing confidential information without permission may result in prosecution for a criminal offence. The duty to observe confidentiality is ongoing and does not cease after staff leave the FSA.

776. Also, where appropriate, Government security clearance is applied to key staff in the FSA, particularly those involved in AML/CFT matters. The main method used to promote and maintain high standards of conduct amongst staff is the FSA's Code of Conduct. This provides a framework for managing potential conflicts of interest and related matters. It also helps to protect staff, and the FSA, against any suggestion that regulatory decisions have been influenced by personal interests or that their investment decisions have been influenced by information made available in confidence to the FSA. The FSA Ethics Officer is responsible for dealing with matters arising from the Code and for

monitoring the information disclosed under its provisions. Compliance with the Code is mandatory through its incorporation into the Staff Handbook and consequentially all FSA employees' contracts of employment. Breach of the Code may result in disciplinary action including, where appropriate, dismissal.

777. The FSA uses a diverse range of selection tools to ensure that the recruitment process recruits individuals who are appropriately skilled for the specific role. Depending on the nature of the post, candidates may be asked to attend structured interviews or assessment centres, prepare case studies or make presentations. The FSA has developed a comprehensive learning and development programme to maintain and extend the knowledge, skills and capabilities required of all its staff. This includes training on regulation, financial services, markets and products, accountancy, information technology (IT), management and interpersonal skills. The FSA's performance management process, including the setting of individual staff objectives and the annual appraisal process, supports the learning and development programme and ensures that FSA staff members remain appropriately skilled.

Training

778. FSA staff are provided with adequate and relevant training to combat ML and TF. This includes:

779. *Computer-based foundation level training*: This is developed by the FSA and is compulsory for all FSA regulatory staff to complete. It is designed to give staff basic training on financial crime covering money laundering and fraud. The course provides staff with an understanding of what financial crime is, how it affects the activities of both the FSA and the financial institutions it regulates, and what controls they should expect to see in well-run financial institutions.

780. *Financial crime workshops:* The one-day workshops are designed to raise general awareness of how financial crime affects FSA-regulated financial institutions. The course is targeted at supervisors and it comes in five different versions to ensure relevance to them (banking; insurance; asset management; retail intermediaries; and capital markets). The aim of the workshop is to ensure that staff are able to establish the level of financial crime risk within a financial institution, assess whether the institution is managing its risk effectively, and propose appropriate mitigation where necessary. The workshops have been in place since February 2006. The table below illustrates the number of FSA supervisors who have attended each of these training courses.

Financial crime workshop	Supervisor attendance
Banking	90
Markets	31
Retail Intermediaries	173
Insurance	67
Asset Management	25
Total	**386**

781. *Financial crime presentations*: Presentations by key external stakeholders such as government departments, law enforcement, and industry practitioners are provided to FSA staff on a monthly basis.

782. *JMLSG Guidance*: The FSA has worked with the JMLSG to provide training on the revised JMLSG Guidance to FSA supervisors. The aim of this training was to explain to FSA supervisors the new thinking and risk-based approach in the revised Guidance, and what this means for the FSA supervisory approach. It also ensured that FSA staff are aware of current AML best practice in different sectors of the financial services industry.

783. *Intelligence training:* The Intelligence Team has undertaken a range of training including training in strategic and tactical techniques for both analysts and managers, to enable the Intelligence Team to provide a range of products and typologies on financial crime specifically, and serious and organised crime more generally (4 members of staff have attended this). Intelligence Team members have undertaken the course for tactical intelligence analysis which includes parts of the National Intelligence Model, handling and dissemination protocols, along with the basic network, crime pattern and comparative case analysis techniques (10 members of staff have attended this).

784. *Financial Investigation Course (accredited by ARA Centre of Excellence):* This course is aimed at those who are working in the financial investigation or financial intelligence arena. A nationally recognised course, POCA powers are similar to some of those contained in FSMA and thus the course complements aspects of FSA training (8 members of staff have attended this). Similar training for managers has also been undertaken.

HMRC: *Structure, funding, staffing, resources*

785. Under MLRs Regulation 14(2), HMRC "may charge …such fees as they consider will enable then to meet any expenses incurred by them in carrying out any of their functions under these Regulations or for any incidental purpose." An annual fee was introduced as part of the supervisory regime in 2002. The fee was £100 per outlet in the first year. In 2003 it was reduced to £60 per premises. It has remained at this level for the last four years. Receipts for 2005 / 06 were just over £2 million.

786. AML supervisory work within HMRC is performed by a number of linked units. These units handle both MSB supervision and "high value dealer" supervision, thus ensuring a centralisation of skills and knowledge. The units are as follows:

- *Registration and Fees Team:* The registration team is responsible for the collection of fees and penalties and maintenance of the register.
- *Money Laundering Regulation Targeting Team (a.k.a. "MLR"):* Registration information is passed to the MLR targeting team that monitors the risk of all MSB and HVD businesses across the country. This team works in conjunction with Intelligence colleagues with whom they are co-located. The targeting team generates visits for assurance officers specifying the risk to be addressed, monitors visit action and applies quality controls to completed visit reports adjusting as necessary the trader risk within the matrix. As indicated below this currently consists of 7 people; this should be increased so as to reach a wider range of MSBs.
- *Intelligence Team:* Intelligence feeds information into the risk matrix and extracts intelligence from assurance visit reports for onward transmission to Criminal Investigation. The team also accesses ELMER, the UK FIU's SAR database.
- *Assurance Officers:* Assurance officers complete visits to traders to monitor compliance with the regulations. (Annually there should be between 1,500 and 2,000 such visits).
- *MLR Policy Team:* MLR Policy prepares guidance for businesses and Assurance staff, liaises with other supervisors and supports Treasury in developing AML policy.

Staffing resources for MLR supervision 2005-2006 (includes staff working on HVD as well as MSB supervision).

Activity	Full Time Equivalent Staff
Registration & fees	4.5
MLR Targeting team	7
Assurance Officers	28.5
Intelligence	19.1
MLR Policy	6.5
Total	**65.6**

787. Seven agents of the MLR targeting team work with the intelligence team to prioritise assurance visits. The actual visits are then carried about by the 28.5 Assurance Officers and are focused on the largest traders which are considered as high risk. Overall, the allocation of resources is a concern, as current resources are focused on the MSBs with the largest turnover which does not adequately address the smaller MSBs which might be of higher risk for ML/FT.

Professional standards, confidentiality, integrity

788. HMRC staff are bound by the concept of "tax payer confidentiality" articulated in the Commissioners of Revenue and Customs Act (CRCA) 2005 (sections 18 and 19). Unlawful disclosure of confidential information renders an individual liable to criminal prosecution up to years and/or a fine.

Training

789. HMRC training is split between that for supervisors and that for investigation staff. Supervision staff undergo a mandatory two-stage training programme:

- Guided Learning Unit. This outlines the background to HMRC's supervisory role, explains the sectors for whom it is responsible and the ways they operate and gives an insight into its assurance techniques.

- Three day residential training course. This event is primarily concerned with the purpose, conduct and post visit activity concerned with AML compliance. It explains the law, officers powers, methods for checking AML compliance, application of sanctions, including penalties and references to Law Enforcement in cases of suspicion. Although aimed at Assurance staff it is also available to HMRC Intelligence and Law Enforcement. 60 people have completed the course since its inception in 2004.

790. Further guidance is also being prepared for officers visiting large businesses (those with 40+ branches) to develop systems based controls assessing large volumes of data effectively.

791. Within HMRC the enforcement of POCA provisions is performed by investigation and intelligence staff. Training for intelligence and investigation staff includes techniques to investigate and prosecute POCA offences, trace and restrain assets. HMRC is an approved training provider on behalf of the Asset Recovery Agency (ARA).

792. The Financial Investigation Training Programme delivered on behalf of the ARA contains a number of skills based courses including; Financial Investigation, Confiscation, Money Laundering; and Enhanced Financial Investigation Skills. These courses deliver the skill sets necessary for financial investigators to pro-actively identify, through financial trails, those involved in criminality; ascertain their patterns of activity, identification of their assets and how to build a successful prosecution.

793. The skill levels of an HMRC financial investigator will therefore be essential from basic financial intelligence enquiries to the investigation of serious and complex financial crime or money laundering. This will include the investigation of predicate offences in assigned matters relevant to HMRC Officers such as VAT offences, tax offences, excise fraud and stand alone money laundering offences under the Proceeds of Crime Act 2002 where the predicate offence cannot be identified.

Authorities Powers and Sanctions – R.29 & 17

Recommendation 29

Adequacy of powers, including on-site inspections, and access to information

FSA

794. The FSA has extensive powers to monitor and ensure compliance by the financial institutions it regulates with requirements to combat money laundering and terrorist financing as a result of its statutory objective on financial crime: FSMA, Part I, section 6: (e.g. the reduction of financial crime.) The FSA expects the financial institutions which it authorises and regulates to comply with their legal obligations under the MLRs, POCA, and TACT and FSA Handbook (the rules issued pursuant to the FSMA).

795. The FSA has the authority to conduct on-site inspections to ensure compliance. Such inspections can include the review of policies, procedures, books and records, and extends to sample testing. FSMA, Schedule 1, Part 1, section 6 states:

> (1) The [FSA] must maintain arrangements designed to enable it to determine whether persons on whom requirements are imposed by or under this Act are complying with them.
> (2) Those arrangements may provide for functions to be performed on behalf of the [FSA] by any body or person who, in its opinion, is competent to perform them.
> (3) The [FSA] must also maintain arrangements for enforcing the provisions of, or made under, this Act.
> (4) Sub-paragraph (2) does not affect the [FSA's] duty under sub-paragraph (1).

796. The FSA has comprehensive powers to require the production of information and documents from persons, including from persons outside of the regulated community. FSMA, Part XI, section 165 states, for example, that the FSA may, by notice in writing given to an authorised person, require him (a) to provide specified information or information of a specified description; or (b) to produce specified documents or documents of a specified description. An officer who has written authorisation from the FSA to do so may require an authorised person without delay (a) to provide the officer with specified information or information of a specified description; or (b) to produce to him specified documents or documents of a specified description. The FSA may require any information provided, whether in a document or otherwise, to be verified in such manner, or any document produced to be authenticated in such manner, as it may reasonably require. These powers may also be exercised to impose requirements on a person who is connected with an authorised person, an operator, trustee or depositary of a scheme recognised under section 270 or 272 who is not an authorised person; or a recognised investment exchange or recognised clearing house.

797. This provides the FSA with a wider range of powers including the power to compel, from any person, (i.e. not just regulated financial institutions or individuals) such information and documents as the investigator may require for the purposes of the investigation and also to attend before the investigator at a specified time and place to answer questions. In addition, investigators may be appointed under FSMA, Part XI, section 168(4) if it appears to the FSA that there are circumstances suggesting that a person may be guilty of an offence under the MLRs or that an authorised firm may have contravened a rule in the FSA's Handbook including the rules in the SYSC which relate to money laundering.

HMRC

798. HMRC's powers to monitor and ensure compliance by MSBs are underpinned by the MLRs. This includes the power to: enter premises and inspect and copy records. Under MLR Regulation 15, HMRC also has adequate powers to obtain access to all records, document or information relevant to

monitoring compliance. This power to obtain access is not predicted upon the need for a court order. MLRs Regulation 15 states:

> (1) Where an officer has reasonable cause to believe that any premises are used in connection with money service business or relevant business falling within regulation 2(2)(n), he may at any reasonable time enter and inspect the premises and inspect any recorded information or currency found on the premises.
>
> (2) An operator or high value dealer must -
> (a) furnish to an officer, within such time and in such form as the officer may reasonably require, such information relating to the business as the officer may reasonably specify; and
> (b) upon demand made by the officer, produce or cause to be produced for inspection by the officer at such place, and at such time, as the officer may reasonably require, any recorded information relating to the business.
>
> (3) An officer may take copies of, or make extracts from, any recorded information produced under paragraph (2).

799. If the HMRC wishes to compel actual production of documents, it may do so under MLRs Regulation 16 but a court order is required. MLR Regulation 16(1) authorises HMRC to obtain access orders from a judge for recorded information if the judge is satisfied that there are reasonable grounds for believing that an offence under the Regulations may be committed or that any recorded information may be required as evidence. Such an order will require the MSV or HVD to give an officer access, permit an officer to take copies of, or make extracts from, any information produced; or permit an officer to remove and take away any of it which he reasonably considers necessary; not later than the end of the period of 7 days beginning with the date of the order or the end of such longer period as the order may specify

800. HMRC assurance visits are geared to ensuring compliance with the regulations as interpreted in HMRC Guidance – MSB2. This is summarised in the acronym CATCH:

Control your business to prevent money laundering
Appoint a nominated officer
Train your staff
Confirm the identity of your customers
Hold records for five years

Overall adequacy of enforcement and sanction powers for supervisors

801. The FSA has a wide range of powers of enforcement powers and sanctions that it can apply to FSA-regulated firms and their senior managers and directors. The range of administrative sanctions is sufficiently broad and includes warning letters, the ability to restrict or revoke a license, and issue financial penalties. There are also some powers for HMRC in relation to MSBs, although these are not as broad. For example, sanctions cannot generally be applied to directors and senior managers. There is also a concern that certain financial activities, while subject to the MLRs, do not have any authority that can supervise or apply sanctions for AML/CFT compliance.

Recommendation 17

Criminal sanctions

802. There are a variety of criminal sanctions available in various pieces of AML/CFT legislation:

803. *Proceeds of Crime Act 2002:* In addition for the main money laundering offences, the maximum penalty for failing to disclose, for the nominated officer offences, and for the tipping off

and prejudicing an investigation offences, is five years imprisonment. In all cases, an unlimited fine can be imposed as well.

804. *Terrorism Act 2000 (TACT)***:** Under TACT, in addition to the penalties in sections 15 to 18 TACT (the terrorist financing offences), there criminal penalties for failure to notify suspicions of terrorist financing; on conviction on indictment, to imprisonment for a term not exceeding five years or to a fine or to both; on summary conviction, to imprisonment for a term not exceeding six months or to a fine not exceeding the statutory maximum or to both.

805. *Money Laundering Regulations 2003:* Under MLRs Regulation 3(2), a person who fails to adopt appropriate procedures and controls for customer identification, record keeping, internal reporting, other procedures of internal control and communication as may be appropriate for the purposes of forestalling and preventing money laundering and employee awareness and training is punishable by a criminal offence. Penalties include an unlimited fine, up to two years imprisonment, or both.

806. *FSA*: Under FSMA, Part XXVII, section 402 the FSA has power to prosecute breaches of the prescribed regulations relating to money laundering (i.e. the MLRs) under section 402(1)(b). The FSA has power to prosecute these offences in England, Wales and Northern Ireland, but not in Scotland. In Scotland, the Crown Office is responsible for prosecutions.

807. The FSA's general policy is to pursue through the criminal justice system all those cases where criminal prosecution is appropriate. When considering whether to prosecute a breach of the prescribed regulations in relation to money laundering the FSA will also have regard to whether the person concerned has complied with the JMLSG Guidance (ENF 15.4.1 G). However, to date the FSA has not used these prosecution powers. This is because the FSA has been able to pursue other avenues through which to secure compliance with the MLRs (through thematic and supervisory work, and where appropriate, regulatory sanctions). It should be noted that the FSA does not have the power to prosecute the substantive offences of money laundering under the Proceeds of Crime Act 2002. Were the FSA to become aware of such offences occurring, referrals would be made to other prosecutors, for example the Crown Prosecution Service or the Serious Fraud Office.

808. The commencement of criminal proceedings against an individual (particularly where that individual is an approved person) will raise concerns in relation to that individual's fitness and propriety to perform functions in relation to regulated activities. The FSA may therefore consider withdrawing approval at the commencement of proceedings and/or making a prohibition order against him if proceedings result in a criminal conviction.

809. When it decides whether to take any of the civil or regulatory actions where criminal proceedings are in contemplation, the FSA will have regard to the following factors:

(1) whether, in the FSA's opinion, the taking of civil or regulatory action might unfairly prejudice the prosecution, or proposed prosecution, of criminal offences;
(2) whether, in the FSA's opinion, the taking of civil or regulatory action might unfairly prejudice the defendants in the criminal proceedings in the conduct of their defence; and
(3) whether it is appropriate to take civil or regulatory action, having regard to the scope of the criminal proceedings and the powers available to the criminal courts.

810. When the FSA decides whether to bring criminal proceedings in England, Wales or Northern Ireland, or to refer the matter to another prosecuting authority in England, Wales or Northern Ireland, it will apply the basic principles set out in the Code for Crown Prosecutors (found at ENF 15 Annex 1). Under the Code for Crown Prosecutors, the FSA will in each case apply the Full Code Test i.e. whether:

(1) there is sufficient evidence to provide a realistic prospect of conviction against the defendant on each criminal charge ('the evidential test'); and
(2) having regard to the seriousness of the offence and all the circumstances, criminal prosecution is in the public interest ('the public interest test').

811. *FSA cautions:* The FSA has the power to issue cautions and in relevant cases may decide to issue a formal caution rather than to prosecute an offender. The circumstances of a case will dictate whether a caution is appropriate; however, in all cases the following criteria must be met:

(1) There is sufficient evidence of the offender's guilt to give a realistic prospect of conviction;
(2) The offender admits the offence; and
(3) The offender understands the significance of the caution and gives informed consent to being cautioned.

812. The issue of a caution may influence the FSA in its decision as to what action, if any, to take against an offender for any subsequent regulatory breaches (see FSA Handbook, Enforcement Sourcebook, section 15.6). To date this power has not been used in AML cases but has been used in other cases.

813. In addition to the FSA, the following authorities may prosecute offences under the MLRs in England or Wales and in Northern Ireland: (1) in England and Wales: the Secretary of State for Trade and Industry, the Director General of Fair Trading (in relation to offences involving the Consumer Credit Act), the Crown Prosecution Service and, in cases of serious or complex fraud, the Serious Fraud Office; (2) in Northern Ireland: the Secretary of State for Trade and Industry, the Director of Public Prosecutions in Northern Ireland, and in cases of serious or complex fraud, the Serious Fraud Office.

814. The FSA has no power to prosecute offences under the Act in Scotland where prosecution will remain the responsibility of the Crown Office.

815. The FSA has agreed guidelines that will establish a framework for liaison and cooperation in cases where one or more of these authorities has an interest in prosecuting any aspect of a matter that the FSA is considering for investigation, investigating or considering prosecuting. These Guidelines are set out in the FSA Handbook, Enforcement Sourcebook, Chapter 2, Annex 1 G.

816. The sanctions under the MLRs and POCA apply both to individuals as well as other legal entities. MLRs Regulation 27 states that any firm subject to the MLRs, or any officer in a body corporate who consents to or connives in the commission of offences under the MLRs, or where the commission of any such offence is attributable to neglect on his part, will be individually liable for the offence. The following criminal sanctions were applied for AML breaches:

2005 ML Offences	Proceeded	Found guilty	Sentenced	CD/ AD*	Fine	Com-munity	Sus-pended	Custody	Avge custody length (mnths)	d/w **
Proceeds of Crime Act 2002										
Failure to disclose - ss 330/334	4									
Failure to disclose - ss 331/334	1									
Tipping off – ss 333 and 334 (1)	1									
Prejudicing an investigation - s 342			1							
Failing to comply with disclosure/cust info order			1						**6**	

- s 359										
2004 ML Offences	**Proceeded**	**Found guilty**	**Sentenced**	**CD/ AD**	**Fine**	**Com-munity**	**Sus-pended**	**Custody**	**Avge custody length (mnths)**	**d/w**
Proceeds of Crime Act 2002										
Failure to disclose - ss 330/334	3	2	2					2	**3**	
Failure to disclose - ss 331/334	1									
Prejudicing an investigation - s 342	1	1	1			1				
Failing to comply with disclosure/cust info order - s 359	3	3	3							3
2003 ML Offences	**Proceeded**	**Found guilty**	**Sentenced**	**CD/ AD**	**Fine**	**Com-munity**	**Sus-pended**	**Custody**	**Avge custody length (mnths)**	**d/w**
Proceeds of Crime Act 2002: Failing to comply with disclosure/cust info order - s 359	2									
2002 ML Offences	**Proceeded**	**Found guilty**	**Sentenced**	**CD/ AD**	**Fine**	**Com-munity**	**Sus-pended**	**Custody**	**Avge custody length (mnths)**	**d/w**
S52 Drug Trafficking Act (DTA) 1994 - failure to disclose		1	1					1		
S53 DTA 1994 - tipping off	1	1	1		1					

**"CD/AD" = conditional discharge / absolute discharge*
***"d/w" = otherwise dealt with*

Administrative sanctions

Administrative sanctions available against FSA-regulated financial institutions

817. The FSA has a broad range of sanctions available to it against financial institutions and approved persons including unlimited financial penalties, public censure, prohibition, variation or cancellation of permission, injunction, issuance of a formal caution and prosecution for breaches of the MLRs. It also has enforcement powers that can be used against persons outside of the regulated community, such as the power to gather information and documents and the power to apply to court for injunctions.

818. *Risk Mitigation Programme (RMP):* The ARROW process is important in imposing requirements on firms to mitigate any deficiencies or risks identified, including compliance with the Joint Money Laundering Steering Group (JMLSG) Guidance. Following the ARROW firm risk assessment, the FSA will send the ARROW letter, addressed to the Board of directors, or equivalent body, along with the RMP. The ARROW letter[26] sets out the key findings from the FSA firm risk assessment setting out: key findings from the FSA work; the FSA's view of main risks and controls within the firm – this provides the context for the firm specific issues which have been identified; a high-level description of the risk assessment process; a summary of the FSA's rating of the firm against its risk model; key issues and points of the RMP; and the length of the regulatory period to the next risk assessment.

[26] The ARROW letter template is included in *The FSA's risk assessment framework* (August 2006), p35-42

819. The RMP sets out: the issues identified by the FSA, the intended outcome the FSA requires for each issue; the action required to achieve the intended outcome, specifying whether the action is to be taken by the FSA or the firm; and the timetable for action. The actions set out in the RMP should be implemented by those responsible for them i.e. the firm or the FSA. If the action has been completed and the intended outcome achieved, the FSA can close the issue. If the action has not been carried out or the action has not resulted in the intended outcome the FSA may consider setting a new action.

820. If a firm declines, fails or is unable to carry out the actions in the RMP, the FSA will consider the use of other regulatory tools e.g. a skilled person report under section 166 or a formal request for information under section 165 of FSMA, or in the most serious cases, the FSA may refer the case to its Enforcement Division for action. It may also be the case that an issue which is included in the RMP is also referred to Enforcement. This may take place if the issue particularly serious, an issue which is widespread or where the firm has a poor compliance history.

821. *Skilled persons report (s.166):* Under section 166 of FSMA, the FSA has the power to require any regulated firm to provide it with a report by an independent skilled person on any matter affecting its statutory objectives, including financial crime. A skilled person need not be an accountant or auditor and can be another specialist such as a lawyer or IT consultants. The use of this tool is considered when the FSA does not have the expertise and/or resources, e.g. the risk review team, to investigate the matter to the necessary standard, and the FSA cannot place reliance on the firm's own senior management, internal audit, or compliance function, to undertake an effective and independent review. The FSA will usually expect the firm to nominate a skilled person, but the FSA must always approve the appointment. This is considered to be a serious administrative sanction as the firm will be required to pay for the skilled person's report.

822. The decision to require a skilled person report will normally be prompted by a specific requirement to assess a risk or suggest mitigating or remedial action for the firm. It will usually be part of the firm's RMP, the result of an event or development relating to a firm, or prompted by a need for verification of information given to the FSA. Before deciding whether to use this tool the supervisor must consider the potential cost of the report and whether it is proportionate to the firm and the risk or potential risk. Therefore, a skilled person's report will be used where particularly serious issues have been identified within the firm given the potential cost of the report.[27]

823. *Varying a firm's permission:* Under FSMA, Part IV, section 45, the FSA can vary or cancel a financial institution's authorisation in certain circumstances including where the institution does not appear to be a "fit and proper" person because it has not conducted its business in compliance with high standards which may include putting itself at risk of being used for the purposes of financial crime or being otherwise involved in such crime. Under FSMA, Part IV, section 45(2) the FSA has the power to vary a financial institution's Part IV permission by removing an authorised activity, varying the description of an authorised activity or varying a requirement imposed on a firm's Part IV permission. Section 45 states:

> (1) The [FSA] may exercise its power under this section in relation to an authorised person if it appears to it that-
> (a) he is failing, or is likely to fail, to satisfy the threshold conditions;
> (b) he has failed, during a period of at least 12 months, to carry on a regulated activity for which he has a Part IV permission; or
> (c) it is desirable to exercise that power in order to protect the interests of consumers or potential consumers.

[27] *Supervision Manual*, Chapter 5.3 sets out the FSA policy on the use of skilled persons reports.

824. Further guidance on varying and cancelling a financial institution's Part IV permission is contained the FSA Handbook, Enforcement Sourcebook, Chapter 3. Where the FSA has cancelled a firm's authorisation under FSMA, Part IV, section 45 it is then required under FSMA, Part II, section 33 to go on to give a direction cancelling the firm's authorisation.

825. *Public censure:* Under FSMA, Part XIV, section 205 FSMA the FSA can issue a *public censure* against an authorised firm or an individual if it considers that they have breached a requirement imposed on them under FSMA: "If the [FSA] considers that an authorised person has contravened a requirement imposed on him by or under this Act, the [FSA] may publish a statement to that effect."

826. *Financial penalties:* Under FSMA, Part XIV, section 206, the FSA has the power to impose a financial penalty on a FSA-regulated financial institution if it considers that they have breached a requirement imposed on them by FSMA of such amount as it considers appropriate. A penalty under this section is payable to the FSA. Further guidance on financial penalties is provided in Chapter 13 of ENF.

827. *Injunctions:* Under FSMA, Part XXV, section 380 the FSA has power to apply to court for an injunction against persons whether authorised or not that have contravened a requirement under FSMA, which includes breaches of the MLRs. The FSA may apply to court for injunctions to restrain or prohibit the contravention, direct a person to remedy the contravention or to secure assets. Any person who disobeys an injunction may be in contempt of court and be liable to imprisonment, to a fine, and/ or to have his assets seized. Further guidance on injunctions is contained in the FSA Handbook, Enforcement Sourcebook, Chapter 6.

Administrative sanctions against individuals

828. The administrative sanctions available against approved individuals are the power to: impose unlimited financial penalties; to issue a public statement of misconduct; to prohibit an individual from performing controlled functions; and to withdraw an individual's approval.

829. Under FSMA, Part V, section 66, the FSA has the power to impose a financial penalty of such amount as it considers appropriate or issue a public statement of misconduct against an approved individual if it appears to the FSA that he is guilty of misconduct and the FSA is satisfied that it is appropriate in all the circumstances to take action against him. Section 66 requires:

> (1) The [FSA] may take action against a person under this section if-
> (a) it appears to the [FSA] that he is guilty of misconduct; and
> (b) the [FSA] is satisfied that it is appropriate in all the circumstances to take action against him.
>
> (2) A person is guilty of misconduct if, while an approved person-
> (a) he has failed to comply with a statement of principle issued under section 64; or
> (b) he has been knowingly concerned in a contravention by the relevant authorised person of a requirement imposed on that authorised person by or under this Act.
>
> (3) If the [FSA] is entitled to take action under this section against a person, it may-
> (a) impose a penalty on him of such amount as it considers appropriate; or
> (b) publish a statement of his misconduct.
>
> (4) The [FSA] may not take action under this section after the end of the period of two years beginning with the first day on which the [FSA] knew of the misconduct, unless proceedings in respect of it against the person concerned were begun before the end of that period…

830. An individual is guilty of misconduct if, while an approved person, he fails to comply with a statement of principle issued under FSMA, Part V, section 64 FSMA (see FSA Handbook, Statements of Principle and Code of Practice for Approved Persons Sourcebook) or has been knowingly concerned in a contravention by a relevant authorised firm of a requirement imposed on that authorised person by FSMA. Where a financial penalty is not appropriate the FSA may issue a public censure against an individual. Further guidance on financial penalties is provided in the FSA Handbook, Enforcement Sourcebook, Chapter 13.

831. Under FSMA, Part V, section 56 the FSA has the power to prohibit an individual from performing controlled functions (e.g. directors and senior management) in the UK if it appears to the FSA that an individual is not a "fit and proper" person to perform functions in relation to a FSMA defined activity. Any individual who performs or agrees to perform a controlled function in breach of a prohibition order is guilty of an offence and liable to a fine on summary conviction. Section 56 requires:

> (1) Subsection (2) applies if it appears to the [FSA] that an individual is not a fit and proper person to perform functions in relation to a regulated activity carried on by an authorised person.
> (2) The [FSA] may make an order ("a prohibition order") prohibiting the individual from performing a specified function, any function falling within a specified description or any function.
> (3) A prohibition order may relate to-
>
> (a) a specified regulated activity, any regulated activity falling within a specified description or all regulated activities;
>
> (b) authorised persons generally or any person within a specified class of authorised person.
>
> (4) An individual who performs or agrees to perform a function in breach of a prohibition order is guilty of an offence and liable on summary conviction to a fine not exceeding level 5 on the standard scale.
> (5) In proceedings for an offence under subsection (4) it is a defence for the accused to show that he took all reasonable precautions and exercised all due diligence to avoid committing the offence.
> (6) An authorised person must take reasonable care to ensure that no function of his, in relation to the carrying on of a regulated activity, is performed by a person who is prohibited from performing that function by a prohibition order.
> (7) The [FSA] may, on the application of the individual named in a prohibition order, vary or revoke it.
> (8) This section applies to the performance of functions in relation to a regulated activity carried on by-
>
> (a) a person who is an exempt person in relation to that activity, and
>
> (b) a person to whom, as a result of Part XX, the general prohibition does not apply in relation to that activity,
>
> as it applies to the performance of functions in relation to a regulated activity carried on by an authorised person.

832. Further guidance on prohibiting individuals is contained in the FSA Handbook, Enforcement Sourcebook, Chapter 8. In particular, the ENF 8.5 to ENF 8.6 set out how the FSA will decide whether approved persons and other individuals are fit and proper to perform functions in relation to regulated activities.

833. ENF 8.4.2 G indicates that the FSA will have the power to make a range of prohibition orders depending on the circumstances of each case and the range of regulated activities to which the individual's lack of fitness and propriety is relevant. Depending on the circumstances, the FSA may seek to prohibit individuals from carrying out any class of relevant function in relation to any class of regulated activity, or it may limit the prohibition order to specific functions in relation to specific

regulated activities. The FSA may also make an order prohibiting an individual from being employed by a particular firm, type of firm or any firm. The scope of a prohibition order will depend on the range of functions which the individual concerned carries out in relation to regulated activities, the reasons why he is not fit and proper and the severity of risk which he poses to consumers or the market generally.

834. ENF 8.4.3 G further indicates that "Depending on the circumstances of the case, it may be appropriate to prohibit the individual from performing only certain functions in relation to regulated activities carried on by certain firms. Alternatively, the FSA may consider it necessary to prevent the individual concerned from performing any functions in relation to any regulated activities carried on by any firm.

835. FSMA, Part V, section 69 requires that the FSA's policy in determining the amount of financial penalty in relation to an approved person should have regard to: the seriousness of the misconduct in question in relation to the nature of the principle or requirement concerned, the extent to which that misconduct was deliberate or reckless and whether the person on whom the penalty is imposed is an individual. The FSA Handbook, Enforcement Sourcebook, Chapter 13, 13.3.1 G (1) further states: that "The FSA will consider all the relevant circumstances of a case when it determines the level of financial penalty (if any) that is appropriate and in proportion to the contravention in question."

836. Under FSMA, Part V, section 63 the FSA has the power to withdraw the approval of an individual if it considers the person is not "fit and proper" to perform the function to which the approval relates. Section 63 requires:

> (1) The [FSA] may withdraw an approval given under section 59 if it considers that the person in respect of whom it was given is not a fit and proper person to perform the function to which the approval relates.
> (2) When considering whether to withdraw its approval, the [FSA] may take into account any matter which it could take into account if it were considering an application made under section 60 in respect of the performance of the function to which the approval relates.
> (3) If the [FSA] proposes to withdraw its approval, it must give each of the interested parties a warning notice.

837. These sanctions can be imposed against individuals that have failed to meet their requirements under FSMA including the requirements relating to money laundering.

838. Prior to a case being undertaken by the Enforcement Division it is considered in conjunction with the FSA objectives, current industry issues, areas of particular concern to FSA as well as the perceived severity of the breach. The FSA will normally consider the appropriateness of utilising supervisory tools to achieve its statutory objectives before a case is referred to enforcement.

839. Since 30 November 2001 the FSA's Enforcement Division has dealt with **one hundred and sixty seven** cases relating to a form of financial crime (including market abuse matters); of these cases, **eighteen have related specifically to anti-money laundering compliance**. Of these, three have resulted in a private warning, eight resulted in a fine, two resulted in a variation of the firm's permissions and one resulted in a prohibition (for a total of 14 enforcement actions). In one instance the FSA required the firm to undertake a skilled persons report under FSMA, Part XI, section 166. The remaining cases were either passed to Law Enforcement or the FSA's investigation did not find that the firm had breached relevant standards.

	Private warnings	Variation of permission	s.166	Public enforcement action	Other
AML compliance	3	2	1	8	5

840. The details of the public enforcements actions are set out below:

NAME AND DATE	PENALTY	DESCRIPTION OF CASE
December 2002 Royal Bank of Scotland	£750,000	• Breach of FSA client identification and record keeping rules. • Failure to either obtain sufficient documentation to establish customer identity or to retain such documentation in a number of new accounts across its retail network. • Failure to adequately monitor compliance with regulatory requirements.
August 2003 Northern Bank Limited	£1,250,000	• Breach of FSA client identification rules. • High rates of continuing non-compliance with FSA rules on client identification over a period of time. • Failure to recognise the seriousness of its breaches and therefore failed to implement prompt and effective remedial action or to inform the FSA.
December 2003 Abbey National companies: ▪ Abbey National Plc ▪ Abbey National Asset Managers Limited	 £2,000,000 £320,000	<u>Abbey National Plc</u> • Breach of FSA rules on systems and controls to prevent financial crime, client identification and internal reporting. • Failure of management information by the branch self-certification process to allow the central MLRO function to adequately assess Abbey National's applicable standards. • Substantial failures on customer client identification rules. • Serious failures in relation to submitting suspicious activity reports to NCIS (UK FIU pre-April 2006). Over half were submitted more than 30 days after internal reports had been submitted to the central MLRO function. <u>Abbey National Asset Managers Limited (ANAM)</u> • Breach of FSA rules on systems and controls appropriate for its business and to prevent financial crime. • Failure to address concerns raised on systems and controls in connection with the FSA's Risk Mitigation Programme (RMP). • Insufficient resources available to maintain adequate compliance oversight. • Insufficient management information to allow ANAM to identify, measure, manage and control risks of regulatory concern.
January 2004 Bank of Scotland (BoS)	£1,250,000	• Breach of FSA rules on record keeping and setting up arrangements to comply with the ML Sourcebook. • High levels of non-compliance with internal procedures on record keeping across its Retail, Corporate and Business Divisions. • As a result of these failures, BoS was unable to adequately monitor the effectiveness of its customer identification policies and procedures.
April 2004 Raiffeisen Zentralbank Osterreich	£150,000	• Breach of rules on client identification and failure to setup and operate arrangements to comply with the ML Sourcebook. • Failure of RZB senior management to sufficiently oversee compliance with the client identification requirements. • Failure of RZB to update its anti-money laundering procedures and Compliance Manual between 1999 and 2002.
August 2004 Bank of Ireland (BoI)	£375,000	• Breach of FSA rules on systems and controls to prevent financial crime. • BoI failed to take reasonable steps to detect the misuse of the bank drafts facility provided by a BoI branch. • Inadequate systems and controls to monitor the issuing of bank drafts at BoI branches. • Failure to take appropriate steps to ensure that staff understood the money laundering training provided to them, specifically to have sufficient understanding to recognize and report suspicious transactions.
November 2005	ISUK -	<u>ISUK</u>

Investment Services UK Limited & Mr. Ram Melwani	£175,000 Mr. Ram Melwani - £30,000	• Breach of FSA rules on setting up arrangements to comply with the ML Sourcebook, client identification, staff training, record keeping and systems and controls appropriate for its business and to prevent financial crime. • Breach of FSA rules for approved persons. • Failure to verify the identity of non-resident, high net worth clients. • ISUK provided introduction certificates which contained misleading statements about the extent of the due diligence it had undertaken and the amount of documentation it held in relation to its clients. • Failure to collect and record sufficient evidence of its clients' identity to comply with the ML Sourcebook (in respect of a small number of clients) and failure to have formal procedures to identify its clients or AML procedures. • Failure to provide staff with AML training for a period of time. <u>Mr. Ram Melwani</u> • Failed to act with due skill, care and diligence nor did he take reasonable steps to ensure that ISUK complied with applicable requirements and standards.
September 2006 Langtons (IFA) Limited	£63,000	A number of failings were identified within the firm. This included a breach of the FSA rule on systems and controls to prevent financial crime. • AML procedures were outdated and not customised for its business. • Money laundering reports on the effectiveness of its systems and controls were not presented to the Board of Directors. • Appropriate training was not carried out with staff.

841. As a prudential supervisor, the FSA emphasises its preventive approach, including written warnings and requiring firms to report regularly on measures taken to address a problem. In accordance with this approach; disciplinary powers are only used when the preventive action does not succeed. This approach may explain the relatively low level of disciplinary sanctions. However, having regard to the size of the UK's financial sector, the number of disciplinary sanctions (since 2001) seems nevertheless relatively low: 14 sanctions including warnings to the cancellation of a licence in one case.

HMRC

842. As indicated above, breaches of the MLRs that are criminal offences can be referred to Revenue & Customs Prosecution Office for a possible criminal prosecution. If it detects a "first time offence", and assesses that the breach is unintentional, HMRC issues a warning letter to the MSB in question before taking punitive action.

Number of warning letters issued by HMRC to MSBs	
Quarter date	No. of letters issued
Q1 30/06/2005	142
Q2 30/09/2005	163
Q3 31/12/2005	226
Q4 31/03/2006	220
Q1 30/06/2006	133

843. The warning letter also sets out what action should be taken by the business to resolve the compliance failure and warns the business that financial penalties may be issued for continued failure to comply. A return visit will be undertaken at a later date to ensure that the necessary steps have been taken.

844. MLRs Regulation 20 allows the HMRC to impose financial penalties up to £5,000, on a person to whom regulation 10 (requirement to be registered) applies, where that person fails to comply with any requirement in regulation 3 (systems and training etc. to prevent money laundering, which incorporates CDD, recordkeeping, and internal reporting procedures), 10, 11 (supplementary

information), 14 (fees) or 15 (entry, inspection etc.). This can be issued repeatedly if necessary – i.e. up to £5,000 for each day the breach continues; it can also be issued separately for separate and / or simultaneous breaches of the Regulations.

Number of MLR fines issued	
Quarter date	No. of letters issued
Q1 30/06/2005	0
Q2 30/09/2005	0
Q3 31/12/2005	3
Q4 31/03/2006	7
Q1 30/06/2006	5

845. The MLRs allow HMRC to cancel a MSB's registration in certain circumstances. Regulation 13 (cancellation of registration) states: that "The Commissioners may cancel the registration of an operator or high value dealer if, at any time after registration, it appears to them that they would have had grounds to refuse registration under paragraph (1) of regulation 12 (determination of application to register)." Registration penalties are levied upon businesses that fail to register or fail to declare all the premises through which they operate. Cancellation of a registration means the business will be removed from the MLR register. This could effectively put an MSB out of business for two reasons: (i) it can no longer legally continue to trade without registration (thus being liable for prosecution if it did); (ii) other financial institutions are aware of the registration numbering system employed by HMRC. If another financial institution was unable to verify the MSB's identity, CDD protocols suggest that the business or transaction should not be undertaken.

846. While this could be a useful tool, the power to cancel the registration only exists where there would have been grounds to refuse a registration in the first place—i.e., the registering information is not adequately supplied to HMRC, supplementary information concerning changes to this information is not supplied, or the adequate fees are not supplied. Currently the HMRC cannot cancel a registration for failure to comply with the MLRs.

Number of Registration penalties issued	
Quarter date	No. of penalties issued
Q1 30/06/2005	8
Q2 30/09/2005	8
Q3 31/12/2005	6
Q4 31/03/2006	10
Q1 30/06/2006	2

847. The administrative sanctions of HMRC do not extend to directors and senior managers. It is not possible to bar individuals from employment within that sector, replacing or restricting the powers of managers, directors, or controlling owners.

Unregulated activity

848. With regard to activity that does not need to be authorized under FSMA and carried on by FSA-regulated financial institutions, the FSA has the power to take action against those financial institutions in a "prudential context" (cf FSA Handbook, SYSC 1.1.5R). "Prudential context" broadly means the context in which the activities might be expected to have a negative effect on confidence in the financial system, the financial institution's fitness and propriety or the institution's solvency.

Market entry – Recommendation 23

(Criteria 23.3, 23.5, 23.7)

Authorisations under Part IV Financial Services and Markets Act 2000 for financial institutions

849. Under FSMA, Part I, section 19, any person who carries on a FSMA-regulated activity in the UK must be authorised by the FSA or exempt (an appointed representative or by some other exemption). Breach of section 19 may be a criminal offence and punishable on indictment by a maximum term of two years imprisonment and/or a fine. Financial institutions will need to establish whether their proposed business requires them to apply for FSA authorisation to carry on FSMA-regulated activities.

850. When a firm seeks authorisation from the FSA, it does so in terms of two principle components: FSMA-regulated activities and specified investments. Financial institutions will apply for a Part IV permission to carry on relevant FSMA-regulated activities in relation to specified investments which are applicable to that activity. In addition, further limitations may be applied on these activities (e.g. the customers they deal with) and/or requirements on the whole permission (e.g. not to hold client money).

851. FSMA regulated activities are defined in Part II of the Regulated Activities Order and comprise, for example, accepting deposits, issuing e-money, effecting or carrying out contracts of insurance as principal, dealing and advising in investments. The specified investments are defined in Part III of the Regulated Activities Order and include: deposits, electronic money, rights under a contract of insurance, shares etc., instruments creating or acknowledging indebtedness, government and public securities, units in a collective investment scheme, and options and futures.

852. The FSA has a series of application forms designed to assess applications according to their business type. All applicants have to confirm that they have procedures in place to prevent them being used to further financial crime including money laundering. A compliance monitoring program must also be submitted by all financial institutions covered by this review indicating how often AML/CFT procedures will be checked to make sure they are up to date. All applicants are required to describe the procedures to be put in place to counter the risk that the business might be used to further financial crime. Their responses are required to identify if the procedures are adequate for the type of FSMA-regulated activities applied for.

853. Corporate applicants must satisfy the FSA before they can carry on a FSMA-regulated activity that they can meet and continue to meet the minimum standards, called “threshold conditions” and that the persons running the financial institution meet the FSA’s criteria.

854. The FSA Threshold Conditions are as follows:

- **Threshold condition 1: Legal status (COND 2.1):** Financial institutions can be any of the following: a sole trader, a body corporate, a partnership, an unincorporated association. A firm effecting or carrying out contracts of insurance, must be a body corporate (other than a limited liability partnership), a registered friendly society or a member of Lloyd's. A firm accepting deposits must be a body corporate or a partnership.
- **Threshold condition 2: Location of offices (COND 2.2):** If the applicant is a body corporate constituted under the law of any part of the UK: unless it carries on *only* insurance mediation activities, its head office and its registered office, if there is one, must be located in the UK; or if the applicant is not a body corporate but has its head office in the UK, it must also carry on its business in the UK.
- **Threshold condition 3: Close Links (COND 2.3):** If the applicant has any close links (links with other financial institutions or individuals), these must not prevent effective FSA supervision of the applicant if the applicant is authorised.

- **Threshold condition 4: Adequate resources (COND 2.4):** The FSA must be satisfied that the applicant has adequate resources. The FSA assesses the quality and quantity of the applicant's resources with regard to: finance, management, staff; and systems and controls.
- **Threshold condition 5: Suitability (COND 2.5):** The FSA must be satisfied that the applicant is "fit and proper" to be authorised. Therefore, the applicant must satisfy the FSA that it meets the threshold conditions including that it is "fit and proper" to conduct the business being applied for. If the financial institution fails to satisfy the FSA of its fitness and propriety (including any matters relating to money laundering or terrorist financing) the FSA will refuse authorisation. In certain circumstances the FSA may consider that a financial institution is not suitable because of doubts about an individual or collective suitability of persons associated with the institution.

855. The FSA applies greater scrutiny to applications identified as higher risk. Cases are assessed as higher risk depending on certain criteria/triggers. Referral triggers for corporate application are:

- Impact rating/business type – e.g. banks or insurance companies.
- Adverse vetting on controllers/individuals
- Financial crime
- Non disclosure - where a financial institution has not disclosed to the FSA information specifically requested on the application form
- Inadequate resources financial/non financial
- Training & competence – doubts on competence of individuals
- Innovation - where a financial institution is proposing a business model which is unusual or has not been seen before
- Complex systems
- Close links/structure
- Mind & management (outside UK)
- Phoenix firm- where the assets of one limited company are moved to another legal entity, sometimes at price below its true market value, and without moving the liabilities
- Hedge fund operators; depending on size
- Conflicts of interest
- Non responders – the applicant is not responding to follow up correspondence on the application

856. The table below shows the number of financial institutions applications received by the FSA and their outcome. These figures cover all types of financial institutions authorised the FSA and not just those captured by the FATF definition.

Firms	1/12/01 to 31/3/02	1/4/02 to 31/3/03	1/4/03 to 31/3/04	1/4/04 to 31/3/05	1/4/05 to 31/3/06	Total
Applications received	95	733	4,607	12,849	1,983	20,267
Authorised	107	646	900	15,378	1,765	18,796
Withdrawn	19	84	86	566	176	931
Refused	0	1	3	47	24	75

857. The FSA maintains statistics on the applications received and authorised in each period. However, at any point in time, there are a number of applications being assessed which represent work in progress and therefore it is possible that a particular period more applications may be authorised than applications received in that period. The significant increase in numbers in the period 2003 to 2005 is because of the extension of the FSA's scope to include the regulation of mortgage and general insurance. These applications were predominantly determined in advance of the introduction of mortgage regulation in October 2004 and general insurance regulation in January 2005.

858. Applicants may withdraw their application at any time before a decision notice is issued. In some cases applicants will withdraw their application once the FSA has advised them of its intention to refuse the application. Final notices are published on the FSA website (http://www.fsa.gov.uk/Pages/Library/Communication/Notices/Refusals/index.shtml).

859. FSMA, Part IV, section 41(2) provides that, in giving or varying permission to carry out FSMA-regulated activities, the FSA must be satisfied that the applicant will satisfy, on an ongoing basis, five Threshold Conditions ("TC"). TC5 (Suitability) requires the applicant firm to satisfy the FSA that it is "fit and proper" to have FSMA Part IV permission, having regard to all the circumstances. TC5 sets out the requirements that financial institutions will need to meet. This tool helps to ensure that criminals or their associates do not gain beneficial ownership. These circumstances include its connections with other persons, the range and nature of its proposed regulatory activities and the overall need to be satisfied that its affairs will be conducted soundly and prudently. The FSA Handbook (COND, 2.5.6G) sets out matters to be taken into account in determining whether a firm will meet TC5 in respect of conducting its business with integrity and in compliance with proper standards.

860. FSMA, Part XII requires individuals or corporate bodies who wish to take, or increase, control in an authorised financial institution to seek prior approval from the FSA. A change in control also occurs when an existing controller decreases control. SUP 11 in the FSA Handbook gives full details of the thresholds and requirements. FSMA, Part XII sets out provisions about control over authorised persons. Acquiring, increasing and reducing control need to be notified to the FSA when the percentage of control moves across a series of thresholds. The FSA has a period of three months to decide whether or not to approve a change of control.

861. Under the FSA Handbook, SUP 16.4.5 R, a financial institution must submit a report on its controllers and close links to the FSA once a year, even if there has been no change. They should submit this report within four months of the financial institution's accounting reference date. Changes in control may not happen until they have been approved by the FSA.

862. The FSA received 1,163 change of control notifications between April 2005 and April 2006. In the same period 1,264 were completed. Of these, 85 were withdrawn by the applicants and 3 refused. Withdrawal of an application is allowed at any stage before determination.

863. FSMA, Part IV, sections 44-46 refer to the variation and cancellation of Part IV Permission at the request of financial institutions or on the FSA's own initiative. This will mean a re-assessment of how the firm meets the Threshold Conditions and the requirements for approved persons.

HMRC

864. Under MLRs Regulation 10(2)(b)(vii) applicants for MSB registration must provide information including: "whether any person concerned (or proposed to be concerned) in the management, control or operation of the business has been convicted of money laundering or an offence under these Regulations." Applications are also subject to checks by officers against other criminal and intelligence databases. A "hit" on these other systems would impact on and be reflected in the risk matrix and focus increased assurance attention towards the business concerned.

865. Exclusion from the register is possible under certain conditions, for example, if it appears to them that any information furnished pursuant to regulation 10 or 11 is false or misleading in a material particular (Regulation 12). HMRC may also cancel a registration under similar circumstances (Regulation 13).

866. The scope for exclusion will increase under the "fit and proper" test being introduced in December 2007 as a result of the implementation of the Third EU Money Laundering Directive.

Fit and proper tests

867. With regard to institutions subject to the Core Principles, the FSA applies adequate measures to verify the integrity of the owners of financial institutions and all directors and senior managers are subject to a fit and proper test. The test includes an assessment relating to expertise and integrity and applies to anyone holding a "controlled function," which includes ((FSA Handbook, SUP 10.4.5 R) the positions of :

- Significant Influence Functions: Director, Non-executive director, Chief executive, partner, directors of unincorporated association, sole trader, apportionment and oversight, EEA Investment business, compliance, money laundering reporting officer, appointed actuary, finance, risk assessment, internal audit, significant management (5 categories available)); or
- Customer functions: Investment adviser, investment adviser –trainee, corporate finance, pension transfer specialist, adviser on syndicate participation at Lloyds, customer trading, investment management

868. Individuals are assessed against FSMA, Part V, sections 59 to 61 and the "fit and proper" criteria in the handbook (FIT). In respect of the senior management of a regulated entity there is a benchmark used to assess the individual's suitability within a financial institution to perform the controlled functions which they have applied to perform. Financial institutions will have to satisfy the FSA that individuals proposed for controlled functions can meet, and maintain, the criteria for approval (FSA Handbook, *The Fit and Proper test for Approved Persons (FIT).* The most important considerations are the individual's:

- Honesty, integrity and reputation (FSA Handbook, FIT 2.1)
- Competence and capability (FSA Handbook, FIT 2.2)
- Financial soundness (FSA Handbook, FIT 2.3)

869. The FSA consults the Shared Intelligence Service database for each individual who applies for approval. Further checks on their credit worthiness are made with commercial information providers and additional checks are carried out externally with other regulatory bodies. Once the FSA has approved the individual, he/she becomes an "approved person." The individual will then need to perform their controlled function in accordance with a set of standards issued under FSMA, Part V, section 64 (FSA Handbook, Statements of Principle and Code of Practice for Approved Persons (APER)). An approved person must: act with integrity in carrying out his controlled function; must act with due skill, care and diligence in carrying out his controlled function; observe proper standards of market conduct in carrying out his controlled function; deal with the FSA and with other regulators in an open and cooperative way and must disclose appropriately any information of which the FSA would reasonably expect notice. An approved person performing a significant influence function must: take reasonable steps to ensure that the business of the firm for which he is responsible in his controlled function is organised so that it can be controlled effectively; exercise due skill, care and diligence in managing the business of the firm for which he is responsible in his controlled function; and take reasonable steps to ensure that the business of the firm for which he is responsible in his controlled function complies with the relevant requirements and standards of the regulatory system.

870. The FSA applies greater scrutiny to applications identified as higher risk. Cases are assessed as higher risk depending on certain criteria/triggers. Referral triggers for individuals are: non-disclosure, a criminal record; a previous disciplinary history, financial issues, business issues, competence and capability, and a previous withdrawal of application. The table below shows the number of individual applications received by the FSA and their outcome. These figures cover all individuals' applications from all types of financial institutions.

Individuals	1/12/01 to 31/3/02	1/4/02 to 31/3/03	1/4/03 to 31/3/04	1/4/04 to 31/3/05	1/4/05 to 31/3/06	Total
Applications received	14,279	53,788	47,928	80,431	53,568	249,994
Authorised	13,934	52,570	48,109	76,745	52,474	243,832
Withdrawn	44	287	555	3,163	1,392	5,441
Refused	0	5	18	19	3	45

871. The FSA maintains statistics of application received and authorised in each period. However, at any point in time, there are a number of applications being assessed which represent work in progress and therefore it is possible that in a particular period more applications may be authorised than applications received in that period.

872. The significant increase in numbers in the period 2003 to 2005 is because of the extension of the FSA's scope to include the regulation of mortgage and general insurance. These applications were predominantly determined in advance of the introduction of mortgage regulation in October 2004 and general insurance regulation in January 2005.

873. These figures show all applications to the FSA. These include applications for customer functions. The FSA applies the 'fit & proper' criteria to all applicants having regard for the role they will carry out.

874. Individual figures for each type of function are not readily available; however 17,781 "Significant influence function" applications were approved between 01/04/2005 and 31/03/2006. Therefore, significant influence functions represented just over 33% of the total applications for that year. The figures also include individuals who applied as "Appointed Representatives" and are therefore exempt. Applications for approved persons who are refused are published on the FSA website at http://www.fsa.gov.uk/Pages/Library/Communication/Notices/Persons/index.shtml).

875. The EU 3rd Money Laundering Directive to be implemented through UK legislation by December 2007 will establish a "fit and proper" test for directors and senior management of MSBs (as well as TCSPs). The form and content of this "fit and proper" test will be developed in partnership between the FSA, HMRC, Treasury, and others, including SOCA, to ensure that it is as effective as possible at focusing on AML/CFT risks.

Money value transfer and money exchange

876. Where a financial institution is already authorised and regulated by the FSA under FSMA and is carrying out money service business (MSB), the FSA – rather than HMRC - is responsible for the AML regulation of the MSB activity. Many banks, for example, will provide remittance services. Under MLRs Regulation 25 and FSA Handbook, SUP 15.8.4 G financial institutions are required to notify the FSA of any bureau de change business. The number of FSA regulated financial institutions undertaking bureau de change business is:

Firm sector type	Number of firms
Wholesale	40
Retail	11

877. All businesses wishing to operate as MSB's must first register with HMRC. There is scope in the regulations for HMRC to refuse registration under specific conditions. MLRs Regulation 10 (Requirement to be registered) requires that a person who acts as an operator or as a high value dealer must first be registered by the Commissioners. An applicant for registration must – apply and supply the following information: (i) his name and (if different) the name of the business; (ii) his VAT

registration number or, if he is not registered for VAT, any other reference number issued to him by the Commissioners; (iii) the nature of the business; (iv) the address of each of the premises at which he proposes to carry on the business; (v) any agency or franchise agreement relating to the business, and the names and addresses of all relevant principals, agents, franchisors or franchisees; (vi) the name of the nominated officer (if any); and (vii) whether any person concerned (or proposed to be concerned) in the management, control or operation of the business has been convicted of money laundering or an offence under these Regulations. Applicants must supply further information within 21 days if requested.

878. MLRs Regulation 11 (Supplementary information) requires that, if there are any changes to this registration information, or if it is clear that the information was not current, the applicant/MSB must supply the updated information within 30 days.

879. HMRC may refuse an application, or later cancel one, for certain reasons: if the proper information is not supplied/re-supplied, or if it appears that information is false or misleading in a material particular. HMRC must notify the applicant within 45 days whether or not the application has been accepted, and if not, the reasons for refusal. In general, there does not appear to be sufficient authority to refuse an MSB registration.

880. Under MLRs Regulation 2(6) also stipulates that "Where the person who obtains the evidence mentioned in paragraph (5) knows or has reasonable grounds for believing that the applicant for business is a money service operator, satisfactory evidence of identity must also include the applicant's registered number (if any)."

881. Businesses are able to confirm the registration numbers of MSBs via a phone call to HMRC. This is an effective deterrent against unregistered MSB's as it limits their access to other financial institutions. Furthermore it is in the commercial interest of legitimate MSB's to confirm the registration details of local competition. HMRC assurance officers are also encouraged to look out for MSB premises and confirm registration in the general course of their duties. Any notifications of unregistered MSB activity are followed up by the MLR Target team by means of the issue of a registration pack. In the absence of any response to the pack the address will be visited by an Assurance officer to establish whether any MSB activity is taking place.

Other financial institutions

882. All financial institutions seeking to carry out FSMA-regulated activities are licensed on the same basis and against the same criteria must acquire authorisation from the FSA. There are however also activities that come under the FATF definition that are not regulated by either the FSA or HMRC. These include lending and leasing, some guarantees and commitments and safe keeping services. The largest make up of this non-FSA authorised sector is lending and consumer credit. There are over 100,000 active consumer credit licences. Under the Consumer Credit Act 1974, recently updated by the Consumer Credit Act 2006, consumer credit firms need a licence from statutory regulator the Office of Fair Trading (OFT) before they can set up. However, they are not yet adequately regulated/supervised for AML/CFT.

883. A large proportion of financial leasing is undertaken through banks, thus bringing it within the FSA's regulatory remit. However, the activity itself is not regulated, although 95% of non-bank firms are within the main representative trade association which is active in AML forums. There are also guarantees and commitments, estimated as a very small number; brokers, estimated as a very small number; factoring: and safe-keeping and administration: unknown, estimated as a small number. Entities that perform these functions outside of the FSMA-regulated entities do not need to be licensed and are not monitored/supervised for AML/CFT compliance.

Ongoing supervision and monitoring – R.23

(Criteria 23.4, 23.6, 23.7)

Determining the level of supervision

884. The FSA's primary focus and activities are designed to ensure that the financial institutions it regulates have adequate systems and controls including in relation to AML and CFT. The FSA has also taken a policy decision that senior management responsibility should be a fundamental part of its approach to regulation. Senior management of financial institutions are explicitly required to ensure that their financial institutions comply with relevant regulatory requirements and have in place the systems and controls necessary to satisfy themselves (and the FSA) that they are compliant. In the FSA's approach to supervision it would normally spend a considerable part of its resources assessing the capabilities of the management team and the adequacy of the systems and controls, including AML/CFT systems and controls, as a way of ensuring that they meet all the relevant requirements. That accountability includes their efforts to reduce the extent to which their firms may be used by criminals for money laundering purposes. To support this focus on senior management, at its inception the FSA established an Approved Persons Regime. (See section on "Market Entry" beginning at paragraph 849 above.)

885. On-going supervision of financial institutions is determined by a risk-based approach. The FSA relies on an internal process to measures risk and determine response against an agreed set of criteria and benchmarks. This internal process is called "Advanced Risk Responsive Operating frameWork" (ARROW). The ARROW process determines nature of the work the FSA will undertake to mitigate the risk, and where relevant the work programme with a financial institution. The FSA measures the risk (the impact and probability) before deciding on the nature of its supervisory relationship or the action (if any) that needs to be taken and by whom to mitigate the risk. The FSA has a range of tools (reports by the FIU, thematic works) that helps it identify those risks, such as Policy or Firm supervision. They are measured using the common ARROW firms' framework and the FSA Risk Dashboard (a table for the analysis of the impact of all risks using a set of qualitative measures of impact to further target FSA resources on key risk areas). This dual framework facilitates operating units within the FSA to prioritise their risks and manage their portfolio. At their disposal they have a variety of tools they can use to monitor and control risks. So a risk identified in a thematic review may be monitored through a sector process and controlled in firm supervision.

886. The ratings for both impact and probability are on a simple four-point scale. The probability scale is as follows:

- low: the likelihood of the event occurring is remote;
- medium-low: there is some possibility the event may occur;
- medium-high: there is significant chance that the event will occur; and
- high: it is highly likely that the event will occur.

887. *Dashboard impact assessment*: The Dashboard allocates impact assessment to risks using qualitative measures as follows

- **High Impact**: Systemic problem/failure across a particular sector or industry-wide; Market Confidence is damaged; Significant detriment to a high or potentially high volume of consumers; Threatens the sustainability/efficiency of a product type/key market/single sector; Risk affecting most sectors;
- **Medium High Impact**: Many firms/high impact firms affected; Some threat to Market Confidence; Individual consumer detriment is high and/or many consumers are affected; Efficiency of product type/market/sector affected; Affects several sectors, or one sector acutely;

- **Medium Low Impact:** Limited population of firms (i.e. sub-sector) affected; Market Confidence not significantly threatened; Extent of detriment on individual consumers is not significant, or few consumers are affected;
- **Low Impact:** Few, low impact firms affected: Negligible consumer detriment; No threat to Market confidence.

888. *Arrow Firms Impact assessment:* The FSA first undertakes an impact assessment of each financial institution, which measures the size of the firm and number of customers. On the basis of this assessment, the FSA gives each institution an impact rating (low to high). The table below indicates this starting point; initial impact scores can be overridden for various factors (including financial crime risk), which would place the institution into a higher or lower level of supervision. The FSA indicated that approximately 31% of initial impact scores are overridden; of these, 29% of these overrides are for financial crimes concerns.

Table: Determining the impact assessment score

Sector	Example Metric	Low to Medium-low	Medium-low to Medium-high	Medium-high to High
Banking	Total Assets from £mn	450	1,800	27,00
Life Assurance and Securities Firms	Total Assets from £mn	900	3,600	54,000
Investment Management	Funds under management Total Assets from £mn	2,000	8,000	120,000

889. *Probability/risk assessment:* For financial institutions whose impact is scored as medium-low or above (i.e., banking institutions with total assets over £450 million, life insurance and securities firms with assets over £900 million, and investment management firms managing funds over £2 billion, although for private equity firms it is £500 million and for Hedge Funds it is £800 million), the FSA undertakes a separate risk/probability assessment to judge the overall risk it presents. Firms below these thresholds are first scored as "low impact" and supervised as "small firms" (unless their score has been overridden as indicated above).

890. The risk/probability assessment process starts with a desk-based review by the supervisor to identify particular areas of risk within the institution. This review takes account of a range of materials including regulatory returns, accounts and other information provided by the financial institution, which could include management information, strategy documents, MLRO annual reports and procedural and training manuals.

Core Principles institutions: General

891. The FSA supervises and monitors most financial institutions (in the banking, insurance and securities sectors) in compliance with the Core Principles as well as compliance with AML/CFT legislation. The regulatory and supervisory measures that apply for prudential supervision and monitoring are also relevant to AML/CFT. The IMF's Financial System Stability Assessment of the UK (March 2003) stated:

> The FSA either fully or largely observes the Basel Core Principles for Effective Bank Supervision and the IOSCO Objectives and Principles of Securities Regulation.
>
> However, the IMF mentions, in Principle 16, that "undue reliance on off-site monitoring makes it difficult to achieve in depth understanding of individual bank's operations particularly with respect to control arrangements and compliance requirements in, for example, the area of anti-money laundering" and underlines that this is a particular concern related to small entities. In Principle 19, the IMF noted that the use of skilled persons reports has been very much reduced and recommended a way forward, which is also shown in this report.

892. In the case of insurance industry, UK authorities carried out a wide-ranging review of the way in which insurance firms are regulated. The programme of reforms has now been implemented and the new regime focuses on delivering an insurance industry that is adequately capitalised, soundly managed and that treats its customers fairly. Since 2005 all insurers have had to meet new capital adequacy requirements. This risk-based approach requires firms to match capital to the risks their business. The UK authorities believe this new approach will help the UK prepare for the European wide risk-based capital regime - Solvency 2.

893. In general, on-going supervision takes place through "Risk Assessments," which occur at different intervals and are of different characteristics and intensity depending up on the institution. Once the risk assessment has been completed, the supervisor prepares a risk mitigation plan (RMP). This sets out issues that are judged to meet a sufficient degree of materiality and that the financial institution is expected to take steps to address, and the timeframe within which the firm has to do so. The RMP is sent to the financial institution for it to implement.

ARROW firms (medium and high impact)

894. **Medium and high impact firms**: For the largest financial institutions (39 complex major retail groups, which account for about 80% of retail business in the UK, and 43 major wholesale groups), where the potential impact of failure on consumers and the wider economy is high (i.e., "high impact"), the FSA adopts "close and continuous" supervision, with more intense supervision and regular risk assessments (typically every 12 - 24 months). This typically involves 10-12 person days on site. A review for a large financial institution can involve between 20 and 40 person days on site.

895. The FSA's focus on senior management and systems and controls, the core work – both in the pre-visit preparation and on-site investigations – assesses the high-level controls within the financial institution. This includes an assessment of the quality of management and governance and the effectiveness of the control functions (audit, compliance and risk management). If the FSA takes the view that these are adequate, it may do little or no detailed testing of lower level controls.

896. As a minimum, the ARROW risk assessment for a financial institution will involve interviews with the chief executive, finance and risk director(s), compliance officer and the Money Laundering Reporting Officer (MLRO). In many cases the supervisor will also expect to meet the head of main business areas, internal audit and members of the board (including non-executive directors). The FSA relies heavily on interviews rather than "file reviews" but in so doing will aim to obtain information that can be verified by the documentation provided before or after the visit. File testing will generally occur only when the interview response of the approved persons is not fully satisfactory. The risks presented by the financial institution are then scored against a standard matrix. This process includes an assessment of the financial crime risk within the financial institutions, as well as the controls that those institutions have in place to mitigate the risk of them being subject to financial crime. The ratings under each heading are aggregated to arrive at an overall assessment of probability for the institution.

897. The FSA has a less intense relationship with the next level down of financial institutions (approximately 650 retail financial institutions and 360 wholesale). For these **medium impact** financial institutions, the FSA adopts a lighter touch approach to the risk assessment process ("ARROW Light"). This involves a shorter visit than a "full" ARROW and will focus on some specific core areas and sectoral priorities. The distinction between "ARROW light" and full "ARROW" is one of scale and the amount of resource allocated to the risk assessment: the basic approach and objectives are the same. These firms are also subject to a relationship management based regime, with dedicated supervisors and regular risk assessments (typically once every 2 to 4 years).

898. The formal risk assessment through the ARROW framework is supplemented with certain "ongoing monitoring" activities. These operate on a continual (rather than periodic) basis. For all financial institutions the FSA conducts "baseline monitoring" (described below; this includes automated or manual analysis of material such as regulatory returns and complaints data). For higher impact financial institutions, the FSA also conducts a series of meetings with the institution's senior management and those holding control functions. This provides an opportunity to discuss issues that arise in the course of normal business or other current issues for the FSA, which could include for example, a discussion of AML/CFT issues.

899. The FSA does not capture statistics on the number of on-site visits to regulated firms specifically for AML/CFT purposes or how much time is spent on these issues as part of an ARROW firm risk assessment. The FSA tracks when the risk assessments are done and what issues they raise. All ARROW firm risk assessments include an AML/CFT element but the amount of time dedicated to exploring and assessing AML/CFT issues will depend on the risks posed by the firm.

Total number of ARROW Firm risk assessments undertaken as at 26 June 2006

Firm Sector	2003	2004	2005	Q1-3 2006	TOTAL
Advising, Arranging & Dealing as agent	189	218	143	45	**595**
IFA's	114	130	58	26	**328**
Custodians	44	40	38	6	**128**
Deposit Takers	324	219	205	35	**783**
Insurance Firms	171	127	126	45	**469**
Investment Managers	323	246	181	69	**819**
Mortgage Lenders	3	10	23	2	**38**
Principal Position Takers	31	33	23	1	**88**
Professional Entities	2	4	0	1	**7**
Trading, Clearing and Settlement Systems	4	12	9	2	**27**
Other	38	10	6	1	**55**
TOTAL	**1243**	**1049**	**812**	**233**	**3337**

900. An on-site visit is only one of a number of tools used as part of ARROW firm risk assessment. Other tools used include regulatory returns, specific information requested ahead of an on-site visit (e.g. Board papers, compliance, MLRO and audit reports, strategy documents etc.) and follow-up assessment work done after the visit either by the FSA e.g. specialist teams, including Risk Review, or by the firm itself or external specialists (e.g. skilled person reports).

Number of "ARROW Firm" risk assessments where
a money laundering issue was flagged as at 30 September 2006

Firm Sector	2003	2004	2005	Q1-Q3 2006	TOTAL
Advising, Arranging & Dealing as agent	163	170	97	53	483
IFA's	79	70	35	22	206
Custodians	37	31	34	7	109
Deposit Takers	275	182	167	54	678
Insurance Firms	137	100	79	44	360
Investment Managers	199	156	116	77	548
Mortgage Lenders	3	10	18	2	33
Principal Position Takers	22	22	16	10	70
Professional Entities	0	0	0	2	2
Trading, Clearing and Settlement Systems	4	4	7	0	15
Other	33	10	6	0	49
TOTAL	**952**	**755**	**575**	**271**	**2553**

Number of actions taken as a result of "ARROW firm" risk assessments where a money laundering element was flagged as at 30 September 2006

Firm Sector	Number of Actions				
	2003	2004	2005	Q1–Q3 2006	TOTAL
Advising, Arranging & Dealing as agent	1124	993	699	188	3004
IFA's	450	239	279	116	1084
Custodians	332	191	540	30	1093
Deposit Takers	1831	1171	1384	323	4709
Insurance Firms	913	754	735	223	2625
Investment Managers	1140	1066	856	272	3334
Mortgage Lenders	20	107	245	20	392
Principal Position Takers	184	118	122	27	451
Professional Entities	0	0	0	2	2
Trading, Clearing and Settlement Systems	58	11	46	0	115
Other	263	44	5	0	312
TOTAL	**6315**	**4694**	**4911**	**1201**	**17121**

Risk Review Department (RRD) specialist supervisory Anti-Money Laundering Visits

Period	Number
2003	50
2004	33
2005	28
Q1 2006	4

901. The higher number of specialist supervisory AML visits in 2003 reflects the tail end of work commissioned by supervisors to follow up on AML weaknesses identified after the FSA took on its new anti-money laundering responsibilities at the end of 2001. These included extensive numbers of visits to review systems and controls in several "clusters" of firms which were identified as posing higher AML risks. In 2005 RRD also conducted visits to review anti-fraud controls for the first time. 16 such visits were completed during 2005/2006 as part of a thematic review.

Skilled Persons Reports

902. FSMA, Part XI, Section 166 gives the FSA the power to commission 'reports by skilled persons'. This means the FSA can require specialists e.g. accountants, auditors and consultants to provide it with a report on any matter in relation to the FSA's duties. The FSA would typically use this report to obtain an independent view of aspects of a financial institutions business which cause it concern, including money laundering. The appointment of a skilled person is a regulatory tool used primarily by Supervision and Enforcement.

903. The area a report would, for example, include: client money handling; controls to prevent money laundering; collateral management; Management of an appointed representatives network; corporate governance arrangements; transaction reporting; past sales of retail financial products; and controls to prevent market abuse. The table below shows the number of skilled persons reports in relation to AML.

Sector	2003	2004	2005	2006
Banking	0	1	1	0

Insurance	0	0	1	0
Securities	0	0	0	1*
Total FSA Skilled Person Reports	24	18	16	6*

*As of 7 September 2006

Money value transfer and money exchange

904. FSA-regulated financial institutions providing a money or value transfer services, or a money or currency exchanging service are subject to the FSA's supervisory approach as described above. Money or value transfer businesses fall within the definition of Money Service Businesses (MSBs) and as such are liable to the monitoring based visiting programmes and sanctions by the HMRC. The HMRC supervision for MSBS for compliance with AML /CFT controls was introduced in 2002. MSBs include high risk categories of financial services in the area of ML/FT like money changers and money transmitters. Under the current regime, 3,621 entities are registered and there are 32,131 premises.

Figures as of 30th June 2006 – The MSB register

BUSINESS TYPE	REGISTERED PRINCIPALS	NUMBER OF PREMISES	PERCENTAGE PREMISES
BdC/CC	73	534	1.6%
Money Transmitter (MT)	1,515	9,767	30.3%
Bureau de Change (BdC)	852	4,276	13.3%
BdC/MT/CC	288	15,465	48.1%
Cheque Casher (CC)	546	1371	4.2%
BdC/MT	244	407	1.2%
MT/CC	103	311	0.9%
TOTAL	**3621**	**32,131**	**100%**

905. When MSBs register, HMRC conducts an initial risk assessment. The "Risk Matrix" devised by HMRC to target its supervisory efforts, developed with the input of experienced HMRC assurance officers, combines factual data about the MSB from HMRC records with the MSB's own input in response to HMRC questionnaires. All MSBs are then scored against the "Risk Matrix" to enable HMRC to prioritise its assurance visits. The questionnaire covers the following issues:

- Number of penalties issued;
- Number of warning letters issued;
- Law enforcement intelligence about trader;
- Previous convictions of licensed principal or any staff under any legislation including AML/CFT;
- Annual turnover of MSB activity;
- Location of business premises;
- Most frequent or average value of transactions; and
- Percentage of transactions in cash.

906. The assurance process then takes place as follows:

Step 1: Trader registers and pays fee.
Step 2: HMRC risk assessment.
Step 3: Trader receives first visit:
- If compliant, risk score adjusted and no further action.
- If non- compliant warning letter issued.

Step 4: Return visit within 12 months:
- If compliant, risk score adjusted and no further action.

- If non-compliant, penalty issued.

Step 5: Further return visit:

- If compliant, risk score adjusted and no further action.
- If non-compliant, penalty increased or if circumstances warrant – prosecution initiated.

907. The system is going through an evolutionary change to focus more consistently on those MSBs that are not compliant. Newly registered businesses are assessed for risk and visited only if the risk is deemed sufficient. Resources are being refocused on businesses that are high-risk and / or non-compliant. The MSBs considered as high risk are the ones with a very large annual turnover.

908. HMRC does not break down its management reports on visits and penalties below MSB level to individual sectors. However, as MVTs comprise a high proportion of the register, and MVTs are considered a high risk business activity, it is reasonable to assume that many of the HMRC visits are to this category of trader are made and warning letters / sanctions applied where appropriate.

No. of Assurance Visits to MSBs by HMRC	
Quarter	No. of visits
Q1 30/06/2005	444
Q2 30/09/2005	360
Q3 31/12/2005	492
Q4 31/03/2006	654
Q1 30/06/2006	394

909. There were 1,950 visits to MSBs during the financial year 2005/2006 (mix of premises and firms). Assurance resources are focussed on businesses designated as high risk and on the largest firms. The top ten firms, controlling 71% of the premises through which MVT services are provided, are automatically allocated a high level of supervisory resource without further risk assessment. However, the remaining 29% of premises are allocated supervisory resource according to a risk matrix that considers all the following issues: size, compliance history, any relevant law enforcement / FIU intelligence, previous convictions of staff, geographic location, percentage of cash transactions, and average value of transactions. For the large firms the visits can last for 5 or 6 days, not including substantial scrutiny of transaction records, which last much longer. The recent government review of the sector has resulted in a number of proposals to tighten the regulatory environment of all aspects of MSB operation, including moving to a licensing regime to strengthen the HMRC supervision. Overall, there are some minor concerns about the current on-going monitoring for MSBs. The current on-going monitoring for MSBs focuses on large firms in an area where the small firms might be more exposed to the ML and FT risks; a better allocation of resources would be welcome in the framework of the current review of the regime.

Small firms (low impact) monitoring

910. Of the approximately 29,000 FSA-authorised financial institutions (see chart after paragraph 26), approximately 13,600 are characterised as "low impact" financial institutions (determined by their asset thresholds) account for the bulk in terms of the number of authorised entities. However, within this number only some 3,971 small firms are subject to the FATF financial institution definition (this includes investment fund managers (managing up to two billion pounds of assets) and stockbrokers, wholesale asset managers and brokers, venture capital and corporate finance firms. – see the table after paragraph 914. In addition, 4,717 financial advisers who are not managing funds) are subject to AML/CFT requirements and the FSA; 4,905 are EEA passported firms providing cross-border services for which the FSA does not have any supervisory responsibility. While individually they have a low impact on FSA's regulatory objectives (and are therefore judged to be low risk), collectively they pose a relatively large risk.

911. These institutions are not assigned a relationship manager and are not subject to a routine risk assessment or other on-site inspections and/or monitoring. Instead, the focus is on baseline monitoring and conducting thematic work with samples of financial institutions (both described below). For these firms, information is collected from various sources including: electronically-submitted regulatory returns from many firms, product sales and other data provided by product-providers, output from visits to firms, and information received from the FSA Firm and Consumer Contact Centres, the Financial Ombudsman Service and from whistleblowers. Much of this information is analysed electronically. None of the information is related to anti-money laundering, and no information is collected on a yearly basis in this regard.

912. Where a number of similar problems or risks are identified across a number of small financial institutions, the FSA will consider whether to set up a project to measure the extent of the risk and to find ways to mitigate it. These projects will normally involve collecting data from a sample of selected small firms by way of a questionnaire, analysing the data and selecting from the sample a number of firms to visit to test the results. The FSA then provides feedback to financial institutions to help them learn from the good practices (and avoid bad practices) seen in other financial institutions. As in other areas, enforcement action is considered where particularly serious breaches at particular financial institutions are found.

913. This thematic work, which addresses risks specific to the small, non-relationship managed firms, only includes small firms in the project population. In addition, thematic work may also be carried out across firms of all sizes, with samples including both relationship-managed and non-relationship-managed firms.

914. The table below indicates the kinds and number of small firms in the UK.

	Custodians	Deposit Takers	Insurance Firms	Investment Managers	Mortgage Lenders	Principle Position Takers	Professional Entities	Trading Clearing & Settlement Systems	Financial Advisers (managing funds)	Advising, Arranging & Dealing as agent	Other	Total Financial Institutions subject to FATF Recs.	Financial Advisers (not managing funds)	Total
Retail Firms	2	565	171	248	41	2	501	2	38	251	15	**1,836**	4,717	**6,553**
Wholesale Firms	9	53	9	985	4	49	103	18	16	874	15	**2,135**		**2,135**
Total subject to AML/CFT supervision												**3,971**	4,717	**8,688**
EEA-Passported Services Firms[28]	0	273	302	57	0	0	0	1	0	4191	81			**4,905**
Total														**13,593**

915. ***Investment fund managers:*** This category includes firms with up to 2 billion pounds of assets under management. These firms are considered "small firms" by the FSA and are subject to the light supervisory approach applicable to small firms. This conclusion is based on the assumption that individually they have a low impact, and pose a low risk to FSA's objectives.

[28] Under EU law, the FSA does not have any supervisory responsibility for these firms.

916. ***Financial advisers:*** typically fall into two categories: (1) 38 such advisers who manage funds on behalf of their clients and, therefore, fall within the financial institutions definition within the FATF Recommendations; (2) 4,717 advisers who do not manage funds but simply provide advice. The UK authorities consider that this latter category poses a low risk for money laundering.

917. ***Deposit-takers:*** The breakdown on the statistics for deposit-takers is as follows:

- Retail – The 565 figure comprises 19 small banks, 3 building societies[29], and 543 credit unions.
- Wholesale – The 53 deposit-takers are predominantly small banks. Of these 53 firms, 15, as at December 2006, are required to submit a compliance report. The remainder are subject to the ARROW Small Firms (including baseline monitoring) and Themes approach.

ARROW Themes

918. "Thematic Works" aim to assess and rate the risks of a particular *issue*--i.e., to identify problems and find solutions. The normal output from this work tends to be in the form of a communication to the regulated sector or individual institutions, discussion papers, or guidance on the FSA website. As in the risk assessment process, serious breaches by particular financial institutions, identified during thematic work, will result in referral to enforcement. Thematic work can be specific to small, non relationship managed firms or it may be carried out across firms of all sizes, with samples including both relationship-managed and no-relationship managed firms.

919. One possible use of the findings of a thematic project is for it to be included in "a sub-sector analysis," which is available to supervisors and an integral part of the ARROW model to ensure current industry issues are considered when planning a firm specific risk assessment. This sub-sector risk process therefore acts as a bridge between the vertical (firms) and horizontal (themes) approaches, as well as providing an efficient mechanism for sharing knowledge across different areas.

920. Thematic works generally involve initial contacts with a sample of financial institutions (e.g. via questionnaires, telephone interviews) and in many cases follow-up on-site visits to selected firms in the sample (typically one day, but can be longer or shorter). Sometimes the FSA might look at issues covering the market as a whole. These thematic projects are usually coordinated across the FSA by a single team that will work closely with the relevant supervisory divisions. The project team analyses and assess the issue in question. In many cases this involves a short visit (typically a day but could be longer or shorter) to a selection of institutions. But other techniques may be used, such as telephone interviews, questionnaires, document reviews and consumer or market research and mystery shopping. See the discussion under R.25 ("Guidance") below for a description of the specific thematic projects and results.

921. Results of these projects are communicated to the regulated sector and can constitute an effective way to improve the awareness of all firms in the AML/CFT area. Referring to the review of compliance standards in venture capital, the first thematic work in August 2005 identified weaknesses and areas for improvement were fed back to the industry via letters and discussions with the industry's trade body. In 2006, the FSA undertook a thematic review in this area; the findings suggested that there are improvements still to be done. Thematic work is an important supervisory tool as part of the FSA's overall regulatory approach, for assessing compliance or otherwise identifying issues within a defined population or sub-sector of firms. This is supported by a communication strategy which includes seminars, road shows and feedback to both trade bodies and firms. However, there remains

[29] While classified as "low impact" because of their size and therefore included in this chart, these 19 banks and 3 building societies are automatically "upgraded" to be supervised as "medium/low" impact firms, which is a category between these low impact and the medium impact firms described earlier. These firms are supervised by a single supervisory team, although they are not subject to regular risk assessments.

room for improvement, and this approach cannot be the only tool used by the supervisor to ensure an adequate level of compliance with AML/CFT requirements by small firms.

Baseline monitoring

922. All retail and wholesale firms, whether classified as small firms or medium-high impact firms (ARROW Firms) are subject to baseline monitoring. This consists of gathering information from various sources such as: product sales and other data provided by product-providers; information received from the FSA's Firm Contact Centre and the Consumer Contact Centre, matters arising during regulatory transactions such as authorisation and change of control, common themes that arise from visits to firms, liaison with the Financial Ombudsman Service, and regulatory returns. In this framework, the regular (normally semi-annual or more frequent) regulatory returns will include information on: firm financial information, staff training & competence information, firm conduct of business information, firm sales data, firm compliance data, but nothing on AML/CFT-related issues.

923. Any intelligence from the baseline monitoring, or through information received from other sources such as firms, staff within firms, members of the public or law enforcement, will generate alerts. This will be assessed and, where judged necessary, acted on. For example, since 1st November 2004, for small retail firms, the FSA has assessed 510 pieces of information in relation to financial crime. Thirty-seven of these have been specific to AML/CFT and in 20 cases the information received has required action from supervisors. For small wholesale firms, on average, 5% of all alerts from baseline monitoring are AML/CFT related.

Analysis

924. While the risk-based approach is sensible and sound in the abstract and NCIS (and now SOCA/UK FIU) have issued some sector specific alerts, the success of the risk-based approach on the ground in terms of effectiveness rests upon certain elements which were not always encountered in practice, in the documents, activities and debates with the UK authorities and the financial sector.

925. The FSA has shown how some of the alerts issued by the UK FIU have led to AML/CFT risk issues which inform its supervisory work. These have included alerts relating to private banking, independent financial advisers and PEPs. The examples given go some way to addressing the core threat to the UK financial system which is probably related to its role as one of the leading international financial centers, and would therefore certainly – simply in terms of volume, and typologies – lie in areas of international finance, whether commercial or private banking.

926. Financial entities in the private sector take their lead from those risks that are identified explicitly in the JMLSG Guidance or other official documents; during discussions with private sector entities on their specific ML/FT risks, the institutions uniformly cited the official information without generally referring to the identification of the firm's own risk. This situation is expected to evolve with the implementation of the recent guidance because, a successful implementation of the risk based approach requires that firms analyse their own risks, and the Authorities need to address the current position, which seemed to the evaluation team that there was no self identification of a firm's own risk. The focus of firms seems to remain on managing regulatory risk, and this points to a weakness in the practical implementation of the risk-based approach which should be addressed if the current UK stance is continued.

927. There is a minor concern that the ML/FT risk does not seem to be effectively taken into account by using impact as the initial means of allocating supervisory resources to identifying and mitigating risk. In the area of AML/CFT, the size of the firm is not a sufficient criterion. While most small banks are considered as medium impact, 3,971 other small firms (i.e. are deemed low impact and therefore subject to less supervision (no regular individual on-site visits). This arises by virtue of their size according to total assets and not according to AML/CFT risk, and therefore the evaluation team could not conclude that these small firms are adequately supervised. These include deposit takers,

insurance firms, investment managers (managing up to 2 billion pounds of assets), "advising, arranging and dealing as agent" that are neither subject to regular on-site visits nor to adequate off-site monitoring. In particular, this includes a certain number of banks (19), insurance, securities dealers, and investment managers—which are Core Principles institutions but only subject to off-site "baseline monitoring" and possibly risk-driven ARROW Themes projects. Although the relatively few low-impact banks are supervised more closely than other small firms, it must be underlined that small firms often have much weaker system of internal control and consequently are more exposed to the AML/CFT risk than larger firms with strong systems and controls. The management of small firms is more often less experienced and small entities are more subject to earning pressure. These concerns are mitigated by the fact that volume of business undertaken by small firms is a tiny proportion of total business passing through the financial sector, and other than a very small number of "core principles" institutions are not in sectors assessed as high risk by UK law enforcement.

928. The vast majority of on-site assessments rely on interview-based visits without an analysis of a sample of customer and transactions files. The FSA has explained its supervisory approach is to hold senior management accountable for running their business in accordance with the FSA's principles for business. The aim of any visit is to see that the senior management has developed and operates a set of controls that address the key risks the firms face, and how they assure themselves that the controls are operating effectively. A review of management information, including internal audit report, may lead to some file testing and sampling but this will generally occur only when they feel that the interview response of the responsible approved persons (management, MLRO) is not fully satisfactory. It is a stated policy to look through files only if there is a reason to do so. As a result, there is a large reliance on the internal reports produced by the firms and generally no external control of customers and transactions files to check whether this reliance was grounded or not. This policy applies not just to firms subject to risk assessments, but also to small firms.

929. An obligation to file AML/CFT reports with the FSA can happen if directed to do so under a risk mitigation program or upon request by the FSA, and these are obtained for large firms as part of the ARROW risk assessment process. This does not occur with small firms, which are not subject to individual risk assessments. The AML/CFT reports have to be written, and the MLRO report has to be presented to the management of the firm, although there is no obligation to regularly send any FSA regulatory returns as related to AML except in the case of a risk mitigation program for large or medium firms, and therefore the FSA does not regularly receive any information related to the implementation of the AML/CFT requirements, especially by medium and small firms. These limitations sharply reduce the efficiency of the supervision, for the small firms, which do not receive on-site visits and only have alert based remote monitoring for AML/CFT risks. Therefore, the evaluation team considers that regular and systematic on-site visits need to be made on small firms including files reviews, given the fact that less reliance can be placed on small firms. The adequacy of remote monitoring for other firms could also be improved if AML/CFT reports already produced by the firm between two on–site visits are more systematically reviewed or analysed.

930. For other activities (consumer credit, financial leasing, and certain guarantees and commitments, brokers, factoring, safe-keeping and administration) there is a lack of AML/CFT supervision. According to the UK authorities, these non-regulated sectors will be supervised for compliance with AML/CFT controls under the Third Directive. It is recommended to strengthen the AML/CFT scope of this major international centre for investment, insurance industry and private banking and one of the largest commercial banking sectors in the world. Effectively, if some of these unregulated activities represent a small number of financial services' firms, consumer credit firms represent 110,000 active licences.

931. HMRC supervision of MSBs, which are recognised globally as a high risk for ML but particularly FT, is a lighter regime than FSA supervision..

Guidelines – R.25 (Guidance for financial institutions other than on STRs)

932. The JMLSG Guidance is the key document that provides practical interpretation to financial institutions in complying with AML/CFT legislation, FSA AML rules and good generic industry practice guidance. These are extensive, comprehensive documents, and are extremely useful for the industry. (Part I: "Guidance for the UK Financial Sector" is over 150 pages long; Part II: Sector Guidance, is over 140 pages long.) The JMLSG website provides relevant AML/CFT information to help financial institutions comply with their obligations (www.jmlsg.org.uk).

933. The FSA has also established a number of mechanisms to help financial institutions to comply with their regulatory requirements. Under FSA Handbook, SUP 9 the FSA is able to provide individual guidance to financial institutions undertaking FSMA-regulated activity. This will normally be given to one particular financial institution, which relates to its own particular circumstances or plans. It cannot be relied upon more generally by other financial institutions. The FSA has a website dedicated to AML/CFT which contains publications, press releases, speeches and other relevant information about the FSA's role in reducing the extent to which FSA regulated financial institutions can be used for the purpose of money laundering: http://www.fsa.gov.uk/pages/Library/ Other_publications/ Money/index.shtml.

934. The FSA has undertaken a number of initiatives designed to help regulated financial institutions to comply with their regulatory AML/CFT requirements. This includes "thematic work", examples of which are set out below:

935. ***Money Laundering Theme: Tackling our new responsibilities*** **(July 2001)**: The main aim of the Money Laundering Theme was to: assess the current level of industry compliance with the MLRs 1993; identify the financial activities and sectors that are subject to the greatest money laundering risks and, therefore, and pose the greatest risks to the FSA objective of reducing financial crime; set out how the FSA is taking forward its responsibilities in this area. The report published in July 2001 included examples of good practice in terms of effective money laundering systems and controls and identified six 'risk clusters' which were perceived to be the most vulnerable to money laundering – international banking, domestic banking, IFAs handling client money from abroad, on-line broking, spread betting and Credit Unions. As a result of the Money Laundering Theme the FSA carried thematic work on the six clusters that were identified. The outcome of this thematic work was published:

- *International banking (*July 2001): http://www.fsa.gov.uk/pubs/other/ml_ibc.pdf
- Domestic banking (August 2002): http://www.fsa.gov.uk/pubs/other/ml_domestic_banking.pdf;
- *Online broking and spreadbetting* (October 2002): http://www.fsa.gov.uk/pubs/other/ml_sb_olb.pdf;
- *IFAs* (February 2003): http://www.fsa.gov.uk/pubs/other/ml_sm-firms.pdf;
- *Credit unions* (January 2004).

936. *Annual MLRO reports (March 2004):* In March 2004, the FSA carried out a review of financial institutions annual Money Laundering Reporting Officers' reports. The findings from this thematic work were communicated to the industry via letter published on the FSA website.

937. *FSA open letters to the JMLSG (2004-2006):* On several occasions the FSA has written open letters to the JMLSG explaining to the industry the FSA position on specific issues. A particular theme adopted within the letters was encouraging financial institutions to adopt a risk-based approach in relation to AML/CFT. Other letters include:

- *FSA Supervisory Approach (October 2004):* One of the areas of feedback the FSA received on its 'defusing the ID issue' initiative was that financial institutions were adopting a

conservative approach to ID because of the FSA's supervisory approach and enforcement actions. In October 2004, the FSA wrote to the JMLSG in a letter aimed to reinforce the FSA's supervisory approach and the circumstances in which it would take enforcement action. http://www.fsa.gov.uk/pubs/other/ money_laundering/jmslg.pdf.

- *Fighting money laundering and terrorist financing more effectively – proposals in the UK Consultation Paper, "Reviewing the FSA Handbook" (July 2005):* In July 2005, the FSA wrote to the JMLSG to explain the rationale behind the proposal in CP 05/06, 'Reviewing the FSA Handbook', to delete the Money Laundering Sourcebook in favour of high level provisions within SYSC. The letter highlighted the FSA's view that the proposals would put a sharper focus on key elements of a financial institution's approach to financial crime: http://www.fsa.gov.uk/pubs/other/letter_jmlsg.pdf.

- *Fighting money laundering and terrorist finance: moving forward over the risk-based approach (April 2006):* In April 2006, The FSA wrote to the JMLSG to set out challenges for the industry, FSA and Government in moving towards a risk-based approach. http://www.fsa.gov.uk/pubs/other/ money_laundering/letter_ml.pdf.

- *Fighting money laundering and terrorist finance: moving forward over the risk-based approach – our supervisory expectations (August 2006):* In August 2006, to coincide with the formal removal of the FSA's Money Laundering Sourcebook, the FSA wrote to the JMLSG to setting out regulatory expectations and stressing the FSA's commitment to supervising in ways that promote the risk-based approach to AML/CFT. As part of this, the FSA published the key messages given to FSA supervisors – a memo setting out the implications of supervising AML/CFT in a risk-based way and a note setting out six key issues on AML/CFT. http://www.fsa.gov.uk/pubs/other/money_laundering/ letter_310806.pdf#search=%22jmlsg%20letters%22.

938. *'Defusing' the ID issue (October 2004 & June 2005):* The FSA initiative to 'defusing the ID issue' resulted in two progress reports; the first report, 'ID – defusing the issue: a progress report', was published in October 2004 and identified a number of key propositions which were designed to feed into the revision of the JMLSG Guidance. A follow-up report on progress to date was published in June 2005: http://www.fsa.gov.uk/pubs/other/id_report.pdf and http://www.fsa.gov.uk/pubs/other/ id_report2.pdf.

939. *Hedge Funds Project (2005):* This project looked at the anti-money laundering (AML) policies, procedures and controls of a small number of UK authorised hedge fund managers and concluded that the fund managers visited as part of this project were sufficiently aware of, and had procedures in place to meet, their AML legal and regulatory obligations: http://www.fsa.gov.uk/pubs/discussion/ dp05_04.pdf.

940. *Review of compliance standards in venture capital firms (August 2005):* In 2005, the FSA carried out a thematic review on the effectiveness of compliance standards in Venture Capital Firms. This included a review of AML/CFT controls. The review identified a number of weaknesses in relation to AML/CFT controls including issues on compliance with sanctions lists, staff training, annual MLRO reports and record keeping.

941. *Feedback from the FSA's review of anti-financial crime controls in venture capital firms (July 2006):* In 2006 FSA undertook a thematic review of Anti-Financial Crime Controls within smaller venture capital firms. This latest review focused on a small, but representative, sample of firm's approach to market abuse and the Market Abuse Directive, the identification and management of fraud risks and follow-up work in relation to anti-money laundering controls.

942. *Wholesale Firms PEPs thematic work (2006):* The FSA carried out thematic work looking at wholesale financial institutions' systems and controls over Politically Exposed Persons (PEPs). The

FSA findings found that firms are aware of and understand their responsibilities in addressing this issue. The outcome of the FSA PEPs thematic work is available on the FSA website at: http://www.fsa.gov.uk/Pages/About/What/financial_crime/money_laundering/peps/index.shtml.

Small firm thematic work

943. The FSA had carried out a number of thematic projects in relation to small firms that have included an AML/CFT element. These include:

- *Annual MLRO reports (July 2003):* A sample of annual MLRO reports were reviewed to assess compliance with the FSA's Money Laundering Sourcebook.
- *AML Identification Procedures in Private Client Investment Firms (July 2004*): The AML identification procedures of Private Client Investment Firms were reviewed.
- *Money Laundering Procedures in small firms* (November 2004 – April 2005): This project was set up to identify small financial institutions who were failing to meet anti-money laundering requirements and to ensure they understood the requirements of the Money Laundering Sourcebook in the context of all relevant Money Laundering legislation.
- *Geographic visits* (April – July 2005): Geographic visits were an initiative launched in 2004 and fitted in with the supervision strategy at the time by collating information on specific issues and identifying concerns feeding back to financial institutions. Anti-fraud and AML questions were designed to ascertain the extent to which firms were aware of their financial crime risks, take seriously the possibility of financial fraud, to remind them of their responsibilities to both staff and external customers, and to determine what procedures and controls, financial institutions have in place to deal with this issue.
- *AML Identification as part of the Quality of Advice Cluster Work* (January – March 2006) AML identification procedures and how source of client funds were validated were reviewed as part of wider thematic project on Quality of Advice Cluster Work.
- *AML/CFT systems and controls in relation to small retail investment firms* (November 2006): The FSA is undertook a thematic project reviewing the level of understanding and awareness of small investment firms following the FSA's new AML rules and the revision of the JMLSG Guidance. The findings of this thematic review were communicated to firms on the FSA website and included a self assessment tool to help small firms adopt appropriate practices to mitigate money laundering and terrorist financing risk (included below). Thematic work findings:
  http://www.fsa.gov.uk/pages/Doing/small_firms/advisers/library/aml_ctf.shtml
  Self assessment tool:
  http://www.fsa.gov.uk/pages/Doing/small_firms/advisers/pdf/aml_tool.pdf

944. The findings from these thematic projects has been fed back to financial institutions and the industry using a variety of methods including newsletters, the small firms website, FSA outreach through "Road Shows and Geographic Visits".

Current and future thematic work

945. *Transaction Monitoring (Q4 2006):* In the FSA's view transaction monitoring (TM) is a key element in a risk-based approach to AML. The FSA has undertaken a review of a sample of financial institutions' experience with operating different kinds of TM software. This resulted in a report which highlights best practice as well as any deficiencies in the implementation and ongoing effectiveness of TM systems.

946. *AML/CFT systems and controls in relation to small retail investment firms (Q4 2006):* The FSA is currently undertaking a thematic project reviewing the level of understanding and awareness of

small investment firms following the FSA's new AML rules and the revision of the JMLSG Guidance. The outcome of this work will be fed back to financial institutions in order to promote good practice

947. *Private banking (Q4 2006):* At the time of the on-site visit, the FSA was undertaking a review of money laundering risk in private banks in O4 2006 which will include looking at PEPs issues.

948. *Implementation of the risk based approach to AML/CFT (Q1 2007):* The FSA intends to conduct some thematic work in Q1 2007, looking at how a variety of different types and sizes of financial institutions have responded to the recent changes in the FSA's money laundering rules and the JMLSG Guidance and the implementation of the risk-based approach to AML/CFT.

HMRC

949. The key guidance provided by HMRC to MSBs in MSB2, which is intended to assist MSBs in complying with their AML/CFT obligations. HMRC also commissioned a Business Needs Survey in 2004 to identify the value of HMRC guidance material: 95% of respondents found HMRC regisration guidance useful or very useful and the registration process easy; 90% had found the operational guidance that HMRC had prepared with industry input useful or very useful; almost three-quarters had seen the educational video HMRC prepared, again with industry input, titled "Money for Nothing" and the vast majority felt it helped their understanding.

950. According to UK authorities, visiting every newly registered trader during the period that the regime was becoming established to explain sectoral obligations was very well received. The survey confirmed very favourable trader opinions about these visits. As a result of the visits: more than 50% of traders felt much more confident in their understanding of the AML/CFT regulatory regime; more than 60% were very satisfied with the the visit and a further 34% fairly satisfied.

951. HMRC has issued leaflets for their (retail) customers in six different languages to date - Bengali, Farsi, Hindi, Punjabi, Spanish, Urdu - and will offer more if this is justified by the take up. In the case of MSBs the video "Money for Nothing" was distributed as part of a registration pack to all enquirers concerning MSB registration until its withdrawal in 2005 (A revised, up to date DVD replacement is presently being prepared).

3.10.2 Recommendations and Comments

952. *Rec. 17:* the FSA has wide range of enforcement and sanction powers, including sanction against the senior management and other the approved persons. It can impose a penalty to an approved person for misconduct and may issue a public censure against an individual. However, the current number of penalties applied (17) appears low; authorities should consider targeting ML/FT more specifically. HMRC should be given more direct powers to take against directors and senior management for AML/CFT breaches.

953. *Rec. 23:* All types of financial institutions as defined in the FATF Methodology are subject to the AML/CFT laws. However, some activities that come under the FATF definition are neither supervised nor obliged to comply with FSA rules and industry guidance (consumer credit, financial leasing, guarantees and commitments, brokers, factoring, safe-keeping and administration). It is recommended to bring these entities into an appropriate AML/CFT supervisory framework. According to the UK authorities, these non-regulated sectors will be supervised for compliance with AML/CFT controls under the Third EU Directive.

954. The current AML/CFT supervisory framework for the largest retail firms is generally intense and comprehensive. However, when conducting on-site risk assessments (for the largest as well as medium impact firms), the FSA should more often and thoroughly review files and conduct more sample testing.

955. For smaller firms, the UK authorities should adjust their risk assessment basis for determining the level of supervision in order to take more into account the actual AML/CFT risks: in the area of AML/CFT, the size of the firm is not a sufficient criterion to justify an assumption of lower risk. Small firms, including among others deposit takers (including some small banks), insurance firms, investment managers, "advising, arranging and dealing as agent ", i.e. 3,971 firms are neither subject to regular on-site visits nor to adequate off-site monitoring (except in the case of thematic work where a sample of small firm can be subject to an on-site visit). Supervision for certain of these entities currently categorised as "small firms" should be strengthened, especially small banks (even if they are supervised more closely than the other small firms), securities brokers/investment managers, and insurance firms which are Core Principles institutions.

956. In addition, the supervisory framework would be strengthened if ongoing monitoring required financial institutions to regularly send AML regulatory reports to the FSA so as to keep aware of the firm's AML/CFT issues and allow for some analysis of these reports—trends, minimum activities, special problems—across the whole range of entities within FSA's remit to identify areas of concern in the less intensely supervised sectors.

957. With regard to the MSBs, the supervisory framework and on-going monitoring program should be enhanced. UK authorities are currently planning this and in this regard current have a public consultation document with various proposals. In order to more effectively perform its tasks, HMRC should deploy a broader allocation of resources at all levels of ML/FT risk.

958. *Rec. 29:* The FSA has comprehensive powers of inspection, including on-site visits, and can obtain all information it seeks. The FSA also has comprehensive sanction powers. The HMRC has adequate powers of inspection; however, enforcement powers should be enhanced (see Recommendation 23). The UK authorities should also designate an authority (or authorities) with adequate powers of inspection, monitoring, and sanction with regard to those activities currently not supervised by FSA (i.e., consumer credit, leasing, etc.).

959. *Rec. 25:* The government authorities and the JMLSG have issued comprehensive guidance to the private sector. While it has only been "approved" by the Government for those financial sector entities participating in the JMLSG, it can also serve as useful guidance for the currently un-supervised sector.

3.10.3 Compliance with Recommendations 23, 29, 17 & 25

	Rating	Summary of factors relevant to s.3.10 underlying overall rating
R.17	**LC**	• The number of FSA disciplinary sanctions (since 2001) seems relatively low: 14 enforcement actions including warnings and the cancellation of one licence. • Administrative sanctions of HMRC do not extend to directors and senior managers.
R.23	**LC**	• The impact assessment method (to determine the level of supervision) does not adequately take into account AML/CFT risk, and therefore there are some concerns about the adequacy of supervision for small firms. • Consumer credit, financial leasing, guarantees and commitments, brokers, factoring, safe-keeping and administration are neither supervised nor expected to comply with professional guidance. • For most on-site assessments (high and medium impact firms), there is an over reliance on interview-based visits without sample testing, and for the medium firms the FSA does not receive any information related to the implementation of the AML/CFT between two on-site visits. • There are some minor concerns about the current on-going monitoring for MSBs.
R.25	**C**	
R.29	**LC**	• With regard to entities that are not subject to the FSA regime (such as consumer credit and leasing) there is not an authority with adequate powers of inspection and sanction for

		AML/CFT. • For MSBs, sanctions cannot generally be applied to directors and senior managers.
R.30	**LC**	• Overall, the allocation of HMRC's resources is a concern, as current resources are focused on the MSBs with the largest turnover which does not adequately address the smaller MSBs which might be of higher risk for ML/FT.

3.11 Money or value transfer services (SR.VI)

3.11.1 Description and Analysis (summary)

Special Recommendation VI

960. The MVT sector is the most ethnically diverse group within the MSB sector. HMRC has pursued a partnership approach with industry in order to improve the effectiveness of AML systems by encouraging participation in preparation of industry guidance, educational DVD's etc. HMRC has sought to reach out to ethnic minority groups by establishing an MSB Forum, an industry grouping that meets quarterly to discuss AML issues, arranging regional seminars and facilitating the introduction and growth of an industry body to represent the interests of MVTs.

961. Money value transfer services fall within the description of money service businesses in the MLRs Regulation 2(2)(d): "the business of operating a bureau de change, transmitting money (or any representation of monetary value) by any means or cashing cheques which are made payable to customers." Therefore, MVT service operators fall within the MSB category. This category includes "traditional" MVT operators such as Western Union and also alternative remittance business since the regulations merely refer to the activity being conducted.

962. HMRC is currently designate to register MSBs (including MVT service operators), maintain a current list of the names and addresses of licensed and/or registered MVT service operators. HMRC is responsible for ensuring compliance with current registration requirements in the MLRs 2003. HMRC holds a register of all MSBs, broken down by category (many firms offer several business within the MSB category). MVTs (whether they conduct only this business, or conduct MVT business along with bureaux de change and/or money changing services and or check cashing services) are separately identifiable within the register.

Figures as of 30th June 2006 – The MSB register

BUSINESS TYPE	REGISTERED PRINCIPALS	NUMBER OF PREMISES	PERCENTAGE PREMISES
BdC/CC	73	534	1.6%
Money Transmitter (MT)	***1515***	***9767***	***30.3%***
Bureau de Change (BdC)	852	4276	13.3%
BdC/MT/CC	***288***	***15465***	***48.1%***
Cheque Casher (CC)	546	1371	4.2%
BdC/MT	***244***	***407***	***1.2%***
MT/CC	103	311	0.9%
TOTAL	3621	32131	100%

963. MVT operators as MSBs are covered by the rules of the MLRs, as described for other financial institutions above. However, MVT are not subject to the government-approved JMLSG guidance and their further details, although HMRC has issued additional and useful guidance to MSBs. Hence, there are some concerns with regard to the extent that certain Recommendations apply: customer identification such as a lack of beneficial ownership requirements (R.5), PEPs (R..6), and transaction monitoring (R.11, 21).

964. As described above, HMRC currently has an assurance program to assess compliance with the MLRs. MVTs are subject to the HMRC risk based visiting programme outlined above. (See paragraphs 904 to 909 for a more detailed discussion). There are seven full time equivalent (FTE) officers tasked with prioritising assurance visits to MSBs (3,600 firms, 32,000 premises) and HVDs (1,500 firms) on a risk-sensitive basis. They are assisted by 19.1 FTE intelligence officers who are directly involved in work to analyse the risk posed by individual firms and premises. There are 28.5 FTE assurance officers who actually undertake the compliance visits. There were 1,950 visits to MSBs

during the financial year 2005/2006 (mix of premises and firms). Assurance resources are focussed on businesses designated as high risk and on the largest firms. The top ten firms, controlling 71% of the premises through which MVT services are provided, are automatically allocated a high level of supervisory resource without further risk assessment. For these large firms, the visits can last for 5 or 6 days, not including substantial scrutiny of transaction records, which can go on for much longer. The remaining 29% of premises are allocated supervisory resource according to a risk matrix that considers all the following issues: size, compliance history, any relevant law enforcement / FIU intelligence, previous convictions of staff, geographic location, percentage of cash transactions, and average value of transactions. Overall, there are some minor concerns with the adequacy and intensity of the program. HMRC is allowed to increase the fee that it charges MSBs for registration (subject to Ministerial approval). It is currently seeking approval to increase the fee in order to increase the amount of personnel it can deploy.

965. MSBs must maintain a current list of its agents and make this available to HMRC. According to MLRs Regulation 10 (2)(b)(v), MSBs must send to HMRC "any agency or franchise agreement relating to the business, and the names and addresses of all relevant principals, agents, franchisors or franchisees…" If there is any change to this information, Regulation 11 requires that this be supplied to HMRC within 30 days.

966. As described above, the HMRC has certain sanction authority in relation to MSBs. HMRC may issue a warning letter, and impose financial penalties up to £5,000. This can be issued repeatedly if necessary – i.e. up to £5,000 for each day the breach continues; it can also be issued separately for separate and / or simultaneous breaches of the Regulations. However, there are not adequate sanctions that can be used against directors and senior managers

Additional elements

967. Certain elements from the best practices paper for SRVI have largely been implemented, including the requirement to register; the review of applications; and some compliance monitoring. It should be noted that a "fit and proper" person test will be introduced in respect of MSB operators under the Third EU Money Laundering Directive.

968. *Business addresses*: the addresses of all principals and all agents are retained by HMRC as part of the registration regime. HMRC has the power to compel the production of such information (cf section 3.10)

969. *Accounts & awareness*: HMRC can compel production of account information (cf section 3.10); also it is judged that awareness amongst financial institutions of the registration regime is good, thus rendering it difficult for MSBs to gain access to the mainstream financial system without a registration number. See section 3.10, Recommendation 17.

3.11.2 Recommendations and Comments

970. MVT service providers are "MSBs" in the UK; they are registered and supervised by the HMRC for AML/CFT regulation. However, the size of this sector poses a challenge to the HMRC to effectively supervise all the money value transfer services. The UK authorities indicate that the supervisory system will be strengthened as part of implementing the Third Money Laundering Directive. It is recommended to increase the resources of the HMRC as well as its powers of sanction to enhance the supervision of MSBs. UK authorities should increase available sanctions, such as considering higher financial penalties, and the ability to sanction directors and senior managers.

3.11.3 Compliance with Special Recommendation VI

	Rating	Summary of factors underlying rating
SR.VI	**LC**	• Minor concerns about the effectiveness of the sector's supervision. • There are not adequate sanctions that can be used against directors and senior managers. • There are some concerns with regard to the extent that certain Recommendations apply: customer identification such as a lack of beneficial ownership requirements (R.5), PEPs (R. 6), and transaction monitoring (R.11, 21).

4. Preventative Measures – Designated Non-Financial Businesses and Professions

Basic legal obligations

971. All categories of DNFBP as defined by the methodology are found in the UK, and all categories of DNFBP are subject to the legal obligations imposed by the Money Laundering Regulations 2003 ("MLRs"), POCA and TACT. MLRs Regulation 2 (2) (f) - (n) sets out the scope of "regulated businesses" other than financial institutions obligated to comply with AML/CFT controls:

> "(2) For the purposes of these Regulations, "relevant business" means -
> …
> (f) estate agency work;
> (g) operating a casino by way of business;
> (h) the activities of a person appointed to act as an insolvency practitioner within the meaning of section 388 of the Insolvency Act 1986[17] or Article 3 of the Insolvency (Northern Ireland) Order 1989[18];
> (i) the provision by way of business of advice about the tax affairs of another person by a body corporate or unincorporate or, in the case of a sole practitioner, by an individual;
> (j) the provision by way of business of accountancy services by a body corporate or unincorporate or, in the case of a sole practitioner, by an individual;
> (k) the provision by way of business of audit services by a person who is eligible for appointment as a company auditor under section 25 of the Companies Act 1989[19] or Article 28 of the Companies (Northern Ireland) Order 1990[20];
> (l) the provision by way of business of legal services by a body corporate or unincorporate or, in the case of a sole practitioner, by an individual and which involves participation in a financial or real property transaction (whether by assisting in the planning or execution of any such transaction or otherwise by acting for, or on behalf of, a client in any such transaction);
> (m) the provision by way of business of services in relation to the formation, operation or management of a company or a trust; or
> (n) the activity of dealing in goods of any description by way of business (including dealing as an auctioneer) whenever a transaction involves accepting a total cash payment of 15,000 euro or more"

972. The principal money laundering offences in the POCA (Sections 327-329) apply to DNFBPs in the same way as to any other natural or legal person. As part of the regulated sector, DNFBPs are also therefore bound by the POCA provisions in relation to: failure to disclose (Sections 330-332 POCA); tipping off (Section 333 POCA); and prejudicing an investigation (part 8 POCA).

973. Similarly, they are obligated to report suspicions and comply with related provisions under Sections 15-23 of the Terrorism Act 2000 (TACT). For full detail on the obligations imposed under the MLRs refer to Section 3 above; and for full details of the obligations imposed by POCA and TACT refer to Section 2 above.

974. Unlike the financial sector, the DNFBP sector has no single piece of enforceable guidance akin to the JMLSG guidance to factor into its compliance programmes. Many of the regulators and trade bodies active in the DNFBP sector however do produce their own specific guidance that, in the case of businesses or professions supervised by statutory regulators or SROs, could result in disciplinary action if it is not adhered to. SAR data compiled by SOCA suggests that SARs are being submitted to the UK FIU even by those areas of DNFBP that are not currently supervised for compliance and / or that have no access to sector-specific guidance (cf criterion 16.1 below).

975. Under the Third Money Laundering Directive, the UK will be obligated to ensure that those sectors of DNFBP that are not currently explicitly or comprehensively supervised for AML/CFT are

so supervised from December 2007 onwards. At the time of the on-site visit, proposals were out for public consultation suggesting that:

- real estate agents should be supervised by the Office for Fair Trading (a statutory regulator);
- accountants and tax advisers that are not members of a professional body should be supervised by HMRC; and
- trust and company services providers, who are not regulated by the FSA or through membership of a professional body should be supervised by HMRC

DNFBPs & authorised activities under FSMA

976. In the UK, some DNFBPs undertake FSMA-regulated activities (*managing of client money, securities or other assets*) and therefore need to be authorised by the FSA. For a full description of what constitutes authorised business, please refer to section 3 above. Just as for authorised financial institutions, this means that the FSA has a regulatory function to fulfil. For example, just over 650 professional firms (mainly accountants and solicitors) are *directly authorised* and regulated by the FSA to carry out FSMA regulated activities. As a result, the FSA Handbook, including its AML rules, will apply to these firms as it does to other FSA authorised financial institutions.

977. FSMA, Part XX allows members of designated professional bodies (DPBs) to carry on a *limited range* of activities defined under FSMA without needing to be authorised by the FSA. For these firms, the relevant DPB is responsible for regulating all aspects of the professional firm's business, including the FSMA regulated activity covered by this exemption. There are ten DPBs covering four main professions. The FSA Handbook, including its AML rules does not apply to professional firms that fall into this second category of professional firms that offer limited activities under FSMA. Instead such firms will be subject to the monitoring arrangements and AML rules of their relevant DPB.

978. However, the FSA retains an oversight role in relation to the FSMA regulated activities offered by such firms. FSMA, Part XX, section 325(3) requires the FSA to be informed of the FSMA regulated activity of professional firms exempt from FSA authorisation and to keep under review the desirability of using powers to restrict that business. Part XX, section 325(4) requires the DPBs to co-operate with the FSA. Furthermore, in accordance with Part XX section 332(3), DPBs are required to make rules covering FSMA regulated activities, in particular to ensure that they are ancillary or complementary to the professional services provided. Section 332(5) of FSMA requires DPBs to seek the FSA's approval of these rules. There are approximately 16,500 firms undertaking FSMA regulated activity in a limited capacity: these are categorised by the FSA as "Exempt Professional Firms" (EPF).

4.1 Customer due diligence and record-keeping (R.12)

Recommendation 12
(applying R.5, 6, 8-11)

4.1.1 Description and Analysis

Applying Recommendation 5

979. All categories of DNFBP fall under the description of "relevant business" as per MLRs Regulation 2(2) quoted above. Thus they are required to adhere to all aspects of the MLRs relevant to this recommendation (Regulations 4, 5, and 6). Regulation 4 requires CDD:

"4. (1) In this regulation and in regulations 5 to 7 -
(a) "A" means a person who carries on relevant business in the United Kingdom; and
(b) "B" means an applicant for business.

(2) This regulation applies if -

(a) A and B form, or agree to form, a business relationship;

(b) in respect of any one-off transaction -

(i) A knows or suspects that the transaction involves money laundering[30]; or

(ii) payment of 15,000 euro or more is to be made by or to B; or

(c) in respect of two or more one-off transactions, it appears to A (whether at the outset or subsequently) that the transactions are linked and involve, in total, the payment of 15,000 euro or more by or to B.

(3) A must maintain identification procedures which -

(a) require that as soon as is reasonably practicable after contact is first made between A and B -

(i) B must produce satisfactory evidence of his identity; or

(ii) such measures specified in the procedures must be taken in order to produce satisfactory evidence of B's identity;

(b) take into account the greater potential for money laundering which arises when B is not physically present when being identified;

(c) require that where satisfactory evidence of identity is not obtained, the business relationship or one-off transaction must not proceed any further; and

(d) require that where B acts or appears to act for another person, reasonable measures must be taken for the purpose of establishing the identity of that person."

Casinos

980. CDD requirements for casinos are more stringent than for other DNFBPs: MLRs Regulation 8 explicitly requires that casino operators obtain satisfactory evidence of identity of any person before allowing that person to use the casino's facilities. MLRs Regulation 4 also applies, so where it is possible to enter into transactions at a casino that do not relate to gaming facilities, CDD will be applied. This includes one-off transactions involving 15,000 euros or more. The Gambling Commission has ensured that CDD required under MLRs Regulation 4 is referred to in its guidance There is no explicit requirement in the MLRs for casinos to conduct CDD for transactions over 3,000 euros. The assessors have some concerns about the effectiveness of processes to link identification on entry to CDD processes for transactions in a casino, although UK authorities claim that generic monitoring of customers for commercial purposes achieves this outcome in practice.

981. The Gambling Commission has issued guidance entitled: "Guidance to the Operators of Casinos for the Purposes of Preventing and Detecting Money Laundering". The Gambling Commission considers failure to adhere to these guidelines to be cause for regulatory intervention. The guidance covers the following areas: knowing your customer; recording identification; retention of identification records; recording transactions; retention of transaction records; reporting systems for suspicious activity; identifying suspicious transactions; training and compliance; and confidentiality. As well as highlighting the importance of the legal obligations, the guidance sets out suggested identification measures, such as the use and retention of photographs of customers (Part 2 of the guidance).

Real Estate Agents

982. Estate agents would need to conduct CDD if and when they establish business relations, conduct a one-off transaction above 15,000 euros, or where money laundering or terrorist financing is suspected. The CDD requirements require that the agent check the ID of the *seller*, but not that of the buyer of real estate, which creates a loophole in the regulatory framework for these professionals which is compounded by the fact that real estate may be purchased in cash. UK authorities indicate that while property may be purchased in cash, estate agents do not usually handle client money.

[30] The definition of "money laundering" in the MLRs includes terrorist financing.

Property transactions usually involve other parts of the regulated sector, such as solicitor or licensed conveyancer, who will also have obligations to conduct CDD for the various participants, thus capturing both buyer and seller. There are currently no comprehensive instructions or requirements in place for real estate agents beyond the legal requirements in the MLRs. The Royal Institute of Chartered Surveyors (RICS) produces guidance and news bulletins on AML/CFT legislation and developments for its members on its website has worked with trade body the National Association of Estate Agents to produce "protecting against money laundering: a guide for members": http://www.rics.org/Management/Businessmanagement/Financialmanagement/Accounting/Moneylaundering/rics+view+-+money+laundering.htm. RICS and NAEA members account for 75% of the estate agents operating in the UK.

983. The guidance produced by RICS includes sector-specific guidance on customer due diligence, including guidance on CDD in relation to different sectors such as companies, trusts, and charities. The guidance for example suggests specific procedures as regards electronic checks. The guidance also recommends that estate agents identify the buyers as well as the sellers, even if they are not the firm's customer

Dealers in precious metals & dealers in precious stones

984. Both of these categories fall into the wider category applicable in the UK, that of "high value dealers" (HVDs), which is adequately covered under the regulations by requiring CDD when conducting any one-off transaction over 15,000 euros. The current HVD register shows that there are 49 HVDs registered in the "jewellery" category and 23 registered as "jewellery wholesale."

Figures as of 30th June 2006 – The HVD register

BUSINESS TYPE	REGISTERED PRINCIPALS	NUMBER OF PREMISES	PERCENTAGE PREMISES
High Value Dealer (HVD)	1055	1834	98%
HVD/CC	4	4	0.2%
HVD/CC/BdC	0	0	0%
HVD/CC/BdC/MT	11	15	0.8%
HVD/MT	9	9	0.4%
HVD/BdC	2	2	0.1%
HVD/BdC/MT	5	5	0.2%
TOTAL	**1086**	**1869**	**100%**

985. HMRC also produced sector-specific guidance ("Anti money laundering guide for High Value Dealers" - HMRC document *"MLR 7: Anti Money Laundering Guide for HVDs"*) that explains and supplements the requirements of the MLRs. It includes a section on customer due diligence (MLR 7 part 9). MLR 7, paragraph 9.3 states: "You must check and retain evidence of everyone in the chain. This includes when your customer is, or appears to be acting on behalf of someone else". In addition, MLR 7, paragraph 9.8 states: "You must satisfy yourself that you obtain acceptable evidence of ID. Because there is no single form of official ID in the UK, you should obtain a range of separate types and cross-refer them to confirm they are consistent".

Lawyers, notaries, other independent legal professionals & accountants

986. The MLRs covers lawyers in the circumstances described in Recommendation 12—i.e., when in involved in the buying and selling of real estate, managing of client money, securities or other assets; management of bank, savings or securities accounts, organisation of contributions for the creation, operation or management of companies, and the creation, operation or management of legal persons or arrangements, and buying and selling of business entities. In order to practice, solicitors must be members of the relevant professional body. Thus, in addition to the legal obligations, solicitors are informed in their CDD activity by guidance produced by their professional body.

987. The guidance produced by the Law Society of England and Wales (LSEW) (available for free on the internet – www.moneylaundering.lawsociety.org.uk) sets out the general rationale for AML compliance requirements, namely: to enable suspicious transactions to be recognised and reported to the authorities; and to ensure that the audit trail is available if a solicitor, client or other party to a transaction becomes the subject of an investigation. The guidance also sets out (chapter 3) the need for Solicitors to obtain 'satisfactory evidence' of the identity of each client (and where the client is acting as agent to take reasonable measures to establish the identity of the underlying principal). The guidance encourages solicitors to be aware of clients who are "smurfing" payments in order to avoid identity checks: such activity is recommended as grounds for a suspicious activity report. The guidance also recommends that solicitors must take evidence of identity even where clients are introduced by partners or other staff members.

988. The guidance advises solicitors to look at actual documentary evidence such as passports and certificates of incorporation issued by Companies House, or make electronic checks of suitable databases such as the FSA Register, the Law Society database of practicing solicitors and the electoral register (and to print and retain a copy of the evidence with their records).

989. There is special guidance for solicitors covering identification and verification of identity for individuals not resident in the UK; and situations where it is not possible to meet the client. Guidance is also provided in relation to trusts, estates, employee and pension trusts and corporate clients (chapter 3 of guidance). The guidance encourages solicitors to be alert to certain warning signs of money laundering and a "Warning Card" is included as part of the guidance, that sets out signs such as unusual settlement instructions, or unusual instructions and transactions involving suspect territories.

990. The Law Society of Scotland (LSS) has made the requirement to comply with the MLRs part of its professional conduct rules, and has extended the requirement to all practices and all their business as if it were 'relevant business' under the legislation. The LSS guidance (available for free on the internet (www.lawscot.org.uk) reflects this situation. It sets out the range of CDD required for individuals and corporate clients, and suggests types of evidence that might be sought (section 3 of the guidance).

991. The Bar Council England & Wales (BCEW) produces guidance that requires barristers to comply with the customer due diligence requirements (guidance available on the internet at www.barcouncil.org.uk). Guidance produced by the Bar Council Northern Ireland is modelled on and mirrors this guidance.

992. The Law Society guidance (either E&W or Scotland) applies for the majority of notaries as they are either solicitors themselves or work in solicitors' firms. Additional guidance by trade bodies has been put into circulation in draft form. In addition some there are a number of notaries that are not solicitors. The professional body for these is the Faculty Office of the Archbishop of Canterbury. Industry guidance notes have been prepared by the relevant industry bodies – the Society of Scrivener Notaries and the Notaries Society. This has been approved by the Treasury and so if a Notary follows it, this must be taken account of by a Court in deciding whether offences have taken place.

Licensed conveyancers

993. Statutory regulator the "Council for Licensed Conveyancers" (the CLC) has produced guidance specific to these specialist property lawyers. The overview of CDD requirements for conveyancers in Section 1, paragraph 6 of that guidance states that: "The level of identity check exceeds that currently required for a mortgage transaction [under conveyancing rules] and applies to both sale and purchase transactions and whether or not a mortgage is involved. If a client fails to provide satisfactory evidence of identity a report must be made. Firms must ensure that: the prospective client is the person that he or she claims to be; a person of that name lives at the address given; a company had identifiable owners and controllers; and its representatives can be located at the address provided.

994. In Part 4 of Section 2 of the guidance, paragraphs 2.C.40 – 2.C.73 explain in depth what CDD means in practice, including for example what kind of evidence of identity is acceptable. In Part 4 of Section 3 at paragraph 3.C.33, the guidance reminds licensed conveyancers that: "[MLRs] Regulation requires that, where satisfactory evidence of identity cannot be obtained, that business relationship or one-off transaction must not proceed any further."

Accountants

995. For accountants, the requirements in the UK go beyond the requirements of Recommendation 12.1(d), in that those providing accountancy, audit or tax advice are required to comply with the customer due diligence, record keeping and other requirements of the MLRs for all their business activities as accountants, auditors or tax advisers, not just those listed in that Recommendation. The requirements also apply to all those providing accountancy services by way of business, not just professionally qualified and regulated accountants.

996. In addition to the legal obligations, accountants are informed in their CDD activity by guidance produced by the Consultative Committee of Accountancy Bodies (CCAB). Though this Guidance has not yet been approved by the Treasury, it represents authoritative professional Guidance, which would be likely to inform the Courts, in any decision as to whether accountants have complied with the legislative and professional requirements. For members and member firms of the CCAB bodies, non-compliance would also represent a foundation for disciplinary action. The Guidance is freely available to all those providing accountancy services by way of business: http://www.ccab.org.uk/PDFs/Antimoneylaundering90304.pdf.

997. The guidance sets out the need for firms to be able to establish that new clients are who they claim to be, and advises on gathering "know your client" information, including the client's expected patterns of business, its business model and its source of funds. In formulating their approach, guidance is given that firms may wish to consider the risks attaching not only to different types of clients, but also different types of services. Based on these risk assessments, firms can determine the appropriate degree of information that may be required in respect of both "know your client" and identification evidence. For example, more extensive procedures may be appropriate for offshore trusts in high-risk jurisdictions.

Trust & Company Service Providers (TCSPs)

998. Trust and company service providers are subject to the ML regulations through Regulation 2 (2)(m) when conducting the activities listed under recommendation 12 and when commencing a business relationship, conducting a one-off transaction over 15,00 euros, or when suspecting money laundering or terrorist financing.

Applying Recommendation 6

999. For financial institutions, the JMLSG has issued useful guidance on dealing with politically exposed PEPs. However, there are requirements with regard to PEPs that will apply to any of the DNFBPs. This will change with the implementation of the 3rd EU Money Laundering Directive.

1000. In respect of Recommendation 6, the CLC guidance states (Section 3, paragraphs 3.B.32 – 3.B.35):

> "The proceeds of … corruption are often transferred to other jurisdictions…and invested in assets such as real estate…risks can be reduced by conducting detailed KYC procedures at the outset of a relationship and on an on-going basis where firms know, suspect, or are advised that the business relationship that they are about to create is being formed with a senior political figure"

Applying Recommendation 8

1001. Under MLRs Regulations (3)(1)(b) DNFBPs should have in place effective systems and controls to mitigate the ML/TF risks faced by their business. While for financial institutions this is expanded upon in the FSA handbook and JMLSG guidance, this is not the case for DNFBPs. For DNFBPs, there is no obligation to have policies in place or take such measures as may be necessary to prevent the misuse of technological developments in ML/FT. (For financial institutions, this obligation is generally covered in the FSA Handbook, which refer to "development of new products" etc.)

1002. DNFBPs are required to have measures in place to deal with non-face to face business and transactions. MLRs Regulation 4(3)(b) indicates that: "A [the DNFBP] must maintain identification procedures which…take into account the greater potential for money laundering which arises when B [the customer] is not physically present when being identified…"

Applying Recommendation 9

1003. For DNFBPs, there are currently no enforceable obligations with regard to introduced business.

Applying Recommendation 10

1004. Record-keeping procedures apply all DNFBPs. In general, records of CDD and transactions should be kept for at least five years. Although there is no requirement that records should be sufficient to permit reconstruction of individual transactions so as to provide, if necessary, evidence for prosecution of criminal activity (this obligation is generally covered for financial institutions through the FSA Handbook and JMLSG guidance.) There is no explicit requirement in law or regulation to maintain records of account files (for financial institutions this requirement is in the FSA Rules).

Casinos

1005. For casinos, Gambling Commission Guidance also recommends that casinos keep transaction records in relation to cash transactions, cheques, bank drafts, and deposits (Part 5 of the Guidance). The guidance also states that transaction records must be retained for at least 5 years from the date of the transaction (part 6 of the guidance); this also applies to identification records, which must be retained for 5 years "beyond the last occasion a person was permitted entry to a gaming facility" (part 4 of the guidance).

Solicitors: England, Wales, and Northern Ireland

1006. Guidance for England & Wales (applied by Northern Ireland) requires solicitors' firms to establish procedures for the retention of the following records: (a) a copy of the evidence of identity obtained, or information as to where a copy of that evidence may be obtained, or where neither of these are reasonably practicable, information enabling the evidence of identity to be re-obtained; and (b) details of each transaction carried out in the course of relevant business.

1007. The guidance recommends that firms keep central records of evidence of identity as a precaution against the inadvertent early destruction of files and to make it easier for staff to refer back to the evidence obtained. See Chapter 3 of the guidance. A specific warning is given about the greater risk posed by Politically Exposed Persons (chapter 6, paragraph 6.34 of the guidance).

Solicitors: Scotland

1008. Law Society Scotland guidance includes (section 3) advice on ID checks involving clients from a range of backgrounds, including "clients at a distance": "if client abroad, use a local notary or British Consulate and obtain an affidavit – not just a letter – from that person". It also advises on ID checks in

relation to clients referred by another solicitor, a mortgage broker, an estate agent, bank, or building society; and in situations involving the receipt of funds from a third party. It does not embellish upon the legal obligation in respect of record keeping.

Barristers/Advocates

1009. Guidance by the Bar Council England & Wales suggests that barristers should comply with the record-keeping requirements as follows. (Guidance applied by the Bar Council for Northern Ireland is also modelled on this guidance):

- As regards evidence of client identity, if a barrister has obtained this himself, he must retain the records for 5 years (*see paragraph 55 of the Guidance*)
- If the barrister has asked an instructing professional to certify that customer due diligence checks have been carried out:
    - (i) the barrister will ask the instructing professional to certify that the instructing professional has proper record-keeping measures in place to comply with Regulation 6 of the Money Laundering Regulations 2003: with the result that the barrister can subsequently request the instructing professional to produce the evidence of client identity if the need to do so arises (*see paragraph 54 of the Guidance*);
    - (ii) barristers in Northern Ireland will apply the same approach as in (i) above, but in addition are required to retain the *certification* for 5 years.

- As regards evidence of the transaction itself, if a barrister has been instructed by another regulated professional, he will ask that professional to confirm in writing that the instructions and advice will be kept by the professional for the requisite period (*see paragraph 56 of the Guidance*). If the barrister has been instructed by a "direct access" client (i.e. not an instructing solicitor), the barrister will retain a copy of his instructions, his advice and a full fee note detailing all work carried out, for the requisite period (*see paragraph 57 of the Guidance*).
- Guidance produced by the Bar Council Northern Ireland recommends that Barristers in Northern Ireland should obtain a receipt for all paperwork returned to the instructing professional;
- The Faculty of Advocates would expect its members to comply with the same general approach as recommended by the Bar Council of England and Wales where the matters are not attended to by the solicitor.

Licensed Conveyancers

1010. The CLC guidance includes comprehensive detail on record keeping requirements in Part 8 of Section 2 at paragraphs 2.C.118 – 2.C.130. Overview text on record keeping at Section 1 paragraph 10 states that "Records of customer identification and KYC transaction assessments must be made and retained for use as evidence in any subsequent investigation into money laundering… Prudence suggests that they should also be capable of identifying all internal suspicion reports received and all external reports made".

Accountants

1011. The CCAB Guidance states that evidence of client identification needs to be maintained for five years after the termination of a client relationship by any part of the firm providing relevant business. Records of transactions also need to be maintained for five years, from the date when all activities in relation to the transaction were completed. Specific guidance is given, to the effect that firms need to ensure that records are not inadvertently destroyed by one department, where another is still within the five-year period or has embarked on a new business relationship with the client.

Applying Recommendation 11

1012. As above, all categories of DNFBP are bound by the legal obligations in MLRs Regulations 4 and 6, in respect of customer due diligence and record-keeping; and are also subject to the reporting arrangements set out in POCA (sections 330 – 331) and TACT (section 21A) that in practice will imply monitoring for suspicious activity. However, as with financial institutions, for DNFBPs there is no specific obligation to pay special attention to all complex, unusual large transactions, or unusual patterns of transactions, that have no apparent or visible economic or lawful purpose. There is no specific requirement to examine as far as possible the background and purpose of such transactions and to set forth findings in writing. DNFBPs are not required to keep such findings available for competent authorities and auditors for at least five years.

Dealers in precious metals & dealers in precious stones

1013. HMRC Guidance for HVDs (MLR 7) advises (paragraphs 9.12 –9.13): "… You should regularly review the relationship and consider reporting any suspicion. You must retain the account file or an equivalent record for five years after you stop dealing with the customer…you need not establish any additional records, provided your commercial files meet the requirements of the regulations and you are able to produce them when required to do so".

4.1.2 Recommendations and Comments

1014. All DNFBPs are bound by the legal obligation in MLRs regulations 4 and 6, in respect of customer due diligence and record keeping and are also subject to the reporting requirements set up in POCA and TACT. However, the concerns raised in the section related to the CDD requirements for financial institutions apply also to the DNFBPs. In many cases, the regulations are supplemented by comprehensive industry guidance from various DNFBP sectors. While the guidance is helpful, it is not mandatory to adhere to it, and cannot be considered as "other enforceable means".

1015. Therefore, there are several gaps in the regulatory framework for DNFBPs with respect to key elements of AML/CFT obligations; the UK should adopt adequate measures for R.6., 9, 11 for DNFBPs. The UK should also require that the estate agents identify the buyer of real estate. This is of particular importance in the UK as it is possible to acquire real estate in cash, which makes the real estate sector particularly vulnerable to money laundering. It has been explained to the assessors, that DNFPB must comply with the CDD measures set out in criteria 5.3 to 5.7 but they may determine the extent of such measure on a risk sensitive basis depending on the type of customer, business relationship or transaction. Similarly, the UK should adopt stronger CDD measures as described under Recommendation 5.

1016. CDD requirements for casinos are stronger than those for other DNFPB and they are obliged to identify every customer entering into a casino whatever the amount he/she will play, although there is no explicit obligation to identify the customer for individual transactions above EUR 3,000. UK authorities should ensure that CDD is linked to transactions above EUR 3,000 as there is a risk that relying on current ad hoc arrangements by casinos to link identification on the door with transactions undertaken inside the casino could potentially give rise to a situation in which it might not be possible to trace a particular transaction to a particular individual.

4.1.3 Compliance with Recommendation 12

	Rating	Summary of factors relevant to s.4.1 underlying overall rating
R.12	**PC**	• *Applying R.5:* Similar deficiencies as indicated under R.5 (no law or regulation to require CDD when there are doubts about the previously obtained data; no requirements to identify beneficial owner, etc.). Some CDD requirements are in guidance, which are not legally binding.

		• For casinos, CDD is not required above the 3,000 euro threshold, and it is not clear that casinos can adequately link the incoming customers to individual transactions. • Estate agents are not required to identify the buyer. • *Applying R.6:* No requirements with regard to PEPs that will apply to any of the DNFBPs. • *Applying R.8:* For DNFBPs, there is no obligation to have policies in place or take such measures as may be necessary to prevent the misuse of technological developments in ML/FT. • *Applying R. 9:* For DNFBPs, there are currently no enforceable obligations with regard to introduced business. • *Applying R.10:* Certain record-keeping requirements in the FSA rules and JMLSG Guidance do not apply to DNFBPs: no requirement that records must be sufficient to permit reconstruction of individual transactions so as to provide, if necessary, evidence for prosecution of criminal activity; no explicit requirement in law or regulation to maintain records of account files. • *Applying R.11*: For DNFBPs there is no specific obligation to pay special attention to all complex, unusual large transactions, or unusual patterns of transactions, that have no apparent or visible economic or lawful purpose. • There is no requirement to examine as far as possible the background and purpose of such transactions and to set forth findings in writing. • No requirement to keep such findings available for competent authorities and auditors for at least five years.

4.2 Monitoring transactions and other issues (R.16)

Recommendation 16 (applying R.13-15, & 21)

Applying Recommendations 13 and 14

1017. The reporting requirements that apply to financial institutions under MLRs Regulation 7 and the obligations to report suspicious activity under POCA Sections 330-331, and TACT 21A, apply to DNFBPs; as do the accompanying safe harbor from liability & tipping off provisions (Sections 333, and 337-338 of POCA and Section 21B of TACT). For a full description of these obligations, refer to section 3.7 above. The same criminal penalties also apply for failure to adhere to those obligations – refer to section 2.1 above.

1018. The guidance available for different categories of DNFBP in respect of their reporting obligations varies; as does the extent to which their compliance is directly monitored. In respect of reporting, however, the UK FIU maintains statistics on reporting by sector so is able to identify potential problems in terms of frequency of reporting against perceived risk in the sector. For example, Part 7 of the Gambling Commission guidance recaps the legal obligations under MLRs and POCA; and Part 8 attempts to provide indicative guidance on interpreting these obligations, for example an illustrative list of what might constitute suspicious activity in a casino is provided, which includes for example " players who buy in with large amounts of cash and after only minimal play where significant funds have not been at risk, seek the issue of a casino "win-cheque" for the remainder of the buy-in;" and "two or more players who in collusion play both sides of even chance bets at roulette or who bet on the player and the bank during the same coups in punto-banco."

1019. Guidance produced by Law Society England & Wales (chapters 6&7), Law Society Scotland (Section 9) and HMRC (MLR7 part 6) all also provide some degree of sector-specific advice on disclosures to the UK FIU.

Legal professional privilege

1020. The reporting obligations in the MLRs and POCA do not apply to a professional legal adviser or other relevant professional adviser (which includes accountants, auditors and tax advisors) where the information or other matter comes to him in privileged circumstances (see Regulation 7 (3) of the MLRs and section 330 of POCA). The circumstances where information is considered privileged are set out in MLR Regulations 7 (4) & (5) and section 330 (10) of POCA.

1021. Section 330 of POCA creates an offence of failing to disclose knowledge or suspicion that another person is engaged in money laundering. The offence can only be committed by a person in the "regulated sector". By section 330(6) (b) of POCA as amended by section 104(3) of the Serious Organised Crime and Police Act 2005, a person does not commit an offence under section 330(1)-(4) if he is "a professional legal adviser " (the phrase is not defined in the Act) and the information or matter came to him "in privileged circumstances". The phrase "privileged circumstances" is defined in section 330(10):

> "(10) Information or other matter comes to a professional legal adviser in privileged circumstances if it is communicated or given to him –
> (a) by (or by a representative of) a client of his in connection with the giving by the adviser of legal advice to the client,
> (b) by (or by a representative of) a person seeking legal advice from the adviser, or
> (c) by a person in connection with legal proceedings or contemplated legal proceedings."

1022. SOCPA 2005 Section106 (2) also amends section 330(9) POCA to ensure that a disclosure to a nominated officer by a legal professional for the purposes of seeking advice is not treated as a

disclosure under section 330(5)(a) (a possible interpretation of the unamended legislation affecting only professional legal advisers).

Bowman v Fels

1023. A crucial recent case has had another important effect for legal professional privilege. The judgment in *Bowman v. Fels[2005-EWCA civ226]* was concerned with the scope of s.328 of POCA, which creates the offence of facilitating money laundering. The Court's conclusion was that the provision by a lawyer of professional services to a client by way of advice and representation in the conduct and settlement of litigation could never mean that he was "concerned in an arrangement [for] … the acquisition, retention, use or control of … property". In other words, regardless of what suspicions or knowledge a lawyer might acquire in the course of acting professionally in litigation, he cannot commit an offence under s.328(1) while so acting, and as a result there is no need for him to make an authorised disclosure under s.328(2) in relation to any material obtained by him in the course of litigation.

Accountants

1024. The Government amended section 330 of POCA in 2006 to provide for the defence to the "failure to disclose" offence, which originally applied to professional legal advisers in certain circumstances, to be extended to include accountants, auditors and tax advisers who satisfy certain conditions. The amendment to POCA was made in POCA and the MLRs 2003 (Amendment) Order 2006 (SI 308/2006). The Order came into effect on 21 February 2006. The equal treatment between these professions applies only to the very limited extent that they are carrying out effectively the same functions in relation to legal advice. The exemption from the obligation to report money laundering to the appropriate authorities is therefore a narrow one which should only apply in specified and appropriate circumstances.

1025. The limited exemption from the requirement to report money laundering does not extend to all accountants, auditors and tax advisers. It applies only to those who are members of a professional body which requires a test of competence as a condition of membership and the maintenance of professional standards, including sanctions for non-compliance with those standards. The amendments to POCA made by the Order also provide a defence for a person who is employed by, or is in partnership with, a professional legal adviser or other relevant professional adviser, as defined in the Order.

1026. UK FIU statistics presented below show the levels of reporting by different sectors:

	2002	2003	2004	2005	2006
Casinos	590	516	525	724	520
Estate agents	7	5	104	209	129
High value dealers	288	309	179	366	196
Solicitors	615	3912	9710	10,654	7,296
Barristers	0	172	82	67	33
Accountants	155	692	7521	14,567	9,896
Company service providers	8	5	19	89	335

1027. The FIU has analysed the "reason for suspicion" field from a selection of casino disclosures received and has identified the following trends:

- Slightly over half of the selection related to suspicions about high buy-ins followed by minimal or no gaming and subsequent attempts to cash in chips;
- there are a number of SARs relating to unsuccessful attempts to exchange Scottish bank notes for other denominations; and

- about one tenth of the SARs related to active police investigations.

1028. Overall, the reporting obligation is comprehensive and appears effective. The various DNFBPs are well aware of their reporting obligations and seem to have effective systems in place to comply with them. The figures illustrate that only a small number of real estate agents file transactions report, although this number is increasing.

Applying Recommendation 15

1029. The general requirement in the MLRs Regulation 3 for relevant businesses to establish internal controls to forestall ML and to educate staff about ML / FT risks and obligations also applies to DNFBPs. However, while the Regulation stipulates the need for an internal reporting officer, there is no specific requirement to designate an AML/CFT compliance officer at the management level; (for financial institutions, this is specified in the FSA Handbook), nor are there any requirements for screening procedures.

Applying Recommendation 21

1030. There is no requirement for DNFBPs to give special attention to business with countries which do not sufficiently apply FATF Recommendations, nor is there a legal obligation to examine as far as possible the background and purpose of such transactions, and make written findings available for authorities. MLR 28 does cover the ability to apply counter-measures.

1031. Only the 650 FSA authorised firms in the DNFBP sector would be expected to review the JMLSG information on other jurisdictions described in section 3.6 above (as a direct consequence of their supervision by FSA). Other DNFBPs might also monitor this information, but are not supervised in such a way that obliges them to do so. Individual DNFBP sectors are thus dependent on: (1) outreach and advisory work by their regulators, SROs, and trade bodies; and by HMT and the UK FIU (as noted at section 3.6, criteria 21.1 and section 3.7 above, UK FIU outreach specifically addresses this issue when relevant); (2) the extent to which this issue is picked up in any sector-specific guidance available; and (3) obligations under the MLRs Regulation 28 if this power is utilised by HMT.

Additional elements

1032. The reporting requirement is extended to all the activities of accountants, auditors and tax advisors, by the Money Laundering Regulations 2003 paragraph 2 (2) (h) to (k), whether they are carried out by a member of a professional body, or by an unqualified accountant or tax advisor.

1033. DNFBPs are required to report to the FIU when they suspect or have reasonable grounds to suspect that funds are the proceeds of all criminal acts that would constitute a predicate offence for money laundering domestically.

4.2.2 Recommendations and Comments

1034. The obligations to report SARs related to ML and FATF are generally comprehensive for all DNFBPs; they are subject to the same regime and sanctions applying to financial institution. Measures to provide a safe harbor and to prohibit tipping off are also comprehensive. There are only limited areas where accountants are not obliged to report. The UK should strengthen the requirements for internal controls and for paying special attention to business and transactions involving jurisdictions that do not adequately apply the FATF Recommendations. These issues will be resolved through the implementation of the 3rd EU Money Laundering Directive.

4.2.3 Compliance with Recommendation 16

	Rating	Summary of factors relevant to s.4.2 underlying overall rating
R.16	**LC**	• There is no specific requirement to designate an AML/CFT compliance officer at the management level; nor are there any requirements for screening procedures. • There is no requirement for DNFBPs to give special attention to business with countries which do not sufficiently apply FATF Recommendations, nor is there a legal obligation to examine as far as possible the background and purpose of such transactions, and make written findings available for authorities.

4.3 Regulation, supervision and monitoring (R. 24-25)

4.3.1 Description and Analysis

Recommendation 24

Overview of DNFBP supervisors

Sub-sector of DNFBP	Supervised for AML/CFT compliance?	Supervisor?	Impact of Third Money Laundering Directive (December 2007)
High Value Dealers	Yes	HM Revenue & Customs (statutory regulator)	
Real Estate Agents	Not supervised at present; however professional body "RICS" encourages compliance amongst its members		Proposal that supervision for AML/CFT will be the responsibility of the Office of Fair Trading (statutory regulator)
Solicitors	Yes	Professional body SROs: *Law Society E&W* *Law Society NI* *Law Society Scotland*	
Barristers/Advocates	Yes	Professional body SROs: *Bar Council E&W* *Bar Council NI* *Faculty of Advocates (Scotland)*	
Licensed Conveyancers	Yes	Council of Licensed Conveyancers (statutory regulator)	
Notaries	No supervisor in England and Wales, but sector largely made up of solicitors and therefore subject to SRO supervision		Supervision required; it is proposed that the Faculty Office of the Archbishop of Canterbury take this on.
Accountants that are members of professional bodies	Yes	Significant numbers are regulated by their SRO professional bodies : *Institute of Chartered Accountants E&W; Institute of Chartered Accountants Scotland; Institute of Chartered Accountants NI; Association of Chartered Certified Accountants; Chartered Institute of Management Accountants; Chartered Institute of Public Finance and Accountancy; Institute of Actuaries* The regulation of these professionals is carried out under the oversight of the Professional Oversight Board (POB), an operating body of the Financial Reporting Council. The Financial Reporting Council (FRC) is the UK's independent regulator for corporate reporting and governance, a non-Statutory body, set up with Government support.	
Accountants and tax advisers *not* members of	There are a large number - potentially 40,000 – of unregulated accountants most of whom are not currently monitored for AML and CTF compliance, but will be under		Proposal that supervision for AML/CFT will be the responsibility of HMRC (statutory

professional bodies	the Third Money Laundering Directive: the proposal is for this role to be taken on by HMRC. Some trade bodies actively encourage compliance amongst their members	regulator)
Trust and Company Services Providers	If lawyers or accountants, will be regulated by SRO. Otherwise not supervised.	Proposal that supervision for AML/CFT will be the responsibility of HMRC (statutory regulator)

Casinos

1035. The supervisory framework for casinos is currently in transition. A regime was established under the Gaming Act 1968, which gave the "Gaming Board" authority to license, supervise, and sanction casinos for provisions of the Act. Under the new Gambling Act 2005, the previous authorities of the Board, with new strengthened supervisory capabilities, has being transferred to the "Gambling Commission." The Gambling Commission has already been established; other provisions of the Act are due to come into effect in September 2007.

1036. All casinos must be licensed under the Gaming Act 1968. Schedule 2 details these provisions for the Commission to grant a "certificate of consent", i.e. licensing requirements. Under current rules (the schedule refers only to "premises"), internet casinos are not licensed, and so they are illegal. When the new Act fully comes into effect in September 2007, it will provide the Commission with an additional responsibility to issue licences for remote gambling by such means as the internet, digital TV, and mobile phones. Numerous non-UK based internet gambling sites can be accessed in the UK: these are not subject to Gambling Commission regulation or supervision.

1037. One of the main objectives of the Gambling Commission (and the legislation it enforces) continues to be to ensure that high standards of probity exist amongst those involved in the gaming industry. An important part of this process is the "section 19" certificate of approval procedure (section 19 of the Gaming Act 1968), which is designed to ensure that those who work on the gaming floor and/or who manage such employees are fit and proper to act in that capacity.

1038. In general, legal or regulatory measures 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. The 1968 Act requires those who perform certain functions to hold a certificate of approval issued by the Commission, and gives the Commission power to require certain others performing managerial, organisational or supervisory duties to be certificated. A licence holder who employs staff in contravention of these procedures commits an offence under section 23(1) of the 1968 Act. It is Gambling Commission policy to make "fit & proper" checks or obtain reports from the appropriate authorities on *all* new applicants for certificates of approval. These same checks are also carried out on shareholders of casinos with 3% or more of stock. Under the Gambling Act 2005 (part 6) there will be two types of personal licences: licences which authorise an individual to perform the functions of a specified management office and licences which authorise an individual to perform a specified operational function.

1039. Local authorities (i.e. county/borough/ parish–based regional government) are responsible for licensing actual casino premises. The Gambling Commission can intervene in a local authority licensing hearing to request that a premises licence not be granted, if it has reason to do so: even where the Commission has already licensed the operator. The Commission is responsible for issuing guidance to local authorities on the manner in which they exercise their functions under the legislation, and the principles to be applied.

1040. The Gambling Commission is a regulatory body with powers of monitoring and sanction under the Gaming Act 1968 and from September 2007 the Gambling Act 2005. In accordance with its statutory objective to prevent the exploitation of gambling for financial crime, it is explicitly tasked with supervising casinos for compliance with the AML/CFT controls, including the legal obligations

under MLRs, POCA, and TACT, and the additional obligations imposed by its own guidance in this regard. It can apply its own regulatory sanctions if it determines that a casino has failed to apply sufficient AML/CFT controls; but for criminal prosecution under MLRs, POCA, or TACT, it refers cases to the police.

1041. The Gambling Act 2005 (Part 2) requires the Commission to issue one or more codes of practice about the manner in which facilities for gambling are provided (whether by the holder of a licence under the Gambling Act 2005 or by another person). The code should describe arrangements required for the purposes of: ensuring that gambling is conducted in a fair and open way, protecting children and other vulnerable persons from being harmed or exploited by gambling, and, making assistance available to persons who are or may be affected by problems relating to Gambling.

1042. Current sanctions available to the Commission include those that go against the licensing requirements and collusion of staff in illegal activities; warnings and financial penalties can be issued for these. In addition, the Commission may revoke a "certificate of consent" (i.e., the license to operate"). However, the possible sanctions available are limited and there is not a sufficient range of sanctions available for dealing with AML/CFT issues as required by FATF standards. Generally sanctions are warnings or revoking a license (by revoking a certificate of consent to operate or by revoking a certificate of suitability, or making a representation to the local authorities to revoke a premises license); a wider range of sanctions will be available under the new Act.

1043. The Gambling commission carries out on-site inspections. Under the current program, the average number of inspections is one visit per premises per month. From April 2006 to March 2007 there were a total of 1,688 inspections of 139 casinos.) Some casinos get inspected twice each month, some are inspected monthly, those viewed as lower risk premises are inspected every two months. Inspections include 20-30 checking 20-30 items, one of which is on AML. Each inspection generally lasts two hours. Items checked include SARs filed and the information behind them, and the records of individuals' transaction records.

Real estate agents

1044. Currently, there is no supervisory or monitoring framework for AML/CFT for estate agents. Until the new supervisory arrangements come into force under the Third Money Laundering Directive (December 2007), the gap is filled by professional and trade bodies providing guidance on a voluntary basis. The Royal Institute of Chartered Surveyors (RICS), the professional body with 123,00 individual members, produces guidance and news bulletins on AML/CFT legislation and developments for its members on its website. It has also worked with trade body the National Association of Estate Agents to produce guidance "Protecting against money laundering: a guide for members": http://www.rics.org/Management/Businessmanagement/Financialmanagement/Accounting/Moneylaundering/rics+view+-+money+laundering.htm.

1045. Members of RICS and NAEA undergo assessments of professional competence, and must sign a declaration indicating that they have not been convicted of any offence. However, up to 25% of real estate agents are not a member of either professional body. Currently, there are no licensing or registration requirements for real estate agents. The private sector confirmed the sector is vulnerable to money laundering, and the system would be better served with requirements for licensing, standards of integrity, and requirements for CDD relating to the buyer of real estate in addition to the seller.

1046. UK authorities explained that the real estate agents estate agents generally do not usually handle client money. Property transactions usually involve other parts of the regulated sector, such as solicitor or licensed conveyancer, who will also have obligations to conduct CDD for the various participants, thus capturing both buyer and seller. Nevertheless, the evaluation team viewed the real estate market as a high-risk sector, particularly the London real estate market, and the lack of supervision for estate agents is therefore a serious vulnerability.

High Value Dealers

1047. HMRC is the statutory supervisor of HVDs (MLRs Part III), including dealers in precious metals and stones. HMRC must maintain a register of traders (MLRs Regulation 10); and has powers under the MLRs to: require further information related to the registration (Reg 11); determine an application to register (Reg 12); cancel a registration (Reg 13) (*although this cannot be applied for AML/CFT breaches)*; set and charge fees (Reg 14); inspect premises (Reg 15(1)); inspect and copy records (Reg 15 (2) and (3)); where a Justice is satisfied that a regulatory offence may be being committed: obtain access orders for recorded information (Reg 16) and obtain a search warrant (Reg 19); impose civil penalties of up to £5,000 for regulatory breaches (Reg 20); and prosecute regulatory breaches (Reg 23). HMRC also issues warning letters.

1048. HMRC applies a similar model of supervision to HVDs as it does to MSBs (see section 3.10 above), with the exception that newly registered traders are not immediately visited but are contacted by phone. In the case of HVDs, on a risk-based approach, this lighter degree of supervision does not weigh as heavily as for MSBs. Staff resources for HVD supervision are shared with MSB supervision: (see 3.10.1 above on resources for HMRC). To ensure compliance with the MLRs, HMRC conducts assurance visits.

Number of HMRC assurance visits to HVDs	
Quarter	No. of visits
Q1 30/06/2005	220
Q2 30/09/2005	156
Q3 31/12/2005	115
Q4 31/03/2006	132
Q5 30/06/2006	23

Number of HMRC warning letters issued to HVDs	
Quarter	No. of letters
Q1 30/06/2005	98
Q2 30/09/2005	76
Q3 31/12/2005	21
Q4 31/03/2006	19
Q5 30/06/2006	4

Number of MLRs Reg 20 (financial) penalties issued to HVDs	
Quarter	No. of penalties
Q1 30/06/2005	0
Q2 30/09/2005	2
Q3 31/12/2005	2
Q4 31/03/2006	2
Q5 30/06/2006	1

1049. HMRC authorities indicated that as of December 2006, a total of 12 penalties had been issued, for a total value of £ 40,250. Seven of these cases involved the maximum penalty of £5,000. In most cases the penalty was applied for failure to take satisfactory evidence of ID. In other cases, penalties were levied for failure to operate appropriate internal controls and or retain adequate records. The HMRC had also issued 31 registration penalties, for a total value of £ 96,500. All registration penalties were levied for failure to register at the appropriate time.

Solicitors

1050. The framework for the professional conduct of solicitors in England and Wales derives from the Solicitors Act 1974, the Administration of Justice Act 1985 and the Courts and Legal Services Act 1990 and the basic principles of conduct in the common law and the guidance of the Law Society England and Wales.

Law Society England & Wales (LSEW)

1051. The LSEW is a supervisory authority in accordance with the Money Laundering Regulations. (Readers should note changes to the structure of the LSEW since the on-site visit, covered in more detail in Section 1.) The LSEW has a range of sanctions in place for material breaches of the professional conduct rules. These sanctions have always been part of the Law Society's regulatory powers and breaches of the Money Laundering Regulations are treated as a material breach of the professional conduct rules, more specifically by bringing the profession into disrepute. The LSEW has the power to impose administrative sanctions such as imposing conditions on a solicitor's practising certificate, intervening and taking control of a solicitor's practise, imposing fines and revoking a solicitor's practicing certificate (i.e. "striking off"). Direct disciplinary sanctions can be imposed through the Solicitors' Disciplinary Tribunal SDT. The LSEW also utilises administrative measures which can take the form of reports requiring a firm to improve an aspect of compliance.

1052. There are formal agreements in place between the LSEW and organisations such as the police, SOCA, HM Customs and Excise, the Office for the Immigration Commissions, the Council of Licensed Conveyancers, and the Legal Services Commission to share information prepared by the Law Society's Forensic Investigators.

1053. The LSEW comprises various business units, including Professional Ethics, the Practice Standards Unit ("PSU"), and Forensic Investigations which are all responsible for the regulation, supervision and monitoring of solicitors for AML/CFT compliance. The PSU monitors solicitors' compliance with practice rules, including reviewing firms' compliance with the Money Laundering Regulations in line with the LSEW's Guidance. The review of AML/CFT compliance is a component of a larger visit programme which monitors solicitors' compliance with professional practice rules. The PSU, through its visits, monitors client identification procedures, training of staff and the appointment of a Nominated Officer. The PSU visited 1300 firms in 2004. Firms that are found to have inadequate controls usually receive recommendations for improvement and the PSU may arrange a further visit to the firm, or make an internal referral to Forensic Investigations so that further action can be considered.

1054. Current practice of the LSEW means that statistics on disciplinary action are usually recorded as "acts of dishonesty and wrongdoing that bring the profession into disrepute" and not specifically as money laundering related. The LSEW has also intervened in, or prosecuted, 35 firms for involvement in "advanced fee fraud", which in some cases involved actual or suspected money laundering.

Law Society of Scotland (LSS)

1055. The LSS is the professional body and SRO for all solicitors in Scotland. It has a similar status and range of powers to the Law Society England and Wales, including the ability to apply administrative sanctions. Solicitors in Scotland are required to adhere to the Money Laundering Regulations as an explicit part of their professional conduct rules – a breach of these rules may result in a referral to the Scottish Solicitors Discipline Tribunal, which is independent of the Society and has the power to revoke a solicitor's practice certificate.

1056. The LSS is governed by a Council of 50 members. There are approximately 20 committees, which deal with all aspects of the Society's responsibilities and interests. The chief executive is supported by a deputy chief executive and nine directors who head up individual departments.

1057. The departments most involved in the relevant areas are:

- *Professional Practice*, which is staffed by three qualified solicitors who provide advice in relation to enquiries by the profession. Enquiries can range from what the requirements are,

how to apply them to a particular practical situation and how to respond to enquiries or orders from relevant authorities.

- *Guarantee Fund*, which carries out the monitoring function. The monitoring specifically covers AML/CFT compliance, as part of the Accounts Rules. Compliance with AML/CFT is part of a larger area of responsibility and there are no separate statistics specifically for money laundering issues.

1058. Twelve members of the team inspect solicitors' records on site on a two and a half year cycle. 500 firms are inspected each year. More frequent inspections are carried out where the initial inspection discloses lack of compliance or other matters of concern. 100 re-inspection visits are carried out each year, on average and 32 firms are interviewed. Approximately 8 firms a year are referred to the Scottish Solicitors Discipline Tribunal.

1059. The team has three office-based staff, including a chartered accountant and a qualified solicitor. The department provides advice and guidance as part of the on site visits and in response to enquiries from solicitors.

Law Society Northern Ireland (LSNI)

1060. The LSNI has statutory powers to discipline, educate, and control the solicitors' profession in Northern Ireland. It has powers to suspend practicing certificates, and intervene in solicitors' practices to take control of clients' monies and documents if there is a reasonable cause to believe that a solicitor has acted dishonestly (this would include a breach of the AML/CFT controls). Any solicitor convicted of a criminal offence of dishonesty or one otherwise bringing the profession into disrepute will be referred to the Disciplinary Tribunal, an independent Tribunal of the High Court. A failure to apply the guidance (LSEW guidance, applied by Law Society Northern Ireland) could also result in a referral to this tribunal – which has the power to revoke a solicitor's practicing certificate.

1061. The LSNI is a Committee-based organisation answering to an elected Council of 30 members. The Society's secretariat is headed by the Chief Executive who is a qualified solicitor, the Deputy Secretary and three Assistant Secretaries are also qualified solicitors, with other professional staff in the form of qualified librarians and chartered accountants. There is a proportionate amount of back office staff. The Society's regulatory functions are carried out on the basis of public interest.

1062. The committee structure comprises both regulatory and representational committees. Relevant regulatory committees are:

- The Professional Ethics and Guidance Committee, which oversees the work of the Society's monitoring team; deals with inter-professional complaints to include both complaints from solicitors about solicitors, where there is no client element, and from other professionals, e.g. barristers and doctors; deals with breaches of the Society's regulations; reviews instances of potential professional misconduct; controls interventions where there has been dishonesty or where clients' monies are in jeopardy; operates a "Compensation Fund"; and maintains the Society's Regulations in relation to professional practice;
- The Financial Services Committee, which interfaces with the Financial Services Authority in the Society's role as a DPB (see above) and also supervises the monitoring of Solicitor Insolvency Practitioners in Northern Ireland; and
- The Client Complaints Committee.

1063. The Society's monitoring officers carry out inspections of all practices in Northern Ireland on a rotational basis on 2 – 2½ year cycle for compliance with the Society's, Solicitors Accounts Regulations 1998, the Financial Services Regulations 2004 and the Anti Money Laundering procedures. Firms who have shown failure to comply with regulations receive return visits more frequently. Inspections include a check for compliance with the requirements of the Money Laundering Regulations, i.e. as regards client identification; staff training and record keeping.

Barristers/Advocates

1064. The practise of barristers (England and Wales and Northern Ireland) and advocates (Scotland) consists, for the larger part, of representing clients in contentious litigation. In addition barristers and advocates will occasionally provide legal opinions in relation to specific circumstances pertaining to a client. Barristers and advocates do not represent or advise clients in relation to investments, business or tax affairs, financial or real property transactions, or the formation, operation or management of companies or trusts. In addition barristers and advocates do not generally accept clients except by referral from a solicitor. As a result barristers and advocates do not receive, manage or deal with client funds directly. There is therefore a relatively low risk the services of a barrister or advocate may be abused for the purposes of money laundering or terrorist financing.

1065. The practise of barristers in England and Wales and Northern Ireland is supervised by the Bar Council England and Wales (BCEW) and the Bar Council Northern Ireland (BCNI), respectively, which would consider failure to comply with the provisions of the Money Laundering Regulations, the POCA, or the TACT to be professional misconduct. This is also likely to amount to professional misconduct for advocates in Scotland. Disciplinary sanctions available include the imposition of a fine and the withdrawal of the barrister's or advocate's practice certificate (more likely if the barrister or advocate in question was convicted of a criminal offence in relation to failure to implement AML/CFT controls).

1066. In England and Wales the disciplinary side of the BCEW's work is conducted by its Conduct Committee, which is made up of around 50 practicing barristers and 9 lay members. Its role is to examine complaints about the behaviour of barristers and to take disciplinary action where appropriate. It has a staff of 13 and a Complaints Commissioner, whose role is to conduct initial investigation of complaints by lay clients. The team is divided into two sections: the complaints handling section which supports the Commissioner in his initial investigations and comprises 2 senior caseworkers and support staff and the investigations team which acts as the prosecutor for particular disciplinary matters. The latter comprises two qualified barristers and a support team. The team responds to complaints and individual matters brought to its attention. There is at present no formal pro-active monitoring.

1067. In the BCNI allegations of breaches of the Code of Conduct are dealt with by the Professional Conduct Committee which determines whether a charge should be laid against a barrister. The process can be commenced by a complaint from anyone (a member of the public, Court Service, the profession or a Judge) or by the Professional Conduct Committee acting on its own initiative. The Professional Conduct Committee is chaired by the vice chairman for the time being of the Bar Council and comprises senior members of the profession together with lay members. Serious breaches of the Code of Conduct are dealt with by the Disciplinary Committee, which is usually chaired by a High Court Judge or a Lord Justice of Appeal. An appeal lies from the Disciplinary Committee to the Disciplinary Appeals Committee, which comprises three Benchers and one lay member. The Lord Chief Justice nominates the chairman, a Judge, usually of no less standing than a Lord Justice of Appeal. There is usually a High Court judge representing the Benchers and a senior member of the profession. All disciplinary hearings are public. The details of a finding of breach of the Code of Conduct are published on a notice board in the Bar Library and in the Great Hall of the Royal Courts of Justice.

1068. In Scotland the disciplinary and regulatory framework of the Faculty of Advocates is administered in terms of the Faculty of Advocates Disciplinary Rules 2005. Complaints may be made by any person, and in fact the Dean himself if a matter is brought to his attention which may constitute a breach of the Faculty's Guide to Conduct. The matter is then administered by two staff together with the Faculty's Office-Bearers and a complaint will be remitted to a Complaints Committee, made up of two senior legal members and two non-legal (lay) members. A complaint can also be remitted to the Faculty's Disciplinary Tribunal, chaired by a retired judge, and prosecuted by a specially

appointed Member of Faculty. There is provision within the rules for publication of decisions on professional misconduct and inadequate professional services, in the Faculty Register or elsewhere if appropriate.

Notaries

1069. "Notaries Public" are not commonly encountered (there are about 1,000 practicing in England and Wales). Most notaries are also solicitors and do their general legal work in that capacity and under the regulation of the various Law Societies. In Scotland, *all* notaries are regulated by the LSS. A few in England and Wales (the trade body the "Notaries Society" estimates about 70 in total) are not solicitors; these practice only as notaries.

1070. Many notaries do work for commercial firms engaged in international trade, and for private individuals. The most common tasks of notaries are:

- preparing and witnessing powers of attorney for use overseas;
- dealing with purchase or sale of land and property abroad;
- providing documents to deal with the administration of the estate of people who are abroad, or owning property abroad;
- authenticating personal documents and information for immigration or emigration purposes, or to apply to marry or to work abroad; and
- authenticating company and business documents and transactions.

1071. Notaries can also provide authentication and a secure record for almost any sort of transaction, document or event, as well as carry out commercial and property work (including conveyancing) and family and private client work (including wills, probate and the administration of estates). Qualification as a notary is regulated by the Faculty Office of the Archbishop of Canterbury under the direction of the Master of the Faculties. Notaries that are not currently solicitors (very few in number) are not currently supervised for compliance with AML/CFT controls in England and Wales.

Licensed conveyancers

1072. Licensed conveyancers offer conveyancing services i.e. the legal process involved in transferring buildings and/or land from one owner to another and dealing with the financial transactions. Licensed conveyancers are in effect specialist property lawyers. Like solicitors, licensed conveyancers can handle funds for their clients.

1073. The statutory registrar and regulator of licensed conveyancers is the Council for Licensed Conveyancers ("the CLC") which supervises its members for compliance with the relevant professional standards and for compliance with AML/CFT controls. Many licensed conveyancers are employed by solicitors' firms and fall within that regulatory regime; however there are approximately 230 firms or individuals which operate separately from solicitors and these are directly regulated by the CLC.

1074. The CLC undertakes monitoring visits to all firms within its jurisdiction for assessing compliance with all relevant professional standards including AML/CFT controls. While currently within the remit of its conveyancing inspectors and accounts inspectors (a team of nine), who are not AML/CFT specialists, it is proposed that it will in the near future deploy one specialist inspector dedicated to AML/CFT aspects of monitoring.

1075. The CLC's "Discipline and Appeals Committee" has statutory sanctions that include the power to levy fines on licensed conveyancers and the power to withdraw licences to operate; these sanctions can be applied in circumstances where the conveyancer has failed to abide by AML/CFT controls.

Accountants (members of accountancy and tax professional bodies)

1076. For the purposes of the ML Regulations 2003, the following bodies (the 4 accountancy supervisory bodies) are "supervisory authorities" under Regulation 2(7)(f)):

- The Institute of Chartered Accountants in England & Wales;
- The Institute of Chartered Accountants in Ireland;
- The Institute of Chartered Accountants of Scotland;
- The Association of Chartered Certified Accountants.

1077. Accountants who are not members of professional bodies (approximately 40,000) are not currently monitored for AML/CFT compliance. All the professional bodies have instituted monitoring and regulatory regimes, where their members participate in the "reserved areas" which are subject to Statutory regulation - which are audit, investment business and insolvency practice. In addition, they have all instituted procedures under which the full range of professional practice work undertaken by their members is subject to "practice review", a system of monitoring, which incorporates enquiry into their compliance with the AMF and CTF requirements. In the case of the Institute of Chartered Accountants in England and Wales, Practice Review entails monitoring visits which have been scheduled to cover all practicing firms on a rolling basis over a six year period, with more frequent visits for firms which are perceived as being high risk.

1078. In addition, there are a number of other professional bodies for accountants and tax advisers which monitor their members' compliance in terms of maintaining a complaints-based system, by which legislative, regulatory and professional requirements are enforced on their members. In particular, the two further CCAB bodies – the Chartered Institute of Management Accountants and the Chartered Institute of Public Finance and Accountancy – and the Chartered Institute of Taxation in addition to the four accountancy based supervisory authorities, have investigative and disciplinary systems. The term "Chartered" is a controlled term, granted only to professional bodies with laid down standards of competence, ethical requirements and disciplinary enforcement.

1079. Non-compliance with the AML and CFT requirements would represent grounds for disciplinary action ranging from informal challenge and reprimands, and increased monitoring activity, through formal public-record reprimand and fines, to expulsion. There are powers in relation to the taking of disciplinary action in all the accountancy related professional bodies. The bodies co-operate with the police, in investigating the activities of any member who is suspected of criminal activity.

1080. The technical and other resources available to accountancy professional bodies, to perform their AML and CTF activities vary between the various bodies, but provisions exist to ensure that they are adequate, in the form of oversight by the POB in the case of the CCAB bodies, and by the restrictions over the use of the term "Chartered" for the CCAB bodies and the Chartered Institute of Taxation.

1081. In the case of the largest of the bodies, the Institute of Chartered Accountants in England & Wales (the ICAEW) the disciplinary structure is supported by teams involved in assessment, conciliation and investigation. Disciplinary decisions are under the control of a tiered system of volunteer committees, with responsibility for investigation, discipline and appeal. All these committees have a membership made up of both senior members of the profession, and non-professionals, to ensure independence.

1082. In addition, in the reserved areas of audit, investment business and insolvency, licensing committees can withdraw permission for a firm or individual to operate in that area of practice on a lower standard of proof and on a shorter time frame than is required for formal disciplinary action.

1083. Monitoring activity carried out by the ICAEW is undertaken by members of its Quality Assurance Directorate. Monitoring visits are carried out experienced personnel, who are themselves members of the professional bodies for accountants, and who can therefore review activity from the basis of understanding and experience of professional activities and requirements.

Recommendation 25 (Guidance for DNFBPs other than guidance on STRs)

1084. Competent authorities have established guidelines to assist DNFBP to implement and comply with their respective AML/CFT requirements. For DNFBP, such guidelines have been issued by the relevant SROs or trade bodies. For more details on the contents of this guidance, refer to the discussions of these sectors under Recommendation 12, 16, and 24 above.

Casinos

1085. The Gambling Commission has issued guidelines for casinos on AML/CFT requirements.

Estate Agents

1086. The Royal Institute of Chartered Surveyors (RICS) produces guidance and news bulletins on AML/CFT legislation and developments for its members on its website has worked with trade body the National Association of Estate Agents to produce "protecting against money laundering: a guide for members": http://www.rics.org/Management/Businessmanagement/Financialmanagement/Accounting/Moneylaundering/rics+view+-+money+laundering.htm.

High Value Dealers

1087. HMRC also produced sector-specific guidance ("Anti money laundering guide for High Value Dealers" - HMRC document "MLR 7: Anti Money Laundering Guide for HVDs") that explains and supplements the requirements of the MLRs. Section 1.5 of the notice explains that ML "is the process by which criminally obtained money or other assets (criminal property) are exchanged for "clean" money or other assets with no obvious link to their criminal origins. It also covers money however come by that is used to fund terrorism."

1088. Specific ML threats and controls to identify and overcome them are included in section 13 of the notice. The threats include staff ignorance / apathy, transactions outside the normal range of activity and unrecorded transactions.

Solicitors

1089. The Money Laundering Guidance of the LSEW aims to provide a practical interpretation of the ML Regulations, the POCA and the TACT and to show firms how to develop policies and procedures appropriate to their own business. The LSNI utilises the guidance produced by the LSEW.

1090. The LSEW took a decision to issue the Guidance in a pilot version, with a view to seeking Treasury approval at a later date (likely to be in 2007). Until the Guidance is approved by HM Treasury the courts are not required to take it into account but may do so when assessing the behaviour of a solicitor.

1091. In addition to production of guidance, and in order to raise solicitors' awareness of money laundering and terrorist financing, the Law Society has applied resources towards communication and outreach with the profession in the following ways:

- Anti-Money Laundering road shows;
- The establishment of 11 regional groups for Money Laundering Reporting Officers ("MLROs");
- A dedicated anti-money laundering area of the Law Society's web-site (www.moneylaundering.lawsociety.org.uk);
- An online AML discussion forum for MLROs;

- A monthly e-newsletter that keeps solicitors up-to-date with key AML issues;
- Guidance to practitioners via the "Ethics Helpline".

Barristers/Advocates

1092. All barristers and advocates are subject to the Code of Conduct drawn up by the relevant professional body (BCEW, BCNI, and the Faculty of Advocates). All three also produce their own AML/CFT guidance. The guidance produced by the BCNI intentionally does not differ greatly in content from the guidance produced by the Bar Council for England and Wales.

Licensed Conveyancers Guidance

1093. The CLC produces both guidance and an interpretative "toolkit" for the sector that it regulates covering AML/CFT controls. The guidance supplements the legal provisions, by setting out for licensed conveyancers both their legal obligations and the explicit expectations of the CLC as regulator. The CLC has also produced a "toolkit" for regulated firms derived from the CLC's regulatory experience to date. The toolkit suggests mechanisms and standard paperwork that firms could implement or adapt to help them deliver on their AML/CFT obligations.

Accountants

1094. The CCAB Anti-Money Laundering Guidance aims to provide a practical interpretation of the requirements of ML Regulations 2003, the Proceeds of Crime Act 2002 and the Terrorism Act 2000 and to provide guidance on best practice in AML and CFT.

1095. The current Guidance is the "Second Interim Guidance for Accountants" with a third edition of the guidance currently under preparation. This version will be revised to take into account recent redevelopments in the law and practice, including the coming into force of the Third EU Money Laundering Directive. It is intended that Treasury approval will be sought, for the Third edition of the Guidance. Until then, the courts are not required to take it into account but may do so when assessing the behaviour of an accountant.

1096. In addition, less formal guidance is available from a number of professional and trade bodies for accountants, Guidance on the implications of new developments is available from the web site of the Institute of Chartered Accountants in England & Wales, on www.icaew.co.uk/moneylaundering. Guidance for auditors has been issued `by the Auditing Practices Board (the independent standard setting body for auditors, and an operating body of the Financial Reporting Council) and issued as Practice Note "PN 12 (Revised) Money laundering - Interim guidance for auditors in the United Kingdom". Guidance for insolvency practitioners has been issued by R3 (the Association of Business Recovery Professionals), also available from www.icaew.co.uk/moneylaundering. The Chartered Institute of Taxation provides Guidance for its members, which is available from: http://www.tax.org.uk/attach.pl/2299/1275/CIOTATT%20anti%20money%20laundering%20guidance%20FINAL1%20010304.pdf. In addition, many professional and trade bodies provide a wide range of informal guidance, published in periodicals, or off the public record.

Notaries

1097. The Notaries Society of England and Wales and the Society of Scrivener Notaries has also issued "Guidance for Notaries" to assist the sector to company with POCA, the MLRs, TACT. The guidelines provide an overview of the legal obligations and indicate situations in which a notary may be at risk of being used for money laundering. They give more specific guidance on identification procedures, internal reporting procedures, and training, and also answer a series of common questions such as those pertaining to identity verification, corporate clients, and client confidentiality/privilege. This guidance has been approved by Treasury which means that the Courts are required to take it into account.

Trust and company service providers

1098. The Association of Company Registration Agents (ACRA) issued "Guidance Notes on Money Laundering for Company Formation Agents" in July 2006. The Guidance sets out what is expected of firms and their staff in relation to the prevention and money laundering and terrorist financing, but allows them some discretion as to how they apply the requirements. The guidance explains the money laundering process, and gives guidance on such provisions as those relating to failure to report, tipping off, consent, training, and customer identification/verification procedures. The Guidance also sets out a list of what could be considered potentially suspicious activities and provides several case typologies.

4.3.2 Recommendations and Comments

1099. It is highly recommended that real estate agents be subject to adequate AML/CFT supervision, in particular in the context of implementing Third EU Money Laundering Directive. It is envisaged that the office of fair trading becomes the supervisor; adequate powers and resources should be provided to the OFT or other supervisor to fulfil this obligations, as there is no experience in AML supervision yet in this organisation. The UK should also ensure that trust and company service providers are subject to adequate AML/CFT supervision. Authorities should also bring the Gambling Act 2006 into full force so as to augment the range of sanctions available to the Gambling Commission.

1100. A significant number of accountants are regulated by their professional bodies but an estimated more than 40,000 do not adhere to any trade association. UK authorities should ensure that these accountants are also adequately supervised for AML/CFT.

1101. Only the HMRC is empowered to prosecute a breach of the MLRs, but other SROs for lawyers and accountants generally have disciplinary powers and can take sanctions for a breach of money laundering requirements. However, there are very few penalties pronounced by the HMRC, the general lack of statistics from the SROs on actual sanctions applies makes it difficult to evaluate the effectiveness of the sanctions.

1102. The supervision for the various kinds of lawyers in the UK is generally comprehensive. It is noted that a system for supervision of compliance by notaries public in England and Wales who are not also practicing as solicitors will be introduced further to the implementation of the EU Third Money Laundering Directive. The UK authorities are encouraged to continue with this process at a steady pace.

4.3.3 Compliance with Recommendations 24 & 25 (criteria 25.1, DNFBP)

	Rating	Summary of factors relevant to s.4.3 underlying overall rating
R.24	**PC**	• Currently no AML/CFT supervision for real estate agents or TCSPs that are not legal or accountancy professionals, or accountants that are not members of professional bodies (approximately 40,000). • Current sanctions for Gambling Commission are not yet adequate, although this will change once the Gambling Act comes into force in September 2007. • Notaries in England and Wales are not supervised for AML/CFT (unless they are also lawyers, or accountants that are members of professional bodies).
R.25	**C**	

4.4 Other non-financial businesses and professions (R.20)

4.4.1 Description and Analysis

Recommendation 20

1103. The UK applies Recommendations 5, 6, 8-11, 13-15, 17 and 21 to non-financial businesses and professions (other than DNFBP) that are at risk of being misused for money laundering or terrorist financing. The UK has taken the view that any high-value goods purchase that can be made in cash is a money laundering risk, and has therefore legislated accordingly. The scope of HVDs includes all businesses that accept cash of EUR 15,000 or more, irrespective of the goods involved. The current register includes 165 different trade categories; the largest of which is retail motor vehicle agencies. In order to reach affected businesses and therefore make the AML/CTF system more effective all UK VAT registered businesses were notified by post of the requirements to identify customers and to register with the supervisor, HMRC, before accepting high value cash payments.

1104. In addition to HVDs, the MLRs also cover investment advisors, tax advisors, and financial advisers that do not manage funds.

1105. Through its risk-based model and Threat Assessments, the UK encourages the development and use of modern and secure techniques for conducting financial transactions that are less vulnerable to money laundering. This kind of analysis by SOCA affects not only law enforcement response to particular threats but also the policy context. For example, SOCA research has suggested that compromised letting agents may be a source of money laundering risk in the UK. The FSA also issued guidance on the supervision of e-money for AML/CFT controls. Currently, the £50 note is the largest banknote issued in the UK.

4.4.2 Recommendations and Comments

1106. This recommendation is fully observed.

4.4.3 Compliance with Recommendation 20

	Rating	Summary of factors underlying rating
R.20	C	

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

Recommendation 33

1107. All limited companies in the UK are registered at Companies House, an Executive Agency of the Department of Trade and Industry. The main functions of Companies House are to:

- incorporate and dissolve limited companies;
- examine and store company information delivered under the Companies Act and related legislation; and
- make this information available to the public.

Companies Act companies

1108. Companies Act companies are established by registering certain documents prescribed under the Companies Act 1985 with the registrar of companies (there are separate registrars of companies for companies registered in England and Wales, Scotland and Northern Ireland). These documents include constitutional information about the company and details of those involved in its formation (notably its first directors and members). On registration, companies are given a "certificate of incorporation" and a unique identifying number.

1109. Companies Acts companies are owned and, ultimately, controlled by their members. A company's members are those persons whose names are entered on its register of members. The register of members is prima facie evidence of legal title. In the case of companies with a share capital, the members are those who own shares in the company, and in the case of companies limited by guarantee, those who give a member's guarantee. Private companies must have at least one director; public companies must have at least two. Day to day management of the company is usually delegated to the directors, who may in turn delegate to others. The precise balance of power between the directors and the members is generally a matter for the company's own constitution (in particular, its "articles of association"), which must be disclosed to the registrar of companies. In addition, the Companies Act 1985 gives members certain inalienable rights (such as the ability to remove directors from office). All Companies Act companies are required to have a registered office in the UK.

1110. A person who acquires shares becomes a shareholder on acquisition, but does not become a member until entry on the register of members. A share transfer must be registered as soon as practicable after the acquisition.. An exception to this exists under section 188 of the Companies Act, which permits the issue of share-warrants to bearer. This section provides that a company, if authorised by its articles, may issue with respect to fully paid shares a warrant stating the holder or bearer of the warrant is entitled to the shares specified in it. Title to the shares then passes manually by delivery of the warrant, which is a negotiable instrument. Upon issue, the company will remove from the register the name of the former registered owner and state the fact and date of issue of the warrants and the number of shares to which the warrant relates. The bearer of the warrant is regarded as a shareholder under law but may or may not be regarded as member of the company depending on the articles (shareholding and membership of a company are therefore not necessarily the same thing in the context of share-warrants to bearer). However, upon surrendering the warrants the holder or bearer is entitled to have his name and shareholding re-entered on the register of the company. The use of share-warrants to bearer is reportedly rare in the UK (see paragraphs 1140-1141.) The definition of "cash" in POCA extends to include them, however, for the purposes of cash seizure powers.

1111. Companies Act companies are required to disclose to the registrar of companies information in the following areas, amongst others.

- Their constitutional arrangements and capital structure (to be disclosed on formation and whenever there are subsequent alterations).
- Accounting information (annually), including in some cases information about directors' remuneration. The precise information to be disclosed and the level of detail / verification required varies depending on the size and type of company (e.g. public companies have to supply more information than private companies).
- Information about their directors (on formation, whenever any registrable particular of a director changes, whenever a person ceases to be a director, and when a new director is appointed (as well as part of the "annual return" to the registrar).
- Information about their members (on formation and annually, although companies limited by guarantee are not required to produce regular updates of their membership).
- Information about the company's registered office and the place where its register of members is kept (on formation, whenever it changes, and in the annual return). It must provide an active address (i.e. not a P.O. Box). If the registered address turns out to be inactive or non–responsive, Companies House can strike it off the register (section 652 of the Companies Act 1985). About 100,000 companies are struck off each year for failing to respond to Companies House requests for information.
- Information about security interests in the company's property (within a fixed period after the interest is taken).
- Companies must provide Companies House with a full list of shareholders (names, addresses, extent of shareholding) once every 3 years; and must alert Companies House to changes once every 12 months during the intervening period (section 364A of the Companies Act 1985).

1112. All Companies Act companies are required to keep an up to date register of the names and addresses of its members (section 352 of the 1985 Act, section 113 of the 2006 Act), which is to be kept available for inspection by the public. The register is to be kept (or at least made available) at the company's registered office or some other place in the part of the UK where it is registered (i.e. England and Wales, Scotland or Northern Ireland) which has been notified to the registrar of companies. If the company has a share capital, the register must include details of the shares held by each member. Companies must also keep registers of their directors (section 288 of the 1985 Act; section 162 of the 2006 Act). In UK law, anyone acting as a director who is not registered as such can still be considered to have fulfilled this function and be held accountable accordingly (section 744(1) and (2) of the 1985 Act). However, the evaluation team still had concerns regarding the possibility to use nominee shareholders who would appear on public record at the company registry instead of the real beneficial owner.

Other types of company

1113. Companies can also be formed by specific Act of Parliament, or by royal charter / letters patent, but these methods are hardly ever used now. Non-Companies Act companies, in broad terms, they follow a similar model with powers and responsibilities divided between members and directors (or other groups with different names but essentially similar functions). Non-Companies Act companies are required to notify the registrar of their principal office in the UK. Although such companies are not subject to registration on incorporation in the same way as Companies Act companies, they are subject to much the same regime of ongoing disclosure as regards as Companies Act companies.

Partnerships

1114. A "traditional" partnership can come into being without any legal formality, although most professional services partnerships, for example, will tend to set out their constitutional arrangements in

a partnership deed. Limited partnerships and limited liability partnerships (LLPs) are obliged to register prescribed information and documents with the registrar of companies on their formation.

1115. Partnerships are owned and controlled by the partners. The governance arrangements are largely a matter of internal agreement between them. LLPs are required to have a registered office in the UK. Limited partnerships are required to register details of their principal place of business.

1116. Limited partnerships must disclose to the registrar information about their names, the general nature of their business, their principal place of business, the partners' names, the term (if any) for which the partnership is entered into, and the sums contributed by the limited partners. This information is to be disclosed on registration and any subsequent changes in it.

1117. The disclosure requirements for LLPs are very similar to those for Companies Act companies. There are no equivalent requirements to disclose to a central authority in the case of "traditional" partnerships.

1118. "Traditional", limited and limited liability partnerships must disclose the names of all their partners in their business communications, unless they have more than 20 partners, in which case they may simply state an address in the UK where a list of the partners' names is available for inspection. Certain changes in the identity of the partners in a limited partnership must be published in the UK's official Gazettes.

UK-specific forms of body corporate (other than companies and partnerships)

1119. Friendly Societies, Industrial Provident Societies, and Building Societies have a range of applicable legislation under which they can become incorporated. All are entered onto registers maintained by the FSA. Basic registration documentation matching that required for companies is required. In addition, building societies (and friendly societies offering authorized business under FSMA) are directly regulated by the FSA as part of its mainstream financial regulation role.

1120. Building Societies, Friendly Societies and IPSs are all owned by shareholder members. Control is by directors elected by the members usually based on a principle of one-member one-vote regardless of shareholding. They all require a registered office in the UK.

1121. Building Societies, Friendly Societies and IPSs all retain the relevant certificates of registration issued by the registering authority. Members of the relevant societies have full access to these records and the documents are required to be retained at the registered offices.

Number and type of companies in the UK

Type	Number
Public companies	11,500
Private Companies	2,118,700 (of which 5,300 are unlimited)
Limited partnerships	13,426
Limited Liability Partnerships	17,499
Assurance companies	930
Industrial & Provident Societies	9,546
Incorporated by Royal Charter	798
Special Acts of Parliament	50
EEIGs	185
European Public Limited Liability Companies	1
Total Companies Act companies:	2,130,200

Reliance on investigative powers

1122. The UK's approach to preventing the unlawful use of legal persons and legal arrangements for ML and FT relies on the investigative and other powers of law enforcement, regulatory, supervisory, and other competent authorities to obtain or get access to information. Such information on beneficial ownership may be available from four sources:

- 'Open source' data;
- Information retained by AML/CFT regulated businesses as part of their compliance obligations;
- Information held by public bodies such as the companies' registrar or the tax authorities;
- Information held by private companies or individuals.

1123. Particular powers under POCA and SOCPA for use in money laundering and related investigations into the proceeds of crime are set out in section 2 (Recommendation 3) above. The use of such powers against businesses in the regulated sector may allow the financial investigator to gain access to beneficial ownership data maintained on a given company by that business, provided that beneficial ownership information is maintained there.

1124. Some of the POCA powers can be used directly on legal or natural persons (such as company directors). For example "production orders" (section 345 POCA) are frequently used to progress the investigation of money laundering offences. The UK authorities anticipate that Disclosure Notices obtained under SOCPA Section 62 will become increasingly important in situations where written records, held either by a business in the regulated sector or by the legal person in question, are incomplete or poorly kept.

1125. Apart from POCA and SOCPA, other relevant powers include: information gathering powers in Schedule 5 of TACT for terrorism / terrorist finance investigations; and the information gateway with the UK tax authorities under section 19 of ATCS, allowing the tax authorities to share information where it will support a criminal investigation: thus allowing law enforcement access to some aspects of tax filing information regarding companies and other legal persons.

1126. The standard timescale given for compliance with POCA Section 345 Production Orders is 7 days. This can vary according to the decision of the judge granting the order. Production Orders are court orders - failure to comply is an offence.

1127. However, the effectiveness of these powers depends upon the type and quality of information that is available and held either by the regulated sector or official records such as those held by the company registrar or otherwise. If these records are not up to date or accurate, or do not contain the details of the ultimate beneficial owner, then the investigator will need to continue with his inquiries by some other means. If the company director or member/shareholder has a foreign address or is resident abroad then the information will not necessarily be available in a timely manner and the ability to obtain the information will depend upon the effectiveness of mutual legal assistance or other forms of international cooperation.

'Open source' data

1128. With very few exceptions, all the information disclosed to the registrar of companies is available to the public. An example of information that is not so available is the home addresses of company directors whom the Secretary of State considers would be likely to be at serious risk of being subjected to violence or intimidation if their home addresses were available to the public.

1129. It is an offence to provide false or misleading information to the registrar, but the accuracy of beneficial ownership information (such as information about members) supplied to the registrar is not checked, which makes it a less reliable evidential source for law enforcement. UK law enforcement

practitioners relate that the information provides a valuable first step in the case of company investigation: in the case where a company is legitimate, the information is normally accurate, whereas in the case of a company which has been set up as a front, the information may not be accurate or indeed may be intentionally misleading. However, UK authorities indicate that this in itself provides law enforcement with a set of "next steps" in terms of leads and intelligence.

1130. The UK permits company directors to include non-natural persons (e.g. other companies) and foreign persons. The company registrar must be supplied with the name and address of each director but verification of this information is not a function of the company registrar. In practice, the director could be any intermediary acting on behalf of a third person. Any changes to directors and their details must be filed in the annual return for the company.

1131. Similarly, the company members/shareholders may be non-natural or foreign persons. Name and address must be supplied and kept up to date. There is no requirement to verify shareholder information.

1132. The UK authorities stated that they had considered the possibility of a system requiring up-front disclosure of beneficial ownership. Consultants were engaged in 2002 and a report produced. Public consultation on the report concluded that there were significant disadvantages and no clear benefits, particularly when taking into account the costs of introducing such measures. Reasons included:

- disclosure of beneficial ownership would add no information of benefit to the register of members. Those engaged in criminal activities would not provide true information about the beneficial owners;
- disclosure would result in misleading information being included on the register. Because beneficial ownership is, as a matter of law, impossible to define precisely, any information requirement designed to require by law disclosure would have to be complex and detailed. Many ordinary, innocent shareholders would be unable to understand it or comply with it.

1133. In the light of these points, it was concluded by the UK authorities that the existing register of members already provides investigators with as much as any disclosure regime can. The view was taken that attempting to add details of beneficial ownership to the existing register would be harmful to investigations through the resulting misleading information provided by both criminal and innocent shareholders.

Information retained by AML/CFT regulated businesses as part of their compliance obligations

1134. Regulated businesses should be retaining data on legal persons and legal arrangements which are their customers; however there is however no set standard for retention of beneficial ownership information. Section 3, criteria 5.5, above provides a detailed description of the obligations imposed on financial institutions to collect such information, and the kind of information to collect, as informed by the JMLSG Guidance. There is a more general obligation to collect such information that applies also to DNFBPs such as solicitors or accountants (as they are covered by the Money Laundering Regulations 2003 but not the JMLSG Guidance), but the nature of information collected will vary with the provisions of any relevant guidance and the firm's own risk assessment. Trust and company service providers are also subject to the Money Laundering Regulations; however, those that are not supervised by one of the legal or accountancy professional bodies are not subject to any supervisory or monitoring regime for their AML/CFT obligations and hence compliance with its CDD and other provisions is not verified. This will change with the implementation of the Third EU Money Laundering Directive; until then the CDD information held by TCSPs may not always be of the highest standards.

1135. Although there is no standardisation of beneficial ownership data held across the regulated sector, the information that is held (such as, for firms following the JMLSG guidance, the identity of beneficial owners holding 25% or more of shareholdings) does have some value to law enforcement

since it has been collected to satisfy particular customer due diligence objectives. To seek beneficial ownership information from a regulated business, the law enforcement agency in question would have to be in possession of some existing information or intelligence suggesting that the legal person in question was a customer of that regulated business.

Information held by public bodies such as the companies' registrar or the tax authorities

1136. Some information collected by the companies' registrar that may help establish beneficial ownership is not available to the public. For example: the home addresses of company directors whom the Secretary of State for Trade and Industry considers would be likely to be at serious risk of being subjected to violence or intimidation if their home addresses were available to the public (such as companies ostensibly involved in scientific research involving tests on animals). Archived items no longer available to the public are other files the disclosure of which would require direct contact with the registrar.

1137. Legal persons liable for corporation tax or other taxes are required by law to file tax returns with the tax authorities (HMRC). These filing requirements vary according to the type of legal person in question, but tend to include information useful to establishing beneficial ownership such as: loans to participants (shareholders or officers), company bank account or nominee bank account information, and supplementary material such as audited accounts. HMRC also has information gathering powers to acquire further data for the purposes of calculating tax liability where it has due cause to do so. Thus a given "file" might hold information additional to the contents of the tax return.

1138. HMRC officials may not disclose information they obtain in the course of carrying out their duties unless there is a lawful authority for that disclosure. There are various forms of lawful authority that permit disclosure to other competent authorities in the furtherance of HMRC's AML and CTF activities: one such is the Section 19 ATCS gateway mentioned above.

Information held by private companies or individuals

1139. Beneficial ownership information may be held by private companies or individuals. The reliability and scope of such information obviously varies enormously. Nevertheless, a law enforcement officer could obtain a production order where the person or company held information about a legal person subject to a money laundering investigation, or were themselves subject to such an investigation.

Share warrants to bearer

1140. See paragraph 1110 above for a description of issuing and functions of bearer share-warrants for Companies Act companies. The UK authorities have stated that the issue and use of share-warrants to bearer is rare and that they do not pose a risk in the context of financial crime. No special measures are in place to ensure they are not misused for money laundering purposes, although the UK has stated that, in the context of financial crime, the rarity of share-warrants to bearer has the effect that use of them by a company would likely attract the interest of the authorities. Academic commentary on the subject in the UK also states that "bearer securities have never been popular with English investors or companies and are rarely used" (Gower's Principles of Modern Company Law, 6th edition). (The description of cash in POCA extends to include bearer shares, so these could be seized on suspicion under powers outlined under section 2 above.)

1141. Private sector feedback confirmed that use of share-warrants to bearer was rare in the UK, although some instances had been encountered when clients would ask for them. For example, a non-UK national owing a yacht in the Mediterranean may register ownership of his yacht under a UK registered company thereby entitling the yacht to fly the UK flag. The shares in the company would issue to a particular person and then be exchanged for share-warrants to bearer. The yacht would not

attract the attention of the national authorities of the owner, who may not wish to openly display his wealth for tax purposes.

5.1.2 Recommendations and Comments

1142. The UK system for access to beneficial ownership and control information of legal persons basically relies upon investigatory powers available to law enforcement. The assessors have also considered the functions of the central company registration system. While the investigative powers are generally sound, the measures in place to ensure that there is adequate, accurate and timely information on the beneficial ownership and control of legal persons that can be obtained or accessed in a timely fashion by competent authorities should be improved. There is a requirement to provide director and shareholder information to the companies registrar and to keep it up to date, but this information is not verified and is not necessarily reliable. In addition, the use of nominee shareholders can hide the identity of the real beneficial owner. Also, it is possible for intermediaries and legal persons (such as other companies) to act as company directors and shareholders, and this means that the investigator must pursue a chain of persons or entities before reaching the ultimate beneficial owner. Should any of the entities or persons be registered or reside abroad, the investigator's task will be complicated by the time and need to make overseas inquiries.

1143. Although the use of share-warrants to the bearer is reportedly rare in the UK, these exist and no special measures are in place to ensure they are not misused for money laundering purposes beyond the provisions of POCA that include them under the definition of "cash" for the purposes of seizure. The provision has been replicated in the new Companies Act 2006 (in force in September 2006) despite its apparent rarity of use. The UK authorities should consider the justification and need for the on-going existence of bearer shares given the apparent lack of demand and potential risk of abuse.

1144. It is recommended that the UK authorities review the current system to determine ways in which adequate and accurate information on beneficial ownership may be available on a timely basis to law enforcement authorities.

1145. Some improvements to the current framework will come into force later in 2007. The new Companies Act 2006 has received Royal Assent, and the UK authorities will bring its provisions into force through statutory instruments by early 2008. Among the improvements will be the requirement that at least one director must be a natural person, requiring all former names and other names used in the course of business since the age of 16 for individuals who are directors, requiring a usual residential address and a service address and the country or state of residence rather than only the usual residential address of individuals who are directors (the service address will be on the public record, while the residential address will be available to enforcement authorities but not on the public record). Improvements in practice planned at Companies House will include (i) arrangements for suspicious activity reports to be submitted to SOCA and (ii) continuing increase in electronic filing where authorisation codes have greater reliability in identifying the source than do traditional signatures (more than 90% of companies are now incorporated electronically and total electronic filings have increased as a proportion from 24.4% to 34.9% year on year as at February 2007). UK authorities should implement the provisions of the new Companies Act as soon as possible and are encouraged to implement the planned changes in practice at Companies House.

1146. In addition, while company formation agents are currently subject to the MLRs 2003; UK authorities should bring company formation agents into an adequate AML/CFT compliance regime. This situation will be improved when the UK implements the 3rd EU Money Laundering Directive and designates a competent authority for supervising this sector.

5.1.3 Compliance with Recommendations 33

	Rating	Summary of factors underlying rating
R.33	PC	• While the investigative powers are generally sound, there are not adequate measures in place to ensure that there is adequate, accurate and timely information on the beneficial ownership and control of legal persons that can be obtained or accessed in a timely fashion by competent authorities. • Information on the companies registrar pertains only to legal ownership/control (as opposed to beneficial ownership) and is not verified and is not necessarily reliable. • Although the use of share warrants to the bearer is reportedly rare in the UK, there are no specific measures taken to ensure that they are not misused for money laundering other than the inclusion of "cash" in the POCA description.

5.2 Legal Arrangements – Access to beneficial ownership and control information (R.34)

5.2.1 Description and Analysis

1147. See section 1.4 of this report for a general description of trusts in the UK. It is not possible to establish trusts in such a way that the trustees have discretion to decide who the beneficiaries are, although with some trusts, particularly charitable trusts, the beneficiaries that fall within the class provided for may change over time (for example, disaster victims, or orphans, or victims of a certain illness or affliction). Equally, there may be some necessary discretion as to how the trustees might discharge their duties in respect of that class of beneficiary. However, it is not the case that the trustees of a trust can simply choose whomever they wish to be a beneficiary of a trust. Under English and Scottish law, certainty of beneficiaries is a requirement for the validity of a trust. They must be identified or at least identifiable, whether as individuals or as a class. Without that certainty, the trust is void.

1148. There is no central filing requirement for trusts and no register of all trusts in the UK, although some trusts are registered. All charitable trusts in England and Wales that meet the minimum requirements for registration must be registered with the Charity Commission and in Scotland with the Office of the Scottish Charity Regulator (at present there is no equivalent for Northern Ireland). The information filing arrangements for charities and the gateways between law enforcement and regulators is explored in more detail under 5.3 below. Unit trusts and other financial trusts to which the general public may subscribe are subject to financial licensing and regulation.

1149. A trustee must maintain accurate records of the trust property. They must allow a beneficiary, or his solicitor to inspect those accounts and the trustee must be prepared to give full information as to the value of the trust fund. If trust money is invested, the trustee must on request, supply a beneficiary with details of those investments. These obligations largely stem from the common law, although the investment activities of trustees are covered by different pieces of statute law in England & Wales, Northern Ireland, and Scotland.

Reliance on investigative powers

1150. The UK's approach to preventing the unlawful use of legal arrangements for ML and FT relies on the investigative and other powers of law enforcement, regulatory, supervisory, and other competent authorities to obtain or get access to beneficial ownership information. Such information is available from three sources:

- Information retained by AML/CFT regulated businesses as part of their compliance obligations;
- Information held by public bodies such as the tax authorities or charity regulators;
- Information held by private companies or individuals.

1151. The UK authorities state that an interdepartmental working group on trusts initiated in late 2001 found that "*current and prospective investigatory powers are generally considered by law enforcement and financial investigators to be adequate to probe the suspected criminal use of trusts*" – and that this view was current before the more extensive investigation tools in POCA 2002 were operational. (See the description of these investigative tools under section 5.1 above). The group also found that there was a desire from law enforcement that there should be a greater requirement on regulated businesses to retain more information on beneficial ownership of trusts: again, this pre-empted the obligations for CDD and record-keeping introduced by the MLRs 2003.

Information retained by AML/CFT regulated businesses as part of their compliance obligations

1152. See section 5.1 (paragraphs 1134 to 1135) above. DNFBPs such as lawyers, who often provide trust services, are monitored for AML obligations by the various relevant SROs. However, providers of trusts services that do not fall under an SRO are not subject to any monitoring system and therefore compliance with their AML obligations is not be verified.

Information held by public bodies such as the tax authorities

1153. Trusts, other than bare trusts, liable for taxes are required by law to file tax returns with the tax authorities (Her Majesty's Revenue and Customs—HMRC). Trusts with income of less than £1000 (formerly £500 up to 2005/06) do not normally need to file annually where the income is already taxed at source. Where filing requirements do apply, they vary according to the type of trust in question, but tend to include information useful to establishing beneficial ownership such as: details of any settlors who have put assets or funds into the trust, names of beneficiaries of discretionary payments, details of non-resident trusts that have made funds available to the UK-based trust, bank account arrangements for the trust, and details of new and retired trustees or their representatives. The tax return for individuals also includes a question on receipt of funds from or transfer of funds to a trust (since it has relevance for capital gains tax calculations). HMRC also has information gathering powers to acquire further data for the purposes of calculating tax liability where it has due cause to do so. Thus a given "file" might hold information additional to the contents of the tax return.

1154. The tax return will include trustee information, frequently a lawyer or accountant, and will provide name and address. It is possible for the trustee to reside abroad. HMRC can ask for a copy of the trust deed to establish the bona fides of the beneficiaries under the trust.

1155. HMRC officials may not disclose information they obtain in the course of carrying out their duties unless there is a lawful authority for that disclosure. There are various forms of lawful authority that permit disclosure to other competent authorities in the furtherance of HMRC's AML/CFT activities: one such is the Section 19 ATCS gateway mentioned above.

Information held by private companies or individuals

1156. Beneficial ownership information may be held by private companies or individuals, but the reliability and scope of such information obviously varies enormously. Nevertheless, a law enforcement officer could obtain a production order where the person or company held information about a legal arrangement subject to a money laundering investigation, or where a natural person was himself the subject of such an investigation in his capacity as a trustee.

5.2.2 Recommendations and Comments

1157. The UK system for access to beneficial ownership and control information of legal persons including trusts relies upon investigatory powers available to law enforcement, which are generally sound. However, in the case of trusts, the information available is, in many cases, minimal with respect to beneficial ownership, making it difficult for authorities to access adequate, timely, and accurate information on beneficial ownership in all situations. Trusts liable for taxes are required to file tax returns with HMRC, but the filing requirements vary according to they type of trust in question.

1158. Regulated businesses (including providers of trusts, as they are subject to the Money Laundering Regulations 2003) should be retaining information on their clients, including trust arrangements, and this information will be available to law enforcement by means of investigatory powers. However, there is no standardisation of beneficial ownership data held, and the nature of information collected will vary with the provision of any relevant guidance and the firm's own assessment risk. Also, providers of trust services who are not lawyers, or accountants that are members of professional bodies are not monitored for their AML/CFT obligations and so it is not clear how reliable the information they regularly maintain would be.

1159. The UK 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.

5.2.3 Compliance with Recommendations 34

	Rating	Summary of factors underlying rating
R.34	**PC**	• While the investigative powers are generally sound, there are not adequate measures in place to ensure that there is adequate, accurate and timely information on the beneficial ownership and control of legal arrangements that can be obtained or accessed in a timely fashion by competent authorities. • There is no standardisation of beneficial ownership data held, and the nature of information collected will vary with the provision of any relevant guidance. • Providers of trust services who are not lawyers, or accountants that are members of professional bodies, are not monitored for their AML/CFT obligations and so it is not clear how reliable the information they maintain would be.

5.3 Non-profit organisations (SR.VIII)

5.3.1 Description and Analysis

Overview of the sector and reviews

1160. The UK has a well established and diverse non-profit sector, thought in its widest sense to encompass up to 600,000 organisations with an annual income of around £72bn. These non-profit organisations can be loosely broken down into a variety of sub-sectors with a variety of bodies tasked with the oversight and/or regulation of their work: charities; social enterprises; campaigning, political, self-help groups, etc; community-based mutual organisations with social objectives. The smallest community-based organisations that are charitable but are beneath the statutory threshold for registration are not directly regulated but are however subject to the powers of the charity regulators.

1161. For England and Wales, there are just under 200,000 charities registered with the Charity Commission, and subject to its regulation. The total income of the sector to June 2006 was almost £38bn. 600 large charities control in the region of 47% of sector income. The assets of the sector are estimated at around £70bn, spread more evenly across the sector. There are about 40,000 NPOs in Scotland, of which 22,000 are charities regulated by Office of the Scottish Charity Regulator (OSCR) (founded in 2003). The income of the NPO sector is estimated in the region of £2.1bn p.a.

1162. There are approximately 9,000 charities in Northern Ireland; the large majority are small community-based groups. Annual income for the financial year 2000-2001 was estimated as £660 million. (There is currently no dedicated charity regulator or registrar in Northern Ireland. This is however subject to change and draft charities legislation for Northern Ireland will, if approved, introduce a charities regulator for Northern Ireland with a similar remit and set of aims as the Charity Commission.)

1163. The "charity" sector in the UK is the most significant aspect of the NPO sector by value and by profile, encompassing trusts with charitable objectives, many religious and faith-based organisations and internationally active aid organisations, amongst others. Most organisations in the UK that raise and distribute funds for social or humanitarian purposes are likely to fall within the definition of "charity". The most well known form of NPO in the UK is the "registered charity" based on a defined set of legal definitions enshrined in a combination of UK statute and UK case law. As a result, the main focus of NPO regulation in the UK is the charity sector, which accounts for the largest single share of all NPO income.

1164. The UK authorities commenced a review in correlation to SRVIII of the charitable sector and its vulnerability for terrorist fundraising during 2006. The review was still continuing at the time of the on-site visit. The results of the review were due to be subjected to a consultation period commencing January 2007. It is envisaged that the review will result in recommendations to be submitted to Ministers once the consultation process is finalised. Since the review was not yet finalised, the findings and recommendations were not available at the time of the on-site visit. However, the UK authorities indicated that early recommendations at a strategic level would include greater involvement, on a formalised basis, of charities regulators in disrupting any abuse of the charity sector for terrorist purposes as in training and skills transfer exercises with police and other regulators. These recommendations would also include enhancements to the duties of charities to alert the authorities of any suspicions of abuse.

1165. In addition to the abovementioned review, a comprehensive review of the sector was undertaken in England and Wales in 2002. As a result, charity law in England and Wales is currently undergoing a process of update and revision which resulted in a new Charities Act 2006. It received royal assent on 6 November 2006; however, its provisions must still be brought into force through separate statutory instruments. The changes that will act to strengthen regulation of the charitable sector as regards AML/CFT in England and Wales are as follows:

- All excepted charities (currently not subject to the regulation of the Charity Commission) will be required to register with the principal regulator as well exempt charities with an income above £ 100,000;
- The Charity Commission will be given extended powers to enter premises;
- Creation of a new type of legal entity called a "Charitable Incorporated Organisation";
- Unification of system for regulating public charitable collections, as opposed to current localised system.

1166. A recent review of the system of regulation of charities in Scotland resulted in the establishment of the Office of the Scottish Charities Regulator (OSCR); the work of this office will be reviewed in due course against a specified set of performance indicators.

1167. Draft legislation proposes the establishment of a charities regulator for Northern Ireland working along the same lines as the Charity Commission. It is expected that a plans for the establishment of this body will be made in early 2007.

Registration

1168. Charity law in England and Wales and Scotland impose a registration obligation on organisations that meet the definition of being charitable which means that the sector under regulation in these jurisdictions is not self-selecting. Regulation and supervision of the charity sector is undertaken by the Charity Commission of England and Wales ("the Charity Commission") in England and Wales and the Office of the Scottish Charities Regulator ("the OSCR") in Scotland. Draft legislation in Northern Ireland will provide, if approved, for the establishment of a charities regulator for Northern Ireland, working along the same lines as the Charity Commission.

1169. In England & Wales, charities with an annual income above £1,000 are required to register with the Charity Commission. (This will increase to £5,000 with the Charities Act 2006.) When prospective organisations apply to register as a charity in England & Wales they will be required to submit: a completed application form, a trustee declaration form, a copy of its governing document; and when required, disclosures of criminal records for all or some of the trustees.

1170. The Register of Charities is publicly available, and the Charity Commission also publishes a searchable internet version of the Register at the following address: http://www.charitycommission.gov.uk/registeredcharities/first.asp. In Scotland all charities are required to register with the OSCR. The Scottish Charity Register is also publicly available and can be searched via the internet at the following address: http://www.oscr.org.uk/TheRegister.stm. Draft charities legislation contains provisions on registration by Northern Ireland charities with a Charity Commission for Northern Ireland.

Outreach to the sector

1171. The charities regulators of both England & Wales and Scotland push for a high media profile and supplement this with an extensive outreach programme via website, media, publications and conferences and use this to raise awareness of a range of regulatory issues, such as: financial crime, the importance of good governance and financial management, and best practice for working internationally, amongst others.

1172. The Charity Commission provides advice and guidance to charities on compliance with charity law in order to minimise the potential for inadvertent non-compliance. As a result, the Commission produces numerous freely available publications on legal compliance and good practice, and policies on charities and terrorism and charities operating internationally. The Commission has also carried out an extensive programme of outreach to religious charities from a large number of faiths, including

those that may be vulnerable to the financing of terrorist according to the current perceived terrorist threat.

1173. A key objective of the charities regulators of England & Wales and Scotland is to promote public confidence in charities through effective regulation and to promote transparency in the charitable sector. The regulation of the sector by the regulators in England & Wales and Scotland contributes significantly towards minimising the potential for money laundering or terrorist financing to take place through charities.

Information on objectives, ownership, and control, and administration/management

1174. A charity in England & Wales or Scotland must have a governing document at the point of registration. This must set out the charity's objectives and the identity of the persons, such as trustees or directors, who govern its activities. The regulatory requirements imposed on charities, including the statutory duty to prepare and submit annual returns, ensure that charities must maintain basic records including changes to trustees / directors, and income and expenditure. Charities are legally obliged to supply a copy of their accounts to a member of the public, on request. In England and Wales, the Charity Commission's register of charities contains files of management and account information that are accessible to the public. Therefore, for England, Wales and Scotland, full access to information on the administration and management of a particular NPO may be obtained.

Transaction and accounting records

1175. Charities in England & Wales are required to formulate accurate accounts, with disclosure levels appropriate to their level of income and expenditure, and keep these accounting records for a period of 6 years. Charities in England and Wales are required by statute to submit financial information to the Charity Commission on an annual basis. Where a charity's income or expenditure is over £10,000 per year, these accounting records as well as an annual return must be submitted to the Charity Commission not later than 10 months after the charity's financial year-end. Information contained on the Annual Return is published on the Charity Commission's website and as of 2005 copies of accounts are available to download online.

1176. The accounting records of charities with a gross annual income or total annual expenditure exceeding £100,000 must be audited. The accounting records of charities with a gross annual income or total annual expenditure less than £100,000 must either be audited or examined by an independent examiner. In addition to this the Charity Commission may institute inquiries into the matters of charities, in accordance with its supervisory function and may call for any documents and search the records of a charity.

1177. Smaller charities are only required to fill out an Annual Return, which requires for example a full list of trustees and information on income and expenditure. The Charity Commission launched an "Accounts aren't Optional" campaign in 2004. This campaign sought to increase compliance with accounting and reporting requirements in charities both by raising awareness of the requirements and by "naming and shaming" persistent defaulters.

1178. From April 2006 all charities registered with OSCR have been required to submit appropriate Financial Statements with their Annual Returns. Details from these documents are added to the publicly available online register and it is noted if submission are overdue. In addition to this a Monitoring Return is issued to charities with an income of over £25,000. This Monitoring Return requires increasing amounts of information from charities with an income level between £25,000 and £100,000, then between £100,000 and £1,000,000, and above.

1179. Charities in Scotland are also required to keep accounting recording for a period of 6 years. These records are subject to audit or independent examination, depending on a charity's income and

other factors. In addition the OSCR has wide powers, in accordance with its supervisory function, to obtain access documents, including accounts of charities.

Powers to investigate and sanction

1180. The Charity Commission has extensive legal powers to allow it sanction wrongdoing or mismanagement in charities or anything purporting to be a charity in England and Wales. These powers include the ability to freeze bank accounts, to suspend and remove trustees and to remove charities from the register. Inquiry reports are published at: http://www.charitycommission.gov.uk/investigations/inquiryreports/inqreps.asp. The Commission also has extensive investigative powers such as the ability to require individuals to attend to answer questions and the ability to require the production of information from individuals and entities such as banks. All such powers are established in the Charities Act 1993. In addition to this the Commission has extensive links with the law enforcement sector and the ability to refer cases of suspected criminality to these agencies for criminal investigation. This would include all instances of money laundering and terrorist financing uncovered through its routine regulatory activities as well as through the use of specific investigative powers.

1181. In Scotland the powers of the OSCR include the suspension of persons from management or control, ability to direct a charity or other body not to take the action that is the cause of concern or in the most extreme cases to take formal action seeking orders against a body into which the OSCR is permitted to make inquiry or those in management or control. The orders sought may include the removal of persons concerned from management or control. Formal directions and suspensions made by the OSCR will be included on Scottish Charity Register against the charity to which they refer. The Charities and Trustee Investment (Scotland) Act 2005 allows the OSCR to investigate charities and other bodies such as those controlled by a charity or charities or any that represent themselves as charities while not on the Register. The inquiry may be made either generally or for a particular purpose.

1182. As indicated above in England and Wales the Charity Commission may require the production of information from individuals, such as trustees of a charity, and entities such as banks and also has the ability to require individuals to attend meetings with the Commission to answer questions. In Scotland the OSCR has powers of enquiry extending not only to charities, but bodies controlled by charities and those which represent themselves as a charity and to relevant individuals and organisations.

1183. In addition to this the investigating authorities, including the Police Service of Northern Ireland (which is currently charged with investigating concerns relating to criminality in charities in Northern Ireland), have the usual array of police powers (including the investigative powers contained in the POCA such as Production Orders).

1184. The Charity Commission conducts 400 targeted "Review Visits" each year to review compliance with the Charities Act 1993. These are normally based on information submitted in the annual returns and accounts as well as other concerns the Charity Commission might identify itself.

Domestic and international co-operation

1185. Both the Charity Commission and the OSCR have statutory duties to exchange information with appropriate authorities. Both organisations also have wide information sharing gateways to allow substantial information exchange between the regulators and law enforcement or other authorities. In addition to this the Charity Commission has a dedicated secondee to the National Terrorist Financial Investigation Unit (NTFIU) based at the Metropolitan Police to facilitate informed information sharing regarding charities and allegations of terrorist financing. The Commission is also a member of government policy forum TFAG.

1186. Relating specifically to the investigation of terrorism, section 17 of the Anti-terrorism, Crime and Security Act 2001 extends existing gateways for information sharing between public authorities, including charity regulators, where such existing information sharing gateways in legislation were not originally created to authorise information sharing for the purpose of criminal investigations.

1187. As mentioned above the Charity Commission has a dedicated secondee to the NTFIU based at the Metropolitan Police to facilitate informed information sharing regarding charities and allegations of terrorist financing. The NTFIU has officers dedicated to the investigation of NPOs with alleged or suspected links to the financing of terrorism and has developed a significant level of expertise in this area.

1188. In Scotland the OSCR has well-established links for sharing information with the Charity Commission and the Crown Office for Scotland. In Northern Ireland, the Department for Social Development, the HMRC, and the Police Service of Northern Ireland have good links for sharing information or making referrals in respect of terrorist financing concerns affecting charities.

1189. The charity regulators do not maintain any specific resource to handle international operational liaison. The UK authorities rely on the close links between both regulators and law enforcement, and in particular between the Charity Commission and the NTFIU, as well as the high level of transparency of information on charities, to ensure that existing arrangements for international intelligence and evidence gathering applicable to law enforcement described in Section 6 would be sufficient to capture any required charity sector information.

5.3.2 Recommendations and Comments

1190. While England and Wales and Scotland have well-established systems for the regulation of charities with adequate provision for the registration, transparency, supervision and investigation of charities, the same does not currently apply to Northern Ireland. Authorities should therefore develop appropriate procedures for registration, transparency, supervision and investigation of charities in Northern Ireland as soon as possible. As indicated above, this issue is due to be addressed by draft legislation which had not yet been enacted at the time of the on-site visit. The charities regulators for England and Wales and Scotland appear to be adequately resourced in order to carry out their functions in terms of their governing legislation and also to provide adequate support to the work of law enforcement authorities in relation to terrorism and terrorist financing investigations. During the on-site visit, the UK authorities indicated that the same model will also be applied in relation to the charity regulator for Northern Ireland, once the relevant legislation is enacted and this office is due to be constituted.

5.3.3 Compliance with Special Recommendation VIII

	Rating	Summary of factors underlying rating
SR.VIII	**LC**	• Northern Ireland not covered relating to registration, transparency and supervision of charities.

6. National and International Co-Operation

6.1 National co-operation and coordination (R.31 & 32)

6.1.1 Description and Analysis

Recommendation 31

1191. In general internal cooperation and coordination between UK policy makers, the FIU, law enforcement and supervisors and other competent authorities is effective. There also appears to be effective co-operation amongst agencies on an operational level.

1192. The UK also benefits from an effective network of interdepartmental and interagency contact and co-operation both for policy and for operational matters. A number of important interagency groupings meet regularly to tackle AML /CFT issues at the policy and operational levels.

Policy development fora

1193. Policy formulation on AML measures is developed through engagement with all interested parties in the **Money Laundering Advisory Committee" (MLAC**). MLAC is a forum for central government, law enforcement, supervisors, and the private sector that is jointly chaired by Home Office/HMT and meets periodically throughout the year to discuss how the regime is functioning and to inform advice to Ministers. For examples of recent MLAC activity, see: http://www.hm-treasury.gov.uk/documents/financial_services/money/fin_money_index.cfm.

1194. The **Terrorist Finance Action Group (TFAG)** is a cross-Whitehall committee that forms part of the wider Whitehall framework on counter-terrorism. It is focused on the development of policy to combat terrorist financing, and brings together representatives from central government, regulators, intelligence, and law enforcement. TFAG is chaired solely by HMT, which leads policy on CFT in government (the Home Office leads on counter-terrorism more generally).

1195. MLAC and TFAG allow for policy initiatives at all levels – including changes to international rules and best practice - to be collected, discussed, and shaped into a coherent whole in order to inform advice to Ministers.

Co-operative operational groups

1196. The **Asset Freezing Working Group (AFWG)** is chaired by HMT and agrees the handling of individual asset freezing cases as well as the architecture of the UK's asset freezing regime. The AFWG was set up by the Chancellor of the Exchequer in 2005 to improve cross-government co-ordination and enhance the operational effectiveness of the UK's asset freezing regime. It comprises: HMT (who lead on domestic designations and have overall ownership of the UK's asset freezing regime), FCO (who lead on UN and EU designations), The Home Office (who lead on the Government's wider counter-terrorism agenda), The BoE (who act as the Treasury's agent in administering financial sanctions), Law enforcement and intelligence agencies. The Group has been successful in improving co-ordination across different agencies and has resulted in a more proactive and effective consideration of cases. This has been demonstrated recently by the: rapid freezing of the assets of the individuals suspected of carrying out the attempted London tube bombings on 21 July 2005; the domestic designations on 11 August 2006 of 19 individuals arrested in connection with a suspected terror plot to blow up airplanes in mid-air; and the freezing action against UK-based members of the Libyan Islamic Fighting Group designated at the UN in February 2006.

1197. The **Concerted Inter-agency Criminal Finances Action group (CICFA)** has been operational for five years. It brings together central government, regulators, and the agencies responsible for

tackling acquisitive financial crime. The group's purpose is to drive forward concerted action to ensure that maximum operational advantage is taken of relevant POCA provisions by making asset recovery a mainstream activity within member agencies; it also seeks to achieve consistency in how these powers are used. Its ultimate aim is to reduce the harm done by crime and increase the value of recovered criminal proceeds. An example of the culture of collective learning present across the law enforcement / regulatory AML/CFT community is the monthly Money Laundering newsletter produced by the CIFCA Secretariat drawing on input from all members and the wider AML/CFT community. It is published on the ARA website: http://www.assetsrecovery.gov.uk/MediaCentre/MoneyLaunderingNews/. As of April 2007, CICFA will become known as the Assets Recovery Working Group.

1198. **Financial Investigators Working Group (FIWG).** At the FIWG, UK financial investigators regularly meet at both national and regional level (Financial Investigators Working Group - FIWG) to discuss best practice in techniques and trends.

1199. The **Organised Crime Task Force (OCTF)** in Northern Ireland, chaired by the Security Minister, provides a framework to bring together all the key agencies involved in the fight against organised crime.

1200. The **Financial Crime Information Network (FIN-NET)** (Formerly known as the Financial Fraud Information Network, FFIN) is a forum for intelligence-sharing on financial crime issues including money laundering and terrorist financing, with more than 10 years of credibility behind it. Currently made up of representatives from central government, law enforcement, and regulatory bodies; but there is potential that private sector trade associations with pseudo-regulatory functions (e.g. private sector anti-fraud initiatives) might be admitted as members.

1201. Set out below are overviews of other co-operative measures deployed by hubs in the AML/CFT regulatory environment to facilitate interaction between the different actors in the UK system

SOCA & UK FIU

1202. The UK FIU within SOCA facilitates regular dialogue between law enforcement end users and other stakeholders of the SARs regime to ensure that there is constructive communication and input into policy development and into developing and publicising best practice and guidance. Controls on confidentiality of data and gateways are as described under sections 2 & 3 above. The UK FIU facilitates a quarterly dialogue meeting with representatives from UK law enforcement agencies in order to share knowledge (trends and typologies) and best practice; and to encourage joint-working across operational and organisational boundaries.

1203. The UK FIU has deployed mechanisms to ensure co-operation between domestic law enforcement, the reporting sectors, and other branches of SOCA. The UK FIU has a Dialogue Team whose core function is to liaise between the sectors outlined above through formal meetings, informal contact, and workshops, and to facilitate feedback and share best practice with the reporting sector in sector specific seminars.

1204. The UK FIU also has a dedicated International Team whose core responsibility is to liaise with international partners through Egmont, FIU Net, FATF, and the FSRBs. Their primary function is to carry out checks of the ELMER database on behalf of foreign FIUs and request searches from foreign FIUs on behalf of UK Law Enforcement.

FSA

1205. The FSA has a statutory obligation to co-operate and co-ordinate domestically with other competent authorities to prevent and detect financial crime: FSMA, Part XXIII, section 354 states:

"the Authority must take such steps as it considers appropriate to co-operate with other persons (whether in the UK or elsewhere) who have functions in relation to the prevention and detection of financial crime."

1206. Secondary legislation, known as "the Gateways Regulations" prescribes the gateways under which the FSA can disclose confidential information to other persons (the original enactment can be found at www.opsi.gov.uk/si/si2001/20012188.htm). FSMA, Part XXIII places a duty on the FSA not to disclose confidential information without the consent of the person who provided it or the person to whom it relates. This prohibition is lifted when disclosure is made through a gateway contained in the above Regulations.

1207. One of the gateways contained in these Regulations is for "the purposes of criminal proceedings and investigations." This covers disclosure to facilitate a determination of whether criminal proceedings or investigations should be initiated. It therefore includes "suspected or actual" criminal activities. Other parts of the Regulations provide gateways for the FSA to disclose confidential information to a person on whom functions are conferred by or under Part 2, 3 or 4 of the Proceeds of Crime Act 2002 (i.e. the civil recovery aspects – see section 2 above). Gateways Regulations 3, 4, 9, and 12 refer.

1208. Further, section 34 of the Serious Organised Crime and Police Act allows the FSA to disclose any "confidential" information to SOCA, whether it is directive or not, to help it carry out its functions. MLRs 2003 Regulation 26 also requires the FSA to disclose to SOCA any information that indicates that a person has been, or may be, involved in money laundering.

1209. As described above under section 3.10, the FSA Intelligence Team liaises widely with law enforcement, the intelligence agencies, HMG and the assets recovery community. It also chairs a number of committees. The first is the Criminal Money Flows Working Group, which brings together representatives from many law enforcement agencies to discuss financial crime trends. The second is the Financial Crime Intelligence Group which allows representatives from the financial industry to hear issues from law enforcement first-hand.

1210. The FSA has seconded personnel to the UK FIU and UK FIU terrorist finance team to enhance co-operation between the organisations.

1211. The FSA has also agreed a number of MOUs with other UK authorities. Those that have a particular relevance to AML/CFT issues include the MOUs with: the Association of Chartered Certified Accountants, the Association of Chief Police Officers, HMRC, Institute of Actuaries, the Institute of Chartered Accountants in England and Wales, the Institute of Chartered Accountants in Ireland, Institute of Chartered Accountants in Scotland, the Law Society of England and Wales, the Law Society of Northern Ireland, the Law Society of Scotland, and the Tri-partite with HMT and Bank of England.

FSA UK MOUs with a relevance to AML/CTF
Association of Chartered Certified Accountants
Association of Chief Police Officers
HM Revenue and Customs
Institute of Actuaries
Institute of Chartered Accountants in England and Wales
Institute of Chartered Accountants in Ireland
Institute of Chartered Accountants in Scotland
The Law Society of England and Wales
The Law Society of Northern Ireland
The Law Society of Scotland
Tri-partite with HMT and Bank of England

HMRC

1212. HMRC has in place ongoing arrangements to share intelligence derived from frontier cash detections across the whole department, particularly with the direct and indirect tax offices.

1213. HMRC has developed good working relationships with security staff at major airports to ensure that any cash discovered during routine security screening of passengers is referred to HMRC for action. HMRC officers frequently attend airport security training courses to give presentations regarding cash awareness. A programme of presentations is underway to promote awareness and understanding of the MLRs 2003 to the Police and other law enforcement agencies. This enables them to identify non-compliance in MSBs and HVDs and gives them a point of contact within HMRC to forward this information.

1214. Links exist between HMRC's Financial National Intelligence Unit and the multi-agency Regional Asset Recovery Teams (RART) with whom good working relationships have been forged.

1215. HMRC has two research and analysis divisions: The Centre for Exchange of Intelligence (CEI) and the Centre for Research and Intelligence (CRI). Both make frequent disclosures to UK law enforcement agencies. In the financial year 2005-2006 CEI made 1,765 disclosures in relation to suspected money laundering offences and another 1,071 disclosures were made in relation to other financial offences under section 19 ATCS 2001. In the same period CRI made 3,944 disclosures under section19 ATCS in relation to suspected financial offences.

1216. HMRC's FNIU and SOCA work closely together on money laundering projects where both parties have a common interest. This approach encompasses strategic, tactical and operational levels. Information sharing has been paramount in the apprehension of major money launderers. An example is bulk data exploitation across various UK law enforcement and public bodies.

1217. HMRC provides secondments and expertise to ARA to support UK efforts to combat money laundering and other crime through civil recovery. One case currently being pursued by ARA with HMRC support relates to a situation where the recoverable amount is in excess of £5million.

Recommendation 32 (Criterion 32.1)

1218. The UK has recently reviewed the performance of several of its authorities involved in the fight against ML and FT. For example, the UK SARs regime has undergone three major reviews since 2001. There has also been a major review of asset recovery work in England and Wales. These reviews include:

- The KPMG Review 2003 commissioned by NCIS (now SOCA) took a holistic approach, from cradle to grave and made recommendations for each component part;
- Her Majesty's Inspectorate of Constabularies review of asset recovery in Payback Time 2004 focused on effort and resource allocation within police forces in England and Wales;
- The Jill Dando Institute of Crime Science Report commissioned by ACPO in 2005 focused on the feedback mechanism of the SARs regime;
- The SARs Review (a.k.a. Lander Review) commissioned by government in 2006 was principally concerned with how SOCA could improve the entire SARs system. The review identifies deficiencies in the reporters and end users participation; the resultant recommendations are now being implemented by SOCA.

1219. Also, a Government review of the UK's AML/CFT systems resulted in the publication of a UK AML strategy being published by HMT and the Home Office in 2004. At the time of the on-site visit, this process was being repeated. The Government published a new strategy on AML and CFT measures entitled "The Financial Challenge to Crime and Terrorism" in February 2007.

1220. The Financial Services Authority is currently undergoing a "value for money" review of its systems and procedures at the request of Treasury Ministers. This review will include some consideration, from a cost effectiveness perspective, of its approach to AML/CFT regulation.

6.1.2 Recommendations and Comments

1221. This recommendation is fully met. The UK has a comprehensive system for domestic co-operation to combat ML/FT, at both the policy and the operational levels. In addition, the UK has regularly reviewed the effectiveness of its AML/CFT systems; results and recommendations of the reviews have been endorsed by ministers and are now being implemented. The UK authorities should continue to implement the recommendations of the various AML/CFT reviews.

6.1.3 Compliance with Recommendation 31

	Rating	Summary of factors underlying rating
R.31	**C**	

6.2 The Conventions and UN Special Resolutions (R.35 & SR.I)

Recommendation 35 & Special Recommendation I

6.2.1 Description and Analysis

United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances (Vienna Convention)

1222. The United Kingdom signed the Vienna Convention on 20 December 1988 and ratified it on 28 June 1991. The UK has fully implemented the convention's provisions. One "Reservation" was made upon ratification:

> *"The United Kingdom of Great Britain and Northern Ireland will only consider the granting of immunity under article 7, paragraph 18, where this is specifically requested by the person to whom the immunity would apply or by the authority designated, under article 7, paragraph 8, of the Party from whom assistance is requested. A request for immunity will not be granted where the judicial authorities of the United Kingdom consider that to do so would be contrary to the public interest."*

1223. This means that the UK would not commit to grating immunity from prosecution in all circumstances listed under the convention. This is not considered an impairment to successful implementation of the convention generally.

United Nations Convention against Transnational Organised Crime (Palermo Convention)

1224. The United Kingdom signed the Palermo Convention on 14 December 2000 and ratified it on 9 February 2006. The UK has implemented the provisions pertinent to the FATF Recommendations.

International Convention for the Suppression of the Financing of Terrorism (CFT Convention)

1225. The United Kingdom signed the CFT Convention on 10 January 2000 and ratified on 7 March 2001. All of the Convention's provisions appear to be adequately implemented.

Special Recommendation I

CFT Convention

1226. See paragraph 1225 above.

S/RES/1267(1999) and successor resolutions and S/RES/1373(2001)

1227. The UK has adopted the United Nations Security Council Resolutions relating to the prevention and suppression of financing terrorism (S/RES/1267 (1999) and its successor resolutions and S/RES/1373 (2001). Details and implementation procedures are set out at Section 2 under the discussion of Special Recommendation III. The UK appears to have adequately implemented the provisions of these two resolutions.

Additional elements

1228. The UK signed the Convention on Laundering, Search, Seizure and confiscation of the Proceeds from Crime on 8 November 1990 and ratified it on 28 September 1992.

1229. In respect of AML and CFT, the UK has ratified the following other conventions:

- Protocol to Prevent, Suppress and Punish Trafficking in Persons, especially Women and Children, supplementing the United Nations Convention against Transnational Organized Crime;
- Protocol against the Smuggling of Migrants by Land, Sea and Air, Supplementing the United Nations Convention against Transnational Organized Crime; and
- Protocol against the Illicit Manufacturing of and Trafficking in Firearms, their Parts and Components and Ammunition, supplementing the United Nations Convention against Transnational Organized Crime.

6.2.2 Recommendations and Comments

1230. The UK authorities have implemented the relevant conventions and provisions of S/RES/1267(1999) and S/RES/1373(2001).

6.2.3 Compliance with Recommendation 35 and SR.I

	Rating	Summary of factors underlying rating
R.35	**C**	
SR.I	**C**	

6.3 Mutual Legal Assistance (R.36-38, SR.V, R.32)

6.3.1 Description and Analysis

Recommendation 36 and SR V

Legislation

1231. The UK is able to provide a full range of legal assistance in criminal matters under Part I of the Crime (International Co-operation) Act 2003 (CICA 2003) and sections 5 & 6 of the Criminal Justice (International Co-operation) Act 1990 (CRIJICA). Assistance for investigations, prosecutions and related proceedings is provided either through the UK's central authorities (UK Central Authority and Scotland's International Co-operation Unit, described below) or through the UK National Central Bureau of Interpol (which is housed in SOCA). It should be noted that in particular circumstances the HMRC can act as a central authority for MLA on fiscal matters relating to England, Wales, and Northern Ireland, and the Northern Ireland Office can handle certain cases related solely to Northern Ireland where the treaties or conventions allow it.

MLA through UK Central Authorities

1232. The range of legal assistance available through the Central Authorities includes:

- serving a summons or other judicial document requiring a person to appear before a judicial authority in the requesting country as a witness or defendant in criminal proceedings;
- obtaining sworn evidence or other authenticated or certified evidence, including banking documentation, for use in criminal proceedings or investigations;
- authenticating or certifying evidence for use in the requesting country where that evidence has already been obtained by the UK police for their own purposes;
- exercise of search and seizure powers where evidence is required for use in criminal proceedings or investigations; (including the of financial records from financial institutions or other natural or legal persons);
- temporarily transferring prisoners, with their consent, overseas to appear as witnesses in criminal proceedings or to assist in criminal investigations;
- actioning incoming requests for video and telephone conferencing of evidence given by witnesses and suspects;
- restraint (freezing) and confiscation of proceeds of crime for both conviction and non-conviction based confiscation regimes;
- requests for interception of telecommunications where this is required for evidence (this applies only to parties to the convention on Mutual Legal Assistance in Criminal Matters between Member States of the European Union of 29 May 2000).

MLA through UK National Central Bureau of Interpol

1233. The range of legal assistance available through the UK National Central Bureau of Interpol includes facilitating the following:

- interviewing witnesses and suspects in criminal investigations where the person is willing to co-operate without appearing before a judicial authority in the UK and where any statement made would be unsworn;
- tracing assets in investigations preliminary to prosecution, particularly where the offence involves money laundering;
- sharing information concerning investigations into offences, which have been committed in the UK;
- obtaining medical or dental statements or records where the patient has given written consent;

- providing details of previous convictions:
  - when provided with a copy of the person's fingerprints: for the purposes of police investigations, vetting applicants for employment in law enforcement or work with access to children or suitability for owning firearms and holding gambling licences;
  - for police intelligence purposes only - without fingerprints;
- providing telephone subscriber details;
- seizing and securing in the UK property stolen abroad (Police in the UK can seize and retain property where the person in possession of it in the UK is suspected of knowing that the property is stolen.)
- providing passport details (all details held by the UK Passport Service can be provided including any photographs held);
- providing medical samples (body orifice swabs and samples of blood, saliva, semen, hair, urine and other tissue fluids can be obtained with the consent of the person from whom the sample is required);
- providing details of keepers of motor vehicles registered in UK and driving licences issued in UK.

Service of overseas process in the UK

1234. Section 1 of CICA 2003 deals with the service of overseas process in the UK. The power conferred by that section on the Secretary of State (or the Lord Advocate in the case of service in Scotland) is to cause a relevant process or document from the Government of a country outside the UK (or one of its executive or law enforcement agencies) to be served by post, or if necessary by personal service by a police officer. The section applies to:

- any process issued or made in that country for the purposes of criminal proceedings;
- any document issued or made by an administrative authority in that country in administrative proceedings;
- any process issued or made for the purposes of any proceedings on an appeal before a court in that country against a decision in administrative proceedings; and
- any document issued or made by an authority in that country for the purposes of clemency proceedings.

Obtaining evidence in the UK

1235. Sections 13 to 19 CICA 2003 deal with the assisting of overseas authorities to obtain evidence in the UK. Requests for assistance may only be made by one of the following:

- a court exercising criminal jurisdiction,; or
- a prosecuting authority, in a country outside the UK; or
- any other authority in such a country which appears to have the function of making such requests for assistance; or
- the International Criminal Police Organisation; or
- any other body or person competent to make a request of the kind under any provision adopted under the Treaty on European Union.

1236. Assistance may be given in obtaining evidence in connection with:

(a) criminal proceedings, or a criminal investigation being carried on outside the UK;
(b) administrative proceedings, or an investigation into an act punishable in such proceedings being carried on there; or
(c) clemency proceedings, or proceedings on appeal before a court against a decision in administrative proceedings being carried on or intended to be carried on there.

1237. In a case within (a) or (b) evidence may be obtained only if the authority is satisfied that an offence under the law of the country in question has been committed or that there is reasonable cause to suspect that such an offence has been committed, and the proceedings in respect of the offence have been instituted in that country or that an investigation into the offence is being carried on there.

1238. If it appears that the request for assistance relates to a fiscal offence in respect of which proceedings have not yet been instituted the authority may not arrange for the evidence to be obtained unless (a) the request is from a country which is a member of the Commonwealth or is made pursuant to a treaty to which the UK is a party, or (b) the authority is satisfied that if the conduct constituting the offence were to occur in a part of the UK, it would constitute an offence in that part.

1239. Section 15 of CICA 2003 sets out the procedure to be followed in nominating a court in England and Wales, Scotland or Northern Ireland to receive evidence. Schedule 1 of CICA 2003 sets out the proceedings of a nominated court. This includes the fact that the court has the same powers for securing the attendance of a witness as it would have for the purposes of other proceedings before the court. Evidence may be taken on oath. Evidence received by the court is to be given to the court or authority that made the request or to the territorial authority for forwarding to the court or authority that made the request. So far as may be necessary in order to comply with the request where the evidence consists of a document, the original or a copy is to be provided and where it consists of any other article, the article itself or a description, photograph or other representation of it is to be provided.

Entry, search, and seizure

1240. When conducting investigations of money laundering and underlying predicate offences, the authorities have the power to obtain documents and information for use in those investigations and in prosecutions and related actions. This includes powers to use compulsory measures for the production of records held by financial institutions and other persons, the search of premises and for the seizure and obtaining of evidence.

1241. In order to action a request for entry, search and seizure, the conduct must constitute an offence under the law of a country outside the UK and if it occurred in England and Wales, constitute an indictable offence (Section 16(1) CICA 2003.) In Scotland, the court that issues the search warrant needs to be satisfied that the conduct constitutes an offence under the law of the requesting state and if that conduct had occurred in Scotland, would constitute a crime punishable by imprisonment (Section 18 of CICA 2003).

1242. A justice of the peace may issue a warrant under section 17 CICA 2003 if he is satisfied that:

- criminal proceedings have been instituted in a country outside the UK or a person has been arrested in the course of a criminal investigation carried on there, and where the conduct constituting the offence which is the subject of the proceedings or investigation would, if it had occurred in England and Wales be an indictable offence, or as the case may be in Northern Ireland, constitute an arrestable offence; and
- there are reasonable grounds for suspecting that there is on premises in England and Wales or Northern Ireland occupied or controlled by that person evidence relating to the offence.

1243. Such a warrant will authorise a constable to enter the premises in question and search to the extent reasonably required for the purpose of discovering any evidence relating to the offence and to seize and retain any evidence for which he is authorised to search.

1244. Scottish provisions apply similar procedures in the same circumstances.

Conditions/restrictions on MLA

1245. The UK's response to requests for MLA is bound by the legislative framework set out above, which is broad. Mutual legal assistance is not prohibited or generally made subject to unreasonable, disproportionate, or unduly restrictive conditions. No request will be declined without stating the reason or reasons why the request cannot be executed; or without consulting the requesting authority and, where appropriate, inviting it to modify the request so that assistance may be provided.

1246. Dual criminality is required for search warrants and may also be necessary in cases of freezing orders under sections 20(4) or Schedule 4 of CICA 2003 where the offences are not those contained in the relevant Framework Decision but rather are additional offences prescribed by order of the Secretary of State. This Section and Schedule are not yet in force; UKCA is liaising with other units in the Home Office to bring these sections into force as soon as possible. Dual criminality is also required under section 14(4)(b) of CICA 2003 (cases where evidence is requested at an investigatory stage in relation to fiscal offences where the request is not from a country which is for example a party to a relevant Treaty to which the UK is also a party. Dual criminality is also a requirement for Customer Information Orders under Chapter 4 CICA 2003).

1247. Also, on the grounds of public policy, the UK will decline to execute requests where a trial in the requesting country would involve double jeopardy (*ne bis in idem*). If the subject of a request has been convicted or acquitted in the UK or a third country of an offence arising from the conduct described in the request, the UK will not assist the gathering of evidence for another trial of the same person for the same conduct.

1248. Requests for assistance are not refused solely on the basis that they may involve tax matters. If it appears that the request for assistance relates to a fiscal offence in respect of which proceedings have not yet been instituted, the authority may arrange for the evidence to be obtained if (a) the request is from a country which is a member of the Commonwealth or is made pursuant to a treaty to which the UK is a party, or (b) the authority is satisfied that if the conduct constituting the offence were to occur in a part of the UK, it would constitute an offence in that part.

1249. There are no constraints on information provided by banks and other financial institutions which can be obtained under court order when required.

1250. Information properly protected by legal professional privilege, excluded material and special procedure material, however, is exempted from disclosure. (Section 26 CICA 2003, and in respect of warrants under section 17 CICA 2003.)

1251. There are no general limitations on assistance based on financial or professional secrecy. Paragraph 5 of Schedule 1 to CICA sets out the privilege of witnesses before a court nominated under section 15 CICA 2003. Such a person cannot be compelled to give any evidence which he could not be compelled to give:

- in criminal proceedings in the part of the UK in which the nominated court exercises jurisdiction, or
- in criminal proceedings in the country from which the request for evidence has come.

1252. The second only applies where the claim of the person questioned to be exempt from giving evidence is conceded by the court or authority which made the request. Further exemptions are that a person cannot be compelled to give any evidence if his doing so would be prejudicial to the security of the UK or in his capacity as an officer or servant of the Crown. (Similar exemptions are in place regarding television links.)

Processes for execution of MLA requests

1253. The majority of legal assistance requests to the UK are channelled through either the United Kingdom Central Authority (UKCA) based in the Home Office or the International Co-operation Unit (ICU) of the Crown Office in Scotland. The UKCA is a unit within the Home Office. It is headed by a lawyer and at the time of the on-site visit had 17 staff. (Further staff have since been recruited bringing the total to 28). It allocates requests to various law enforcement agencies for execution.)

1254. Where a request is for the service of documents this does not need to be done via the UKCA; the documents may be sent direct to the person concerned. MLA requests in relation to the following offences may be sent directly to HMRC, unless they relate to Scotland, when they should be sent to the ICU in Crown Office:

- Indirect taxation (e.g. value added tax on goods and services)
- Alcohol and tobacco smuggling
- Evasion of duties (excise fraud)
- Importation and exportation offences (e.g. drug trafficking; arms trafficking; smuggling of protected animal and plant species; smuggling of pornography; smuggling of counterfeit goods and other offences relating to customs prohibitions and restrictions and customs duties)

1255. Matters relating to drugs trafficking will be allocated to either SOCA or HMRC. Serious and complex fraud matters (with a value of more than £1 million) are normally dealt with by the Serious Fraud Office, and most other matters are dealt with by the police force best geographically located to execute the request.

1256. MLA guidelines are published on the Home Office website (available at: http://police.homeoffice.gov.uk/news-and-publications/publication/operational-policing/HO_MLA_webguidelines3rd1.pdf. These guidelines include a Code of Practice to be followed when dealing with these requests.

1257. With regards to requests for evidence, the Home Office will:

- acknowledge all requests for evidence upon receipt, giving contact details and a reference number for any queries;
- respond to all enquiries about the execution of requests for assistance within 10 working days of receipt;
- upon receipt of the request where the request is marked "urgent", or no later than 20 working days after receipt in other cases, either: provide the requesting authority with the assistance sought; or inform the requesting authority of the action being taken to obtain the assistance and provide, where possible, the name(s) and other contact details of the person(s) with responsibilities for executing the request, or provide the requesting authority with a full explanation why the request cannot be executed in its entirety or in part and where possible indicate how the assistance might otherwise be obtained;
- if the requesting authority notifies the United Kingdom that it is necessary, provide within 20 working days of receipt of the notification a report on the progress of the request and, where possible, indicate by when the request will be executed and update that report on a similar time scale;
- endeavour to meet all reasonable time scales for the execution of requests, including urgent requests.

1258. UKCA staff members vet incoming requests. Such requests are vetted to ensure that the request is made by an authority within section 13(2) or (3) of CICA 2003 and that the other statutory provisions within CICA have been complied with. They then allocate the request to the most

appropriate law enforcement agency to execute. Where issues have to be raised with the requesting state, this may be done by UKCA caseworkers.

1259. Requests for coercive measures are dealt with differently to those for non-coercive measures. It is common for requests for search and seizure to be put before the UKCA's senior management for an initial assessment and, if necessary, that member of the senior management team will take over the allocation of the request personally. Special procedures are also in place in relation to terrorism related requests—the Head of UKCA will engage in difficult cases, especially those involving terrorism as well as those which involve the use of coercive powers.

1260. Outgoing requests are examined by caseworkers to ensure that they refer to the correct legal base e.g. bilateral Treaty or International Convention. Caseworkers also ensure that any requirements which the requested country has made the UKCA aware of previously in relation to such requests are complied with (e.g. legalisation of documents etc).

1261. There is no UKCA policy which prohibits requesting jurisdictions dealing directly with the law enforcement officer allocated to execute the request. On the whole, UK authorities report that officers are content to deal directly with requesting jurisdictions; however, the UKCA does encourage the requesting jurisdiction and the executing officer to keep them informed of progress.

1262. The UKCA is responsible for monitoring progress on cases which have been allocated by it. This is mainly done in response to inquiries by the requesting jurisdiction for progress reports on the case in question. As described above it is hoped that the introduction of a clearer timescale for the execution of requests will assist the UKCA in this role. Recent changes in UKCA's working practices also aim to improve the current situation; however it is too early to report on whether this improvement is taking place.

1263. The UKCA has an internal review process to monitor the performance pledges stated in the MLA Guidelines. There has been a recent dip in performance; the UK authorities explain this as being due mainly to the bedding down of the new system and the move from focussing on the initial action to a more balanced and pro-active approach.

1264. The staffing of UKCA is kept under review. At the time of the on-site visit it was hoped that the resourcing of the UKCA as a whole will be looked into in 2007 in view of the increased work-load of requests for evidence (which have more than doubled since 2000). As mentioned in paragraph 1253 above, further staff have since been recruited.

Timeliness of responses to MLA requests

1265. The UKCA database does not allow for statistics to be compiled as to the average turnaround time for a request for mutual legal assistance. The UKCA and executing authorities will take into account any deadlines set out in the request when allocating resources to the request. A working group on turnaround times is being set up by the UKCA with its law enforcement stakeholders with the first meeting in December 2006. The agency with the largest number of requests to execute, the Metropolitan Police Force, has internal time limits for execution of requests. High priority requests are to be executed within one to three months, medium priority requests are to be executed within 6 months and low priority requests are to be executed within nine months.

1266. It is hoped that the results of this working group will be an agreement on common timescales for executing requests. Such timescales should be adhered to before the implementation of the European Evidence Warrant into UK law in order to improve overall response times.

1267. UK authorities are aware that even in straightforward requests problems can occur that will delay the execution of the request. It is anticipated that the adoption of common time limits will allow UKCA to case manage better and to "bring forward" cases to realistic dates.

1268. Complaints concerning delays have been received from overseas authorities. The view contained in a number of such complaints is that the UK is considered slower than other countries in executing MLA requests. Complaints do not usually relate to truly urgent requests but rather there appears to be dissatisfaction with the UKCA's handling of "routine" requests of a non-coercive nature e.g. for witness statements or for the provision of documentary evidence. As a result of this view, and as part of the recent review, a central enquiries line has been set up providing a single telephone number and email address. Bi-lateral meetings are held with certain partner countries (those which send larger numbers of requests to the UK) in order to examine perceived problems with the MLA process in the UK. UK authorities report that such meetings have proved useful.

Northern Ireland

1269. As the Northern Ireland Office can now act as its own Central Authority (following the Crime (International Co-operation) Act 2003), requests can now be sent directly to them where evidence is located solely within their jurisdiction, unless this is not permitted under the relevant bilateral treaties or international conventions. The same applies to outgoing requests.

Scotland

1270. The International Co-operation Unit (ICU) in the Crown Office operates under similar guidelines as the UKCA. However, there is a greater degree of flexibility of approach in the execution of requests for assistance as the legal staff within the Crown Office retains the authority to direct police officers in enquiries (Police (Scotland) Act 1967, section 17).

1271. The head of the ICU has supervisory responsibility for the execution of requests in Scotland, acting on behalf of the Lord Advocate. The ICU is able to be reasonably flexible in its approach to dealing with requests. It has a substantial amount of legal staff, and is therefore more able to get involved in the actual execution of requests. A rigorous reminder system is in operation, and timescales for execution are generally fairly tight.

1272. Scottish authorities are not aware of any complaints on MLA handling in the last 5 years. In 2003, a requesting state noted that the Scottish authorities had in fact been too assiduous in completing the request, and had gone further than was anticipated by the requesting state. As a result, the authorities reconsidered their response to the request.

Mutual Legal Assistance Treaties

1273. The legislative framework means that mutual legal assistance treaties are not necessary in the UK; however, to provide a basis for the execution of requests the UK has entered into a number of these. There are currently 32 such agreements in force, namely with the following countries: Australia, Ukraine, India, Nigeria, Bahrain, Canada, Ecuador, Hong Kong SAR, Ireland, Malaysia, Panama, Saudi Arabia, Spain, Thailand, United States of America, Antigua and Barbuda, Argentina, Romania, The Netherlands, Sweden, Bahamas, Barbados, Colombia, Grenada, Guyana, Paraguay, Italy, Trinidad and Tobago, Uruguay, Chile, Bolivia, and Mexico. Agreements with Brazil and Algeria have been signed but are not yet in force.

Multi-lateral agreements

1274. The UK is a party to the following multi-lateral agreements which include provisions on mutual legal assistance:

- The Vienna Convention 1988;
- United Nations Convention against Transnational Organised Crime, done at Palermo 2000
- United Nations Convention against Corruption, done at Mexico 2003;

- European Convention on Mutual Legal Assistance in Criminal Matters, done at Strasbourg in 1959 and Additional Protocol done at Strasbourg in 1978;
- Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds of Crime, done at Strasbourg in 1990;
- Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union, Brussels, 2000 and Protocol to the Convention on Mutual Assistance in Criminal Matters between Member States of the European Union, Brussels, 2001;
- Scheme relating to Mutual Assistance in Criminal Matters within the Commonwealth (the Harare Scheme) (amended 2002).

1275. Policy in relation to MLA is developed and co-ordinated by means of meetings between Home Office officials and various stakeholders. These include MLA forums attended by representatives from agencies such as SFO, Eurojust, HMRC, PPSNI, ARA, Crown Office, Scottish Executive, SOCA, Police, FSA, CPS, RCPO and the Court Service. There is also a separate judicial co-operation forum which looks at similar issues.

Avoiding conflicts of jurisdiction

1276. When a request is received for MLA relating to a criminal investigation or prosecution overlapping with an ongoing UK criminal investigation or prosecution a mutually beneficial agreement will be sought. If such an agreement cannot be reached the UK will usually postpone the execution of the request or the transmission of the evidence until such time as the transmission etc would no longer interfere with the UK criminal investigation or prosecution.

1277. "Eurojust" (a European Union body established in 2002 to enhance the effectiveness of the competent authorities within Member States when they are dealing with the investigation and prosecution of serious cross-border and organised crime) is available as a forum on conflicts of jurisdiction when they arise with another EU member state.

Additional elements

1278. Powers for compulsory measures (e.g. compelling production of, search and seizure of documents from financial institutions) are available in the UK; however, if they are for other than service of procedural documents they must be made via the relevant UK central authority (UKCA / ICU) or directly to HMRC in relation to certain offences.

Recommendation 37 (dual criminality relating to mutual legal assistance) and SR V

1279. As indicated above, certain elements mentioned in the CICA require dual criminality for compulsive measures, including search and seizure, and arrest warrants. In order to action a request for entry, search and seizure the conduct must constitute an offence under the law of a country outside the UK and if it occurred in England and Wales, constitute an indictable offence (Section 16(1) of CICA 2003) or an arrestable offence in Northern Ireland. In Scotland, the court that issues the search warrant needs to be satisfied the conduct constitutes an offence under the law of the requesting state and if that conduct had occurred in Scotland, would constitute a crime punishable by imprisonment (Section 18 of CICA 2003).

1280. A justice of the peace may issue an arrest warrant under section 17 CICA 2003 if he is satisfied that:

- criminal proceedings have been instituted in a country outside the UK or a person has been arrested in the course of a criminal investigation carried on there, and where the conduct constituting the offence which is the subject of the proceedings or investigation would, if it had occurred in England and Wales be an indictable offence, or as the case may be in Northern Ireland, constitute an arrestable offence; and

- there are reasonable grounds for suspecting that there is on premises in England and Wales or Northern Ireland occupied or controlled by that person evidence relating to the offence.

1281. If it appears that the request for assistance under section 15 CICA 2003 relates to a fiscal offence in respect of which proceedings have not yet been instituted the authority may not arrange for the evidence to be obtained unless: (i) the request is from a country which is a member of the Commonwealth or is made pursuant to a treaty to which the UK is a party; or (2) the authority is satisfied that if the conduct constituting the offence were to occur in a part of the UK, it would constitute an offence in that part.

1282. In Scotland, the prosecutor makes application to the Sheriff to grant an arrest warrant which the Sheriff may grant if he is satisfied: (i) there are reasonable grounds for suspecting an offence under the law of the foreign state has been committed and (ii) the criminal conduct constituting that offence, would if it occurred in Scotland constitute an offence punishable by imprisonment.

1283. For other, non-compulsory measures, dual criminality is not required. In fact, the majority of requests received by the UKCA and answered involve MLA requests regarding non-compulsive measures.

1284. For those forms of mutual legal assistance where dual criminality is required, the UK appears to have no legal or practical impediment to rendering assistance where both countries criminalise the conduct underlying the offence. In relation to MLA requests, it is the conduct constituting the offence which is examined rather than the manner in which the offence is classified or described. If the dual criminality test is met, there are no further impediments to rendering assistance.

Recommendation 38 and SR V

1285. POCA 2002 (External Requests and Orders) Order 2005 introduced in 2006 provides more effective support for responding to MLA requests by foreign countries that relate to the freezing, seizure or confiscation of (a) laundered property and (b) proceeds from the commission of any ML, FT or other predicate offences. The Criminal Justice (International Co-operation) Act 1990 (Enforcement of Overseas Forfeiture Orders) Order 2005 provides powers to respond to MLA requests by foreign countries to freeze, seize, and confiscate instrumentalities intended for use in the commission of any ML, FT, or predicate offences. Once this latter order came into force it put it beyond doubt that the instrumentalities of crime could be restrained or confiscated based on foreign requests even if they were not based on drug trafficking offences. This Order replaced a previous Order made pursuant to the 1990 Act (SI 1463/1991 as amended).

1286. Both these pieces of legislation allow for the receipt of requests to freeze assets in anticipation of a final confiscation or forfeiture order. Prosecution agencies can apply to court for a restraint order on the relevant property. This power is available from the commencement of the related criminal investigation overseas. After a final confiscation or forfeiture order is issued by a court abroad, it can be received by the UK and registered in UK courts for it to then by enforced against relevant property and assets within the UK.

1287. All applications come to the Home Office in the first instance. In Scotland, any overseas requests for asset restraint or confiscation go directly to the Lord Advocate's office.

1288. The Proceeds of Crime Act 2002 (External Requests and Orders) Order 2005 requires criminal confiscation and restraint requests to come to the Secretary of State. UKCA can then pass it to ARA (although operationally they do not), CPS, RCPO or SFO (as appropriate), who make a request to court for a restraint order or register the confiscation order to then enforce. In relation to civil orders, final orders are sent to the Secretary of State who then forwards them to ARA for registering in the High Court and then enforce. This is the procedure in England and Wales; there are different but

parallel procedures, where necessary, in Scotland and Northern Ireland, variable because of their different agencies.

1289. RCPO has obtained restraint orders in three cases following the enactment of the POCA (External Requests and Orders) Order 2005. The CPS has obtained four restraint orders in 10 cases referred under The POCA 2002 (External Requests and Orders) Order 2005. No final orders have been submitted for enforcement.

1290. UK confiscation legislation allows the request to be met where it relates to property of corresponding value. As indicted in the description and analysis under Recommendation 3, confiscation in the UK is value-based, i.e. the defendant's proceeds of crime are calculated as a value and they are then ordered to pay that amount (see Section 2 above).

1291. The UK has informal arrangements which assist in coordinating seizure and confiscation actions with other countries. In particular, SOCA deploys a network of international liaison officers to act as key points of contact overseas between foreign and UK law enforcement during investigations. These officers tend to be based in UK embassies and work closely with other representatives of UK government posted abroad. The network builds on bilateral and multilateral partnerships established by precursor agencies or by central departments such as the Home Office. The international liaison officers act as a national point of contact for all UK operational cooperation through Interpol, Europol, and the Schengen Information System. Responsibilities also include relevant input into, or engagement with, G8 processes, the European Police Chiefs Task Force, Eurojust, the UK magistrates' liaison network, and other bodies including UNODC.

Consideration of an asset forfeiture fund and asset sharing

1292. England, Wales, and Northern Ireland use funds confiscated to incentivise law enforcement prosecution agencies and the courts to pursue further asset recovery work. For these countries, confiscated funds are remitted to the Home Office. Under an incentive scheme 50% is paid back to front–line agencies e.g. police, prosecutors, and courts, and while the other 50% contributes to funding of core Home Office programmes e.g. policing, and asset recovery. In Scotland, confiscated funds up to a certain limit are applied for particular purposes decided by Scottish Ministers, with the balance being remitted directly to HM Treasury.

1293. The UK is able to share confiscated/ forfeited assets with other countries that have assisted operations in bringing the confiscation to fruition. The UK has authority to share up to 50% of the proceeds of confiscation, net of costs. Where funds recovered represent the proceeds of grand larceny or corruption by a kleptocrat and an entire state is the victim, it is UK policy to repay 100% of recovered funds, minus costs. The UK has no need for a formal instrument such as an agreement or treaty to cover asset sharing. The UK can share with other countries on an ad hoc case-by-case basis. However the UK has concluded such agreements, with the United States of America in 1992, and with Canada in 2001, and a memorandum of understanding (MOU) with Jamaica. The UK is also prepared to enter into negotiations with other states who feel that an agreement would be of benefit.

1294. The UK has shared with and received such money from foreign jurisdictions previously, although the Home Office does not systematically record comprehensive statistics. Information from the Crown Prosecution Service shows that in 2004 it enforced a US order to the value of £4.2 million, and this sum was shared equally between the US and the UK. UK authorities also assisted the US concerning a drug money laundering operation resulting in an order for $20 million to be paid to the US authorities, of which $10 million was shared with the UK in 2004.

Additional elements

1295. The UK can recognise and enforce foreign non-criminal confiscation orders. As mentioned in paragraph 1288 above, the Secretary of State will forward civil forfeiture orders to ARA for registration in the High Court and enforcement.

Recommendation 32 (statistics)

MLA statistics: total requests that have passed through UKCA *(source: Home Office):*

	Asset Restraint		Coercive Evidence		Non-Coercive Evidence		Service of process		Other	
	received	sent	received	sent	received	sent	received	sent	received	sent
2002	6	5	87	21	1428	2533	1588	74	140	13
2003	5	47	58	13	1283	1761	1512	119	51	5
2004	11	14	45	11	1561	1555	1300	187	157	53
2005	5	13	65	16	1803	1517	1504	180	57	8
2006	7	8	54	5	2187	1120	1073	180	62	16

1296. Neither the UKCA nor the Crown Office retains a breakdown of the offences concerned in each case (i.e., ML, predicate offences, or FT), so these statistics do not relate solely to matters of money laundering or terrorist financing.

Total requests that have passed through Crown Office 2002 to 2006 (source: Crown Office)

	MLA – incoming	MLA – Outgoing	Service Of Process
2002	52	24	61
2003	53	70	51
2004	80	156	43
2005	96	140	81
2006	126	118	63

1297. The UKCA database does not provide statistics on the number of MLA requests refused. As a result of recent improvements to the UKCA database, UK authorities are now able to identify the length of time taken to execute a given mutual legal assistance request. Although this information is useful, the database remains a relatively unsophisticated tool. It is unable to provide average turnaround times for MLA requests.

HMRC legal assistance requests

1298. The Mutual Legal Assistance incoming requests fall broadly into the following categories. It should be noted however that many of the cases overlap; and many have an associated money laundering aspect not shown here. In 2004, **42** letters of request in relation to money laundering offences were issued by the prosecutor on behalf of HMRC. This increased to **76** in 2005.

Type of incoming MLA requests	**2004/05**	**2005/06**
Arms	3	4
Drugs	84	195
Money laundering	16	34
Customs	47	75
Tobacco	12	44
VAT	12	9
Tax Evasion	18	27
Weapons of Mass Destruction	3	7
Total	**195**	**395**

1299. The CPS presently has 50 requests for restraint and confiscation assistance derived from 24 countries. They are broken down as follows:

	Number of requests	Provisional measures (restraint) taken	Final orders taken and being enforced
Criminal Justice Act 1988	27	11	2
Drug Trafficking Act 1994	7	6	4
POCA 2002	16	10	None yet submitted for enforcement

6.3.2 Recommendations and Comments

1300. The UK has broad legal provisions to facilitate requests for mutual legal assistance. Standard evidence gathering mechanisms have recently been reviewed and updated in the Crime (International Co-operation) Act 2003, and new provisions have been introduced to allow for the restraint and confiscation of instrumentalities of crime at the request of foreign jurisdictions. New legislation has also been introduced under POCA to give effect to foreign restraint, confiscation and forfeiture orders in both the criminal and civil context. There are no unduly restrictive measures placed on the provision of assistance, and dual criminality is only required for a few types of assistance (i.e., coercive measures such as search warrants).

1301. The UK is able to share confiscated or forfeited assets with other jurisdictions, and internally is able to use funds confiscated to incentivise law enforcement and prosecution agencies in their work.

1302. However, there remain concerns about the ability of the UK authorities (excluding Scotland) to handle mutual legal assistance requests in a timely and effective manner. This is an implementation issue which goes beyond the existence of the legal framework itself, which is generally seen as being adequate.

1303. Whilst the UKCA can give priority to urgent or important requests on a case by case basis, it is presently unable to ensure timely and effective turnaround of routine requests. The UKCA allocates the request to a responsible law enforcement agency and although it is responsible for monitoring progress on the case, in practice this is mainly done in response to inquiries by the requesting jurisdiction concerning progress.

1304. It is recommended that the UKCA institute a far more pro-active approach to monitoring progress on execution of requests and ensuring a timely and effective response. Case officers within the UKCA should assume overall responsibility for each request and the case officer should be centrally and actively engaged in dialogue between the allocated law enforcement agency and the requesting jurisdiction concerning execution of the request on a regular and unprompted basis. The focus should shift from a "case allocation" approach to a pro-active "case monitoring and completion" approach.

1305. The UK authorities should improve mechanisms for overall co-ordination of execution of requests, both domestically with its own law enforcement agencies and externally with requesting jurisdictions. The UKCA should ensure that clear lines of communication exist with established points of contact between itself and the law enforcement officer responsible for execution of the request, as well as between itself and the requesting jurisdiction.

1306. The UK authorities are encouraged to continue their bilateral dialogue with certain partner countries to examine perceived problems and work towards resolution.

1307. If deemed necessary to improve implementation issues identified, the Home Office should consider providing additional resources to the UKCA, particularly by way of additional manpower or

case officers to support the workload, which continues to increase. The additional recruitment of lawyers to become more actively involved in execution the requests should be considered.

6.3.3 Compliance with Recommendations 36 to 38 and Special Recommendation V

	Rating	Summary of factors relevant to s.6.3 underlying overall rating
R.36	**LC**	• There are concerns about the ability of the UK authorities (excluding Scotland) to handle mutual legal assistance requests in a timely and effective manner; the UK is presently unable to ensure timely and effective turnaround of all routine requests.
R.37	**C**	
R.38	**C**	
SR.V	**C**	

6.4 Extradition (R.39, 37 & SR.V)

6.4.1 Description and Analysis

Recommendation 39 and SR.V

1308. Extradition from the UK is governed by the Extradition Act 2003 ("the 2003 Act") which came into force on 1 January 2004. The 2003 Act allows for extradition where the conduct for which extradition is sought is punishable by a custodial sentence of at least 12 months in both the requested and requesting states. Money laundering is therefore an extraditable offence in the UK. The UK can also extradite its own nationals.

1309. All the extradition arrangements described below apply in respect of terrorist financing. In addition, the UK has ratified the UN Convention on the Suppression of the Financing of Terrorism and the provisions of the 2003 Act will apply in any extradition request received by any co-signatory to this Convention with which the UK otherwise has no general extradition arrangements in place.

1310. "Part 1" of the 2003 Act gives effect in the UK to the Framework Decision on the European Arrest Warrant (EAW) which the UK operates with the other 24 EU Member States. "Part 2" governs the UK's extradition relations with the rest of the world.

1311. Under Section 3 of the Prosecution of Offences Act 1985 as amended, the Crown Prosecution Service of England and Wales gives effect to the UK's various international extradition obligations by providing advice and court representation to foreign judicial authorities and states seeking the extradition of persons arrested in England and Wales. In practice, this work will be carried out by specialist lawyers from the Special Crime Division at CPS Headquarters in London. There are currently seven lawyers engaged in this work with arrangements to recruit more. They are supported by four administrative staff. Liaison with the foreign authorities concerned will depend on the country and the nature of the case. Generally, with requests from Part 1 countries (that is countries operating the European Arrest Warrant system) communications will be facilitated by the SIRENE Bureau of the Serious Organised Crime Agency. Communications will also be facilitated where appropriate by UK Liaison Magistrates stationed in Paris, Rome and Madrid and by the UK representative to Eurojust. In respect of Part 2 countries, the main channel of communication will be via the Judicial Co-Operation Unit at the Home Office. Liaison in requests from the USA is often assisted by direct contact with the Department of Justice and the UK Liaison Magistrate stationed in Washington, as well as the US Liaison Magistrate based in London. On occasion liaison will be via diplomatic channels or directly with the lawyer responsible for the case in the requesting territory.

1312. As at July 2006, the UK also had extradition relations through bi-lateral and multi-lateral treaties with 115 countries. In addition to this, the UK's extradition legislation contains provision for extradition between the UK and another country with which no general extradition relations are in place. This is done through two means:

1313. Section 193 of the 2003 Act establishes extradition relations with countries party to international conventions, that the UK is also a party to, which contain extradition provisions. These conventions relate to specific forms of very serious crimes such as terrorism, drug trafficking and torture. It should be stressed that extradition can only take place under section 193 if the alleged conduct for which extradition is sought falls under the convention concerned and if the country concerned has been designated under s.193 of the Act by way of secondary legislation.

1314. Section 194 allows for special one-off extradition from the UK to countries with which the UK does not have a formal extradition treaty. Under this section, the UK can agree to ad hoc arrangements for extradition of a particular person, and extradition proceedings in UK courts can then take place on a similar basis to cases based on a treaty. For extradition to be possible, dual criminality must apply. The UK authorities advised that the secondary legislation under s. 193 has not yet been

enacted for the new extradition channels opened up by the Palermo Convention, but that this was a technical rather than substantive gap because of the availability of the s. 194 procedure on a case by case basis. the CFT convention is included on the s. 193 Order, see http://www.opsi.gov.uk/si/si2005/20050046.htm.

"Part 1" (European Arrest Warrant) cases

1315. For Part 1 cases, SOCA is the central authority for the receipt and transmission of European arrest warrants (EAWs) in England, Wales, and Northern Ireland. SOCA is also responsible for the UK National Central Bureau of Interpol which facilitates provisional arrest requests from non EAW partners. The Fugitives Unit of SOCA currently comprises 23 staff and a pro-active approach to locating fugitives has been developed. The functions of the unit are supported by means of a 'duty officer' shift function covering the full 24-hour cycle.

1316. Part 1 cases in Scotland are directed to the Crown Office (ICU) as the designated central authority. In urgent cases it is possible for a requested person to be arrested prior to the receipt of an extradition request. The EAW with accompanying translation, where appropriate, must be received in time for a court hearing to be held within 48 hours of the arrest.

1317. The designated authority may issue a certificate if the warrant has been issued by a judicial authority in the requesting territory. If the warrant is certified then the requested person is arrested and brought before a court. The documentation can only be certified if the requirements of section 2 of the 2003 Act are met. Prior to January 2007, in cases where the requested person has been convicted, the documentation must make it clear that the person is "unlawfully at large", i.e. has been convicted and is liable to immediate arrest and detention. The Extradition Act 2003 was amended in January 2007 by way of Schedule 13 to the Police and Justice Act 2006; the requirement for a person to be shown to be unlawfully at large has been amended to a requirement for the request to demonstrate that the person has been convicted, and his extradition is sought for the purpose of being sentenced or to serve a sentence.

1318. At the initial hearing after a person's arrest, the District Judge must: confirm, on the balance of probabilities, the identity of the requested person; inform the person about the procedures for consent; and fix a date for the extradition hearing if the requested person chooses not to consent to his or her extradition.

1319. The extradition hearing should normally take place within 21 days of arrest. If the judge is satisfied that the conduct amounts to an extradition offence and that none of the bars to extradition apply (the rule against double jeopardy; extraneous considerations; passage of time; the person's age; hostage-taking considerations; speciality; the person's earlier extradition), he is required to decide whether the person's extradition would be compatible with the Convention rights within the meaning of the Human Rights Act 1998. If the judge decides that question in the affirmative, he must order the person to be extradited.

Dual Criminality Test

1320. The Framework Decision contains a list of 32 categories of offence for which the "dual criminality" test is not needed. The offence must carry a minimum 3 year sentence in the issuing state. If the conduct for which extradition is sought is not covered by one of these list offences, then the conduct must be an offence in both the issuing and executing states. Also, if any of the conduct for which extradition is sought was carried out outside the issuing state, the conduct must be an offence in both the issuing and executing states

Appeals and surrender

1321. An appeal against extradition must be lodged within seven days of a person's extradition being ordered. The requested person may appeal to the High Court if the judge orders his extradition. The issuing territory may appeal against the discharge of the person by the judge at the extradition hearing. The decision of the High Court may be appealed against in the House of Lords by either the requested person or the issuing territory provided that leave to appeal has been given by either the High Court or the House of Lords. An appeal to the House of Lords can only be made on a point of law of general public importance and where it is agreed by the High Court that the point is one which should be considered by the House of Lords. Section 32 of the 2003 Act refers.

1322. The person in respect of whom extradition has been ordered should normally be extradited within 10 days of the final court order. If there are exceptional circumstances, and with the agreement of the Issuing State, this time-limit can be extended.

"Part 2"cases

1323. For extradition requests received under Part 2 of the 2003 Act ("incoming requests" or "export extradition"), the Extradition Section of the Home Office's Judicial Co-operation Unit is the central authority for England, Wales, and Northern Ireland for the receipt of requests from the diplomatic or other recognised authorities of requesting States. On behalf of the Secretary of State, the section is responsible for placing request before the courts. It also advises the Secretary of State on the decision he may have to make under Part 2 of the Act as to whether a person is to be extradited; and initiates the practical arrangements when extradition is to take place. In these roles, it liaises with requesting states (to advise on procedures and obtain information), the courts, the Crown Prosecution Service and the Metropolitan Police Service as necessary. The section has 10 staff, comprising of a Head of Section, 6 caseworking staff and 3 policy staff.

1324. The Secretary of State then issues a certificate and sends the papers to the court, which then issues a warrant for the requested person's arrest. The documentation can only be certified if the requirements of section 70 of the 2003 Act are met. In cases where the requested person has been convicted, the documentation must also include a statement that the person is "unlawfully at large", i.e. has been convicted and is liable to immediate arrest and detention (although cf amendments to legislation in paragraph 1317 above). Requesting states are advised to submit a draft request to the Crown Prosecution Service to ensure potential difficulties are resolved before the request is finally submitted.

1325. The ICU in the Crown Office in Scotland is responsible for extradition operation in Scotland. There are 4 lawyers in the ICU. These lawyers prepare EAWs and liaise as appropriate with foreign authorities. Part 2 cases are then directed to the Scottish Executive Justice Department. Scottish Ministers consider the certification of such a request, which if certified is then dealt with procedurally before the Court by the Lord Advocate.

1326. Generally the information required to accompany the request will include:

- particulars of the person whose return is requested;
- particulars of the offence of which he is accused or was convicted;
- in the case of a person accused of an offence, a warrant or a duly authenticated copy of a warrant for his arrest issued in the requesting state, or for a provisional arrest, details of such a warrant;
- in the case of a person unlawfully at large after conviction of an offence, a certificate or a duly authenticated copy of a certificate of the conviction and the sentence, or for provisional arrest, details of the conviction;

- evidence or information that would justify the issue of a warrant for arrest in the UK, within the jurisdiction of a judge of the court that would hold the extradition hearing – see "Evidence" below.

1327. Some countries are not required to provide *prima facie* evidence in support of their request for extradition. These countries were, as of 28 July 2005: Albania, Andorra, Armenia, Australia, Azerbaijan, Bulgaria, Canada, Croatia, Georgia, Iceland, Israel, Liechtenstein, Macedonia FYR, Moldova, New Zealand, Norway, Romania, Russian Federation, Serbia and Montenegro, South Africa, Switzerland, Turkey, Ukraine and the United States of America. Romania and Bulgaria acceded to the EU on 1 January 2007, and they are accordingly now listed on the Order designating them so that Part 1 of the Extradition Act applies to their requests (see paragraph 1311 above). Further to this Bosnia Herzegovina has acceded to the Council of Europe, and no longer needs to supply prima facie evidence with requests.

1328. After the person has been arrested, he is brought before the court as soon as is practicable and the judge sets a date for the extradition hearing. The judge must satisfy himself that the request meets the requirements of the 2003 Act, including dual criminality and where appropriate, prima facie evidence of guilt; and that none of the bars to extradition apply (the rule against double jeopardy; extraneous considerations; passage of time or hostage-taking considerations). Finally, he is required to decide whether the person's extradition would be compatible with the Convention rights within the meaning of the Human Rights Act 1998. If he decides all of these questions in the affirmative, he must send the case to the Secretary of State for the latter's decision whether the person is to be extradited. Otherwise, he must discharge the person.

1329. Where a case is sent to him, the Secretary of State must consider whether surrender is prohibited because:

i) the person could face the death penalty: This is an absolute prohibition unless the Secretary of State receives an adequate written assurance from the requesting state that the death penalty will not be imposed, or will not be carried out, if imposed;

ii) there are no speciality arrangements with the requesting country: The condition of "speciality" requires that the person must be dealt with in the requesting state only for the offences in respect of which the person is extradited (except in certain limited circumstances); or

ii) the person was earlier extradited to the UK: This might require the Secretary of State to obtain the consent of the earlier extraditing country, before the person can be extradited on to the requesting state.

1330. In this event, the defence has to make any representations within six weeks of the case being sent to the Secretary of State (42 days, including the day the case was sent). This was revised down to four weeks in January 2007. The Secretary of State has to make his own decision within two calendar months of the day the case is sent to him, or else the person may apply to be discharged.

1331. However, if the representations are complex and require enquiries being made of the requesting state, the Secretary of State may apply to the High Court for an extension of the decision date, of any length but usually of no more than two moths – it is a matter for the court as to whether and for how long this is granted, although it has not to date refused any such application. More than one extension may be sought in any one case; and granted if it appears necessary.

1332. If the Secretary of State does find that surrender is prohibited, he must order the discharge of the person. If none of the three prohibitions apply, or appropriate assurances have been given, the Secretary of State must order the person to be extradited.

Appeals and surrender

1333. A requested person may appeal within 14 days to the High Court if:

i) the district judge sends the case to the Secretary of State; and
ii) the Secretary of State orders his extradition.
Such an appeal may be against either or both of the decisions at (i) and (ii).
A requesting state may appeal within 14 days to the High Court against the discharge of the requested person by:
iii) the judge at the extradition hearing; or
iv) the Secretary of State (after the case has been sent to him by the District Judge).

1334. A decision of the High Court in an extradition case may be appealed against in the House of Lords by either a requested person (or if a person is discharged by the High Court, by a requesting state) provided that leave to appeal has been granted. An appeal to the House of Lords can only be made on a point of law of general public importance and where it is agreed by the High Court that the point is one which should be considered by the House of Lords. Section 114 of the 2003 Act sets out the details and time limits for such an appeal.

1335. Unless there is an appeal the person whose extradition has been ordered should be extradited within 28 days of the Secretary of State making his decision. Where there is an appeals process, the 28 days will begin once all the legal remedies have been exhausted. If there are exceptional circumstances, this time-limit can be extended, although if the person applies to the District judge for discharge, reasonable cause must be shown for the delay.

Restrictions on extradition

1336. In Part 1 cases, responsibility for deciding whether to order extradition lies with the District Judge. In such cases the bars to extradition are

- Identity – the judge must be satisfied that the person in front of him is the person named on the EAW;
- The rule against double jeopardy;
- The risk of prejudicial treatment upon return on account of the person's race religion, nationality, gender, sexual orientation or political opinions;
- The passage of time since the commission of the offence/the person became unlawfully at large, where it is such as to make extradition unjust or oppressive;
- The person's age if it he/she would have been under the age of criminal responsibility in equivalent circumstances in the UK;
- Hostage-taking considerations – that is to say where the offence falls within s. 1 of the Taking of Hostages Act and communication between the person and an appropriate representative would not be possible were he/she to be extradited;
- Speciality
- Earlier extradition to the UK from a category 1 territory, where that territory's consent is required to the onward extradition now under consideration and such consent has not been given.
- Earlier extradition to the UK from a category 2 territory, where that territory's consent is required to the onward extradition now under consideration and such consent has not been given.

1337. Extradition must also be refused where the request relates to a conviction in absence if the court concludes that the person had not deliberately absented himself from his trial and would not have an automatic right to a retrial (or equivalent upon return. Extradition can only be ordered if the judge is satisfied that doing so would not breach the person's rights under the European Convention on Human

Rights. Extradition must be postponed until any domestic charges against the person have been finalised and any domestic sentence of imprisonment completed. It is possible for the court to order the temporary surrender of a serving UK prisoner in order that a foreign trial can go ahead promptly.

1338. If during the extradition hearing the judge concludes that the person's physical/mental condition is such that it would be unjust or oppressive to order his extradition, he must either adjourn the hearing until the person recovers or discharge the proceedings altogether.

1339. In 2005 (the last full calendar year for which statistics are available), the courts in England and Wales refused to execute 12 EAWs. The grounds for these were: double jeopardy; time limit for prosecution expired; insufficient information concerning the alleged conduct; voluntary presentation to the issuing judicial authority; and the offence not being an extradition offence. In addition to these 12, seven individuals were discharged twice due to a lack of information.

1340. In Part 2 cases, the District Judge must determine whether the requirements of the Extradition Act are complied with, whether any of the bars to extradition apply and whether extradition would be compatible with the person's human rights. The bars to extradition in Part 2 cases are listed in bullet points 1-6 for Part 1 cases (in paragraph 1336 above):

1341. Similar rules apply to those under Part 1 in respect of convictions in absence, the person's physical or mental condition, domestic proceedings/sentences and compatibility with the persons' human rights.

1342. If satisfied in relation to these matters the judge must send the case to the Home Secretary who decides whether the person should be extradited. The Home Secretary may only refuse extradition on one of three grounds: (1) where the person has been, will be or could be sentenced to death for the offence concerned in the requesting territory; (2) if there are no speciality arrangements with the requesting territory; and (3) where the person has previously been extradited to the UK from another territory if that territory's consent is required to the onward extradition now under consideration and such consent has not been given. A decision on extradition must be deferred pending the determination of any domestic UK charges and the completion of any UK sentence of imprisonment.

1343. In 2005 (the last full year for which figures are available), 22 extradition requests, made under Part 2 of the 2003 Act, were unsuccessful for various reasons. Of these 22, 4 (or 18%) were refused for passage of time or politically motivated request grounds.

Measures for handling requests without undue delay

1344. There are time limits laid out in the 2003 Act concerning extradition cases. However, where the subject of an extradition request made to the UK is also the subject of domestic proceedings against him or her, then the domestic proceedings will take precedence, with an obvious impact on the timeframe in which extradition cases can be handled.

1345. Since entry in to force of the 2003 Act, CPS' extradition caseload has more than doubled. This is principally due to the Act's implementation of the (European Arrest Warrant) EAW Scheme. CPS anticipates that the increase will continue with the accession of new EU Member States. In 2010, the UK is scheduled to implement the Schengen Information System and it may reasonably be anticipated that this will add a further and very significant increase to the caseload. However, the CPS also indicated that the courts, particularly the Administrative Court, have very significantly reduced listing times for extradition cases, with the Lord Chief Justice recently emphasising the importance of expedition in dealing with extradition cases. The impression at the City of Westminster Magistrates' Court is that, except for a few cases, extradition is much faster under the 2003 Act.

1346. Challenges in the Administrative Court have increased as follows:

Year	2004	2005	2006 (through October)
Judicial Review Criminal	20	13	21
Statutory Appeals and Applications	24	46	48
Writ of habeas Corpus		11	2
Extradition Total	44	70	69

1347. Of the 61 cases involving extradition (of all types) which were listed in the Administrative Court so far this year, over 26 were heard within 70 days of being lodged.

Additional elements

1348. Legislation and policy regarding the European Arrest Warrant (EAW) allows for the direct transmission of EAWs between foreign designated competent authorities and SOCA in England, Wales and Northern Ireland, or the Crown Office in Scotland. All other extradition requests must be made through diplomatic channels.

Recommendation 37 and SR.V (dual criminality relating to extradition)

1349. As long as dual criminality applies (irrespective of any technical differences in the respective laws of the two countries), then the UK will consider any extradition request made under Part 2 of the 2003 Act by a designated extradition partner. Dual criminality is generally not required for Part 1 requests. The Framework Decision contains a list of 32 categories of offence for which the "dual criminality" test is not needed; the offence must carry a minimum 3 year sentence in the issuing state. Money laundering and terrorist financing are included on the list.

Additional elements

1350. With regard to terrorist financing, simplified procedures (the European Arrest Warrant) applies for those situations meeting the conditions in Part 1 of the Extradition Act 2003.

Statistics

2005 statistics (all crimes)—proportion of surrenders to refusals and reasons for refusal (England, Wales, and Northern Ireland):

	Number received	Arrests	surrenders	refusal
Part 1 (EAW)	5986	154	77	12*
Part 2	54		25	22**

*Reasons for refusal: Double jeopardy; time limit for prosecution expired; insufficient information concerning conduct; voluntary presentation to issuing judicial authority; offence not an extradition offence.
**(Reasons: Politically motivated requests (3); judge not satisfied offence was extradition offence; insufficient information; Immigration Status (2); Arrest Warrant withdrawn (person discharged at court); passage of time; conviction in absentia; no extradition papers received).

2000-2006 Statistics—number of extradition requests concerning money laundering (England, Wales, and Northern Ireland):[31]

	No of Requests	No of Surrenders

[31] The European Arrest Warrant has been in force in the UK since 1 January 2004. Many countries circulate EAWs to a large number of Member States because the whereabouts of the target are unknown; the apparently poor figure for EAW surrenders below is a result of this: the targets have turned out not to have a link to the UK. The UK will only issue an EAW when the whereabouts of the suspect is known. One UK request was refused by the requested state because of a lack of dual criminality.

Incoming Part 1 cases (EAWs)	86	0
Incoming Part 2 cases (extradition requests)	4	4
	No of Requests	**No of Returns**
Outgoing EAWs	2	2
Outgoing extradition requests	3	2

Extradition for terrorist finance offences (England, Wales, and Northern Ireland):

1351. Home Office records indicate that terrorist finance is a factor in: two active cases, where the subject for extradition is currently under arrest; one pending case, where no arrest warrant has yet been issued; and one completed case where the subject has been surrendered. A further three extradition case histories on record at the Home Office cite "support for terrorist organisations" although financing is not specifically referenced.

2004-2006 Statistics—number of challenges lodged in Administrative Court (England, Wales, and Northern Ireland):

	Judicial Review Criminal	Statutory Appeals and Applications	Writ of habeas Corpus
2004	20	24	
2005	13	46	11
2006 (to end of October)	21	48	2

2002-2006 Scotland extradition statistics (all crimes*):

	Incoming extradition requests (Part 1 & Part 2 cases)	Incoming extradition requests: Surrenders**	Outgoing extradition requests (Part 1 & Part 2 cases)	Outgoing extradition requests: Returns**
2002	4	1	4	5
2003	8	1	12	3
2004	8	3	19	11
2005	9	2	18	11
2006	26	7	21	9

*Scotland has received no extradition requests for money laundering offences.
**Surrender/Return figures relate to actual surrender/returns in the year in question, and do not relate necessarily relate to requests received in the same year.

6.4.2 Recommendations and Comments

1352. Money laundering and terrorist financing are extraditable offences and there are no restrictive conditions or impediments existing in law for extradition. The UK can extradite its own nationals.

1353. Extradition law and procedure in the UK was significantly altered by the introduction of the Extradition Act 2003. This was necessary to implement obligations in relation to the EU Framework Decision concerning the EAW scheme (Part 1). However, procedures for all other jurisdictions (Part 2) were also changed with a view to expediting the process of extradition, which at times had been cumbersome and slow under the precursor legislation.

1354. One significant change in the Part 2 procedure has been the reduced role that the Secretary of State now plays in the surrender decision. Another is the abolition of the requirement to provide *prima facie* evidence in support of the request for extradition for certain listed jurisdictions. These changes are positive as they have simplified the extradition process, while at the same time retaining some essential safeguards in the legislation. In practice, the courts now assume a greater role in determining the outcome of the extradition request.

1355. Since the introduction of the Act, the number of extradition cases has risen, principally due to the implementation of the EAW scheme. The proportion of challenges does not appear to have risen, and feedback from the authorities and the courts suggests that overall cases are in fact being handled more expeditiously under the 2003 Act. Implementation efforts also therefore appear positive under the 2003 Act, with the chances of delay arising in the procedure in practice having been reduced.

1356. Extradition requests continue, in certain cases, to be refused and this is to be expected. In some cases the request will not meet the minimum legal requirements to go forward, and in others the court may intervene to apply safeguards built into the legislation. The UK authorities are encouraged to keep operation of procedures under the 2003 Act under active review to ensure that a proper balance is achieved between the interests of the requesting state in securing the fugitive's return and the rights of the fugitive in that process.

6.4.3 Compliance with Recommendations 37 & 39, and Special Recommendation V

	Rating	Summary of factors relevant to s.6.4 underlying overall rating
R.39	**C**	
R.37	**C**	
SR.V	**C**	

6.5 Other Forms of International Co-operation (R.40, SR.V & R.32)

6.5.1 Description and Analysis

Recommendation 40 and SR.V

1357. The majority of UK International Mutual Assistance is in the criminal sphere and is either based in Mutual Legal Assistance (MLA) requests or Mutual Administrative Assistance (MAA). MAA co-operation is used in both criminal and non-criminal matters where coercive powers and judicial oversight are not required (e.g. consent evidence). It involves the exchange of information or non-coercive evidence on an officer-to-officer, law enforcement co-operation basis. MAA is often conducted under Memoranda of Understanding (MOU) — a non-legally binding international arrangement — or binding legal arrangements. It can also be obtained from and provided to foreign authorities with whom the UK has not concluded formal MAA agreements. Whilst MAA allows for the passage of information and evidence in relation to assigned matters, or the passage of technical assistance information, it does not allow for intrusive or coercive measures to be applied (for example search, seizure etc), which are matters of MLA. All the mechanisms and arrangements apply to international co-operation on terrorist financing.

FIU-FIU cooperation

1358. In general, the UK FIU has broad capabilities to co-operate with foreign FIUs. Exchanges of information are allowed spontaneously and upon request. The UK FIU is authorized to conduct enquiries on behalf of its foreign counterparts, including searches of its SAR database and other databases to which it has access.

1359. When a foreign FIU requests assistance from UK FIU, it must complete a request for information form, preferably the official Egmont form. This form should contain as a minimum a clear link between the subjects and the UK, and all relevant subject identifying data and case background information. The request is assessed on receipt, to ensure that the requesting FIU has provided adequate information to enable a search to be completed. If there is insufficient data, the UK FIU will correspond with the requesting FIU to obtain the additional information, and only when this information is received will the request be processed. Records of all requests, including those initially rejected, are kept. The UK FIU referral policy has resulted in the successful exchange of information between UK law enforcement and foreign FIUs.

1360. Any requests for information on CFT matters are dealt with by the CFT staff within the FIU. Requests are prioritised in part relying on criteria within the UK policy on CFT. After the initial assessment is made to ensure a request meets the required standard grounds, a UK FIU case officer is assigned to the case. The request is then searched against the ELMER SAR database, commercial databases, financial databases and law enforcement databases to which UK FIU has access. If other agencies, national or international, have requested data on the same entities (and all parties agree), the UK FIU actively seeks opportunities to facilitate networking amongst the agencies involved.

1361. When a foreign FIU requests information from a U.K. law enforcement agency whose records UK FIU cannot access directly, the case is sent to the appropriate law enforcement agency representative at SOCA for completion of the relevant queries. The UK FIU does not have the authority to approve the dissemination of an outside law enforcement agency's information without prior approval. The decision to release any law enforcement information is left to the discretion of the agency from which the information originated.

1362. Where there is no information but a previous search from an Egmont partner is identified, the UK FIU will contact the FIU concerned and ask permission to forward their details to the requesting party. No action is taken without the express permission of the FIU in question.

1363. UK FIU also uses the Egmont network to request checks on behalf of SOCA as well as on behalf of other UK law enforcement. SOCA adheres to the Principles of Information Exchange, making use of the 'Egmont Request for Information' form to submit requests. SOCA specifies the originator of the request, the suspected misdemeanour, whether it is civil/criminal, an active case and whether the information is needed for court proceedings.

1364. The FIU's average time to respond to requests from an Egmont FIU has improved following the increase in staffing levels in 2006 resulting from its transfer to SOCA; it typically takes 22 days to respond to an Egmont request, although the incoming requests are assessed and prioritised daily to ensure that any request marked "urgent" takes precedence. In 2006, 80% of the requests were replied to in an average of 10 days. This is a continuously improving response, and exceeds the Egmont standards of 30 days. Processing time is influenced by the complexity of the case, and the amount of data that has to be analysed by the team before a response is formulated.

Requests received from Egmont FIUs

Year	2002	2003	2004	2005	2006
Requests received	353	529	465	366	525
Average response time (days)	54	63	110	148	22

Gateways for co-operation

1365. There are generally clear and effective gateways for the FIU to exchange information with foreign FIUs. UK legislation allows exchanges of information on a reciprocal basis; bilateral or multilateral agreements or arrangements such as an MOU; and exchanges through appropriate international or regional organisations or bodies such as Interpol or the Egmont Group of FIUs.

1366. There is no legislative requirement in the UK for the FIU to sign an MOU in order to exchange information with other FIUs. However, where such a prerequisite exists in a foreign jurisdiction, the UK FIU has the power to sign an MOU without any ministerial intervention. In accordance with the Egmont Statement of Purpose and Principles for Information Exchange between Financial Intelligence Units, the UK FIU exchanges information on a reciprocal basis with Egmont partners.

1367. The UK FIU continues to be proactive in the establishment of data sharing arrangements with Egmont partners, and has signed MOUs with the following jurisdictions: Australia, Canada, Colombia, Israel, Japan, Korea, Panama, Poland, Russia, Thailand, United Arab Emirates, and the USA. UK FIU is engaged in discussions to sign MOUs with other Egmont jurisdictions.

1368. The UK FIU also subscribes to FIU Net, an electronic system involving 15 EU countries which allows the exchange of basic identifying information. This is increasingly used as a pre-EGMONT check, prompting a full, formal EGMONT request if a search request results in a positive hit. SOCA responds to international subject information requests, as well as using this system to send out requests for information.

FIU.Net enquiries received

Year	Quantity
2002	89
2003	278
2004	383
2005	446
2006 (to 12 July)	275

1369. The number of FIU.Net enquiries has increased significantly over the years due primarily to the fact that member nations have more than doubled, from 7 to 15 nations, now consisting of: Belgium; Czech Republic; Estonia; Finland; France; Germany; Italy; Latvia; Luxembourg; Netherlands; Poland; Slovakia; Slovenia; Spain; and Ukraine, with further countries now awaiting set-up and connection to the FIU.Net system.

1370. The UK FIU is also involved in the European Suspicious Transaction Reporting Project, which has been established in order to promote the use of AWF SUSTRANS, the Europol analytical work file on money laundering in the EU. SOCA has given an undertaking to support the project working groups and is a member of the group which is responsible for producing a Statement of Intent.

1371. UK FIU is not prevented from exchanging information owing to any unduly restrictive conditions; UK FIU would not refuse co-operation to foreign counterparts on the grounds that the request involves fiscal matters. In all appropriate cases a referral to HMRC would be considered as the lead agency for such matters in the UK.

1372. There are appropriate safeguards to ensure that information received by the UK FIU is used only in an authorised manner. SOCA (and hence the FIU) follows the national standards for the recording and dissemination of intelligence as defined in the ACPO Codes of Practice (Appendix).

Law enforcement co-operation

1373. Law enforcement officials can co-operate with their foreign counterparts. Co-operation is not subject to unduly restrictive conditions. Nor would assistance be denied because they might also involve tax matters. SOCPA 2005 sections 34 and 35 ensure that requests for co-operation cannot be refused on the grounds of laws imposing secrecy or confidentiality requirements on financial institutions or DNFBPs.

1374. Information can be shared spontaneously rather than purely in response to a request, subject to a consideration of the proportionality of such a step. The UK authorities provided examples where local police, SOCA, and HMRC co-operated with foreign authorities to produce positive results, although there are no comprehensive statistics.

1375. Law enforcement officials are authorised to conduct inquires on behalf of their foreign counterparts. For SOCA, Section 5 of the SOCPA 2005 gives authorisation to conduct such investigations; SOCA has permission to act "at the request of any law enforcement agency, in support of any activities of that agency." The legislation also allows SOCA to "enter into arrangements for co-operating with bodies or persons (in the UK or elsewhere) who it considers appropriate in connection with the exercise of any of SOCA's functions." Additionally, "SOCA may furnish such assistance as it considers appropriate in response to requests made by any government or other body exercising functions of a public nature in any country or territory outside the UK."

1376. HMRC and UK police forces can also conduct enquiries on behalf of foreign counterparts on a Customs to Customs (or agencies with similar powers for taxation and previously drugs enquiries); or police to police basis. The conduits for such requests within HMRC are the International Mutual Assistance Treaty team (for MLA and MAA), Fiscal Crime Liaison Officer network or the Double Taxation Treaty Teams. Each LEA has an International Liaison Officer who receives foreign requests from Interpol. These may be either via Letter of request or the Police to Police route (this being the most common) and is a relatively common occurrence. The enquiries can be conducted by the LEA officers or by visiting officers from foreign jurisdictions supported by the LEA.

SOCA International Liaison Officers

1377. SOCA deploys a network of international liaison officers to act as key points of contact overseas between foreign and UK law enforcement. These officers tend to be based in UK embassies

and work closely with other representatives of UK government posted abroad. The network builds on bilateral and multilateral partnerships established by precursor agencies or by central departments such as the Home Office.

1378. The international liaison officers act as a national point of contact for all UK operational cooperation through Interpol, Europol, the Schengen Information System, other Schengen measures including cross-border surveillance, the European Arrest Warrant, and other capabilities. Responsibilities also include relevant input into, or engagement with, G8 processes, the European Police Chiefs Task Force, Eurojust, the UK magistrates' liaison network, and other bodies including UNODC. All this activity is coordinated centrally from SOCA.

1379. The development of this network means that international law enforcement agency co-operation at the level of regional police forces is more co-ordinated than in the past, with SOCA international liaison officers directly joining up relevant actors across borders for effective information sharing or joint investigation.

1380. Although the central co-ordination provided by SOCA is relatively new, international law enforcement co-operation by UK forces is not. There is a long tradition of forces using Home Office or other central departments or Foreign Office contacts to build their own operational relationships on the basis of need: a more case-by-case approach rather than the continuous relationship management that SOCA has introduced. UK authorities provided numerous cases of UK law enforcement authorities co-operating with foreign counterparts.

1381. In addition, SOCA is the UK Law Enforcement representative to the Camden Asset Recovery Inter Agency Network (CARIN). The CARIN group is an informal network of contacts and a cooperative group that considers all aspects of tackling the proceeds of crime. Members are drawn from law enforcement agencies and judicial authorities within principally but not exclusively EU member and EU applicant states.

1382. There are appropriate safeguards to ensure that information received by the UK FIU is used only in an authorised manner. SOCA follows the national standards for the recording and dissemination of intelligence as defined in the ACPO Codes of Practice (Appendix).

HMRC

1383. HMRC's Centre for Exchange of Intelligence ("CEI") deals with exchange of information overseas under the UK's bilateral double taxation agreements and EU Directives on mutual administrative assistance, mutual legal assistance, and taxation of savings. Under these treaties, information can only be exchanged by HMRC for taxation purposes although in cases of tax evasion there will usually also be a money-laundering offence. In the year to April 2006, CEI made 670 case-specific requests to overseas treaty partners and received 821 requests from overseas. It also exchanged over 12,000 spontaneous reports in addition to bulk 'automatic' exchanges of data such as under the EU Savings Directive.

1384. HMRC is frequently engaged in co-ordination with Home Office/HMT/FCO to develop AML efforts at the frontier. For example, two projects in respect of repatriation of sterling cash from UAE and from Belgium have recently been started.

1385. The UK is also part of the World Customs Organisation, which is an independent intergovernmental body whose mission is to enhance the effectiveness and efficiency of Customs administrations. The WCO hold regular meetings between its 169 members. The meetings allow members to exchange ideas, procedures, emerging trends etc.

1386. HMRC is seeking to sign a MOU with the Irish Revenue Commissioners that will allow them to proactively identify and exchange financial intelligence between the two departments. This would also

include predicate-related intelligence that is of tax or financial (money laundering) interest. HMRC proactively contributed details of UK cash seizures to Europol Project SATURN. This Europol led Project, involving seven Member States, was focused on the movement of drugs related criminal cash. HMRC deploys 18 Fiscal Liaison Officers overseas; and has a range of MOUs and Double Taxation Treaties internationally.

1387. HMRC receives between 1,500 and 2,000 mutual assistance requests a year, and makes approximately 1,000 outgoing requests in the same period. A summary of the requests is shown in the table below. The statistics cover the work of the "International Mutual Assistance Team" (IMAT) and the "Fiscal Crime Liaison Officer" (FCLO) network - both part of HMRC.

Year	MAA Requests IN IMAT	MAA Requests IN FCLO Network	MAA Requests Out IMAT	MAA Requests Out FCLO Network	MAA Requests Closed IMAT	MAA Requests Closed FCLO Network
2004/2005	20	44	22	30	8	1
2005/2006	25	63	117	37	59	6

1388. An average response time for incoming requests was approximately 2.75 months compared to 3 months in respect of outgoing requests. The vast majority of the FCLO's requests relate to information exchange, compared to IMAT who deal with evidential requests. In respect of informal Officer-to-Officer contact the Department discourages this, as all requests should be sent via IMAT or FCLO network. HMRC use SOCA to make requests via Interpol or Europol, which are housed within SOCA and staffed by their officers, but independent from them.

1389. UK authorities reported that it is impossible to provide detailed statistics on police to police cooperation, since this is mainly done through informal channels. Intelligence Reports forwarded to, or received from, international partners are not spilt into crime categories - AML/CTF, drugs, illegal immigration etc, and it is not possible to estimate the statistics on this type of information, the number of daily telephone calls or mutual visits which take place to further intelligence gathering and information flows.

Regulatory Co-operation

1390. The FSA can provide a wide range of assistance to international counterparts. The FSA is able to share information with foreign counterparts pro-actively and on request. The exchange of information by the FSA is not subject to disproportionate or unduly restrictive conditions. The FSA would not refuse co-operation to foreign counterparts on the grounds that the request involves fiscal matters.

1391. Under FSMA, Part XXIII, section 354 the FSA is under a statutory duty to co-operate with other persons with similar functions to the FSA or in relation to the prevention or detection of financial crime.

1392. The FSA is authorised to conduct inquiries on behalf of foreign counterparts. Under FSMA, Part XI, section 169 the FSA may appoint investigators (without a court order) at the request of an overseas regulator. An investigator appointed under this section has the power to require a person who is neither the subject of the investigation nor a person connected with the person under investigation to attend before the investigator at a specified time and place and answer questions or otherwise provide such information as the investigator may require for the purposes of the investigation. Such a requirement may only be imposed if the investigator is satisfied that it is necessary or expedient for the purposes of the investigation.

1393. The FSA's policy for exercising its power to conduct investigations to assist overseas authorities is set out in the FSA Handbook, Enforcement Sourcebook, Chapter 2, section 2.8.

1394. The FSA is generally able to provide assistance in a rapid, constructive and effective manner. The FSA follows CESR ("Committee of European Securities Regulators") Service Level Guidance which states:

> Requests should be acknowledged within 5 to 7 days of receipt…..The processing of requests…. should be aimed at producing responses …as quickly as possible….. The maximum turnaround time for requests should be no more than four to eight weeks after receipt of the request depending on the complexity of the request and the necessity to involve third parties or another competent authority.

1395. The FSA tracks requests from the moment they are received to the moment they are closed. The time taken can vary from days to months, depending on the nature of the assistance requested. For example, straightforward information requests can be very quick to deal with, whereas requests to obtain and disclose testimony and other material can be very complex and time consuming. The FSA seeks to comply with the CESR Service Level Guidelines when dealing with all requests for assistance received by the FSA and the great majority are closed within the CESR recommended maximum turnaround time.

1396. The FSA reported that it had acknowledged receipt of every foreign request received in 2005 and 2006 (up to the time of the on-site visit) within five working days. In addition, FSA provided the following statistics on turnaround time for queries received.

Turnaround

	2005-2006	2006-present
Average number of days to Response to very simple requests (e.g. goodstanding)	15	13
Average days taken to respond to simple requests (e.g. transactional data)	34	32
average days taken for complex requests	77	85

Gateways for co-operation

1397. In order to determine the levels of co-operation with its counterparts the FSA assesses the reliability and legal comparability of other regulators. European Union members are already legally equivalent and the FSA is required to co-operate with them fully and proportionately under FSMA. For non-EEA regulators the FSA will assess whether the counterparts are legally equivalent i.e. the confidentiality regime is subject to standards of "professional secrecy at least equivalent" to those that apply to the FSA as the competent authority for EU Single Market Directives; and is sound and reliable.

1398. The FSA is a signatory to a number of bilateral and multilateral Memoranda of Understanding with foreign counterparts dealing with mutual assistance. This includes the International Organisation of Securities Commissions ("IOSCO") "MMOU Appendix A" signatories concerning enforcement consultation and co-operation and the exchange of information to which there are now thirty signatories worldwide. The FSA is also an active member of a number of international organisations such as Committee of the European Securities Regulators (CESR) which also promote mutual assistance between their members.

1399. The following list consists of the active bilateral MOUs the FSA has agreed with overseas authorities since 1 December 2001(N2), and selected pre N2 MOUs, where the parties have agreed to publication.

FSA Bilateral MOUs	
Country	**Authority**
Australia	Australian Prudential Regulation Authority Australian Securities and Investments Commission
Bermuda	Bermuda Monetary Authority
Canada	Canadian Office of the Superintendent of Financial Institutions
Dubai	Dubai Financial Services Authority
Gibraltar	Gibraltar Financial Services Commission and the Financial Services Commissioner
Guernsey	Guernsey Financial Services Commission
Hong Kong	Hong Kong Insurance Authority
Isle of Man	Isle of Man Financial Supervision Commission
Jersey	Jersey Financial Services Commission
Singapore	Monetary Authority of Singapore
South Africa	South African Reserve Bank
Switzerland	Swiss Federal Banking Commission Swiss Federal Office of Private Insurance
USA	Commodity Futures Trading Commission Federal Deposit Insurance Corporation Federal Reserve Board Securities and Exchange Commission Office of the Comptroller of the Currency Office of Thrift Supervision

1400. The FSA has safeguards to ensure that information received is used only in an authorised manner. In relation to FSA staff, FSMA, Part XXIII, section 348, indicates that confidential information must not be disclosed in an inappropriate manner. See also the discussion under Recommendation 4, which sets out the relevant parts of the UK Data Protection Act regime.

FSA statistics

1401. The following statistics on international requests received by the FSA in 2005 and 2006 illustrate the extent to which the FSA assists its international counterparts. Although no cases are mentioned as specifically relating to money laundering, it is certain that many of the cases in which assistance is provided will have a money laundering element to them, especially those cases relating to market manipulation, insider dealing and fraud.

	2005	**2006 (up to 31 July)**
Total number of requests	***306***	***206***
Type of assistance sought:		
Administrative assistance	3%	1
Bank records	4%	4
Goodstanding	10%	14
Interview(s)	3%	7
Investigation	0%	1
Regulatory information	21%	7
Transaction data	44%	46
other	13%	19
Breakdown of requests by sector:		
Banking	1%	0%
Insurance	2%	1%
Securities	92%	70%
Other	5%	28%
Breakdown of MOUs used:		
Bi-lateral	6%	11%
CESR	39%	36%
IOSCO	40%	40%

Not specified	15%	36
Geographical breakdown:		
EU only	67%	69%
Non-EU	33%	31%

6.5.2 Recommendations and Comments

1402. Overall, the UK has systems in place for adequate administrative cooperation, equally for the FIU, law enforcement, and financial supervisors. However, authorities should keep more comprehensive statistics for law enforcement cooperation, and for HMRC whether the requests were granted or refused, so as to more effectively monitor the effectiveness of their systems for international co-operation.

6.5.3 Compliance with Recommendation 40 and Special Recommendation V

	Rating	Summary of factors relevant to s.6.5 underlying overall rating
R.40	**C**	
SR.V	**C**	

7. OTHER ISSUES

7.1 Resources and statistics

1403. 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 the boxes showing the rating and the factors underlying the rating.

	Rating	Summary of factors relevant to Recommendations 30 and 32 and underlying overall rating
R.30	**LC**	• Overall, the allocation of HMRC's resources is a concern, as current resources are focused on the MSBs with the largest turnover which does not adequately address the smaller MSBs which might be of higher risk for ML/FT. • The FIU should increase resources in order to meet commitments made under recent government reviews.
R.32	**LC**	• MLA requests: There are no statistics on the breakdown of the offences concerned in each case (i.e., ML, predicate offences, or FT), nor on the number granted and refused, or the time required to respond. • No comprehensive statistics for CFT convictions. • The FIU does not have precise figures on the number of SARs analysed and disseminated. • The UK does not maintain comprehensive statistics on cross-border disclosures concerning suspected ML/FT.

TABLES

Table 1: Ratings of Compliance with FATF Recommendations
Table 2: Recommended Action Plan to improve the AML/CFT system
Table 3: Authorities' Response to the Evaluation (if necessary)

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).

Compliant	The Recommendation is fully observed with respect to all essential criteria.
Largely compliant	There are only minor shortcomings, with a large majority of the essential criteria being fully met.
Partially compliant	The country has taken some substantive action and complies with some of the essential criteria.
Non-compliant	There are major shortcomings, with a large majority of the essential criteria not being met.
Not applicable	A requirement or part of a requirement does not apply, due to the structural, legal or institutional features of a country e.g. a particular type of financial institution does not exist in that country.

Forty Recommendations	Rating	Summary of factors underlying rating
Legal systems		
1. ML offence	**C**	
2. ML offence – mental element and corporate liability	**C**	
3. Confiscation and provisional measures	**C**	
Preventive measures		
4. Secrecy laws consistent with the Recommendations	**C**	
5. Customer due diligence	**PC**	• JMLSG Guidance only partly deals with identification where there are doubts regarding previously obtained customer identification data. There is no requirement in law or regulation. • It is not specifically required by law or regulation to verify that any person purporting to act on behalf of the customer is so authorised. • There is no requirement in law or regulation to: identify the beneficial owner or take reasonable measures to verify the identity of the beneficial owner, or to determine who are the natural persons that ultimately own or control the customer, including those persons who exercise ultimate effective control over a legal person or arrangement. • The wording of the guidance does not create an obligation to *verify* beneficial ownership in any situation; there is no obligation to verify the beneficial owner before or during the course of establishing a business relationship or conducting transactions for occasional customers. • There is no explicit obligation to obtain information on the purpose and nature of the business relationship in the UK in all cases. • A requirement to conduct ongoing monitoring does not exist in law and regulation. Nor is there a general requirement that ongoing due diligence should include scrutiny of transactions undertaken throughout the course

		of that relationship to ensure that the transactions being conducted are consistent with the institution's knowledge of the customer, their business and risk profile, and where necessary, the source of funds. The limited procedures for on-going due diligence in the guidance only apply for higher-risk scenarios. • There is no general obligation that documents, data or information collected under the CDD process be kept up-to-date and relevant by undertaking reviews of existing records. • There is no general requirement to take additional steps when there is a higher risk scenario, whatever that higher risk scenario may be, although the Guidance makes it clear that this is expected. • Provisions for reduced/simplified CDD are overly broad—providing a full exemption from CDD in respect of financial institutions from certain countries (not just reduced); this is not based on an actual risk assessment, either by the UK itself or by the financial institution, which would confirm the assumption of low risk. • The exemption from CDD within the context of a business relationship could still apply when money laundering is suspected. • Once the business relationship has commenced, it is not a specific requirement to terminate the business relationship if proper CDD cannot be conducted. • There is no enforceable obligation to apply CDD to existing customers on the basis of materiality and risk. • A number of measures are mentioned only in JMLSG guidance and have no significance in respect of MSBs or the non-supervised sector other than as guidance.
6. Politically exposed persons	**NC**	No currently enforceable obligations with regards to PEPs.
7. Correspondent banking	**NC**	No currently enforceable obligations pertaining to correspondent banking.
8. New technologies & non face-to-face business	**C**	
9. Third parties and introducers	**PC**	• The information provided concerning the CDD process makes only a limited reference to beneficial owners (i.e. for certain businesses and not all customers). • There is no enforceable requirement that the financial institutions be satisfied that the introducer will make ID and other relevant documentation available upon request. • Financial institutions are not required to satisfy themselves that the third party is regulated and supervised (in accordance with Recommendation 23, 24 and 29), and has measures in place to comply with, the CDD requirements. • In determining in which countries the third party that meets the conditions can be based, competent authorities only to some extent take into account information available on whether those countries adequately apply the FATF Recommendations.
10. Record keeping	**C**	
11. Unusual transactions	**PC**	• There is no specific obligation to pay special attention to all complex, unusual large transactions, or unusual patterns of transactions, that have no apparent or visible economic or lawful purpose. The expectation in guidance only covers the JMLSG covered part of the financial sector. • There is no specific requirement to examine as far as possible the background and purpose of such transactions and to set forth findings in writing.
12. DNFBP – R.5, 6, 8-11	**PC**	• *Applying R.5:* Similar deficiencies as indicated under R.5 (no law or regulation to require CDD when there are doubts about the previously obtained data; no requirements to identify beneficial owner, etc.). Some CDD requirements are in guidance, which are not legally binding. • For casinos, CDD is not required above the 3,000 euro threshold, and it is not clear that casinos can adequately link the incoming customers to

		individual transactions. • Estate agents are not required to identify the buyer. • *Applying R.6:* No requirements with regard to PEPs that will apply to any of the DNFBPs. • *Applying R.8:* For DNFBPs, there is no obligation to have policies in place or take such measures as may be necessary to prevent the misuse of technological developments in ML/FT. • *Applying R. 9:* For DNFBPs, there are currently no enforceable obligations with regard to introduced business. • *Applying R.10:* Certain record-keeping requirements in the FSA rules and JMLSG Guidance do not apply to DNFBPs: no requirement that records must be sufficient to permit reconstruction of individual transactions so as to provide, if necessary, evidence for prosecution of criminal activity; no explicit requirement in law or regulation to maintain records of account files. • *Applying R.11*: For DNFBPs, there is no specific obligation to pay special attention to all complex, unusual large transactions, or unusual patterns of transactions, that have no apparent or visible economic or lawful purpose. • There is no requirement to examine as far as possible the background and purpose of such transactions and to set forth findings in writing. • No requirement to keep such findings available for competent authorities and auditors for at least five years.
13. Suspicious transaction reporting	**C**	
14. Protection & no tipping-off	**C**	
15. Internal controls, compliance & audit	**LC**	• There is not a direct requirement for firms to maintain an independent audit function. • Some minor legal issues (coverage of all MLRO duties under MLR 7, coverage of the full range of training requirements under MLR 3 (1)(c)) are of concern; particularly related to those financial sector entities who are only subject to the MLRs, without further rules or guidance. • No requirement for screening procedures for all employees.
16. DNFBP – R.13-15 & 21	**LC**	• There is no specific requirement to designate an AML/CFT compliance officer at the management level; nor are there any requirements for screening procedures. • There is no requirement for DNFBPs to give special attention to business with countries which do not sufficiently apply FATF Recommendations, nor is there a legal obligation to examine as far as possible the background and purpose of such transactions, and make written findings available for authorities.
17. Sanctions	**LC**	• The number of FSA disciplinary sanctions (since 2001) seems relatively low: 14 enforcement actions including warnings and the cancellation of one licence. • Administrative sanctions of HMRC do not extend to directors and senior managers.
18. Shell banks	**PC**	• There is no enforceable obligation for financial institutions not to enter into, or continue, correspondent banking relationships with shell banks. • No obligation to require financial institutions to satisfy themselves that respondent financial institutions in a foreign country do not permit their accounts to be used by shell banks**.**
19. Other forms of reporting	**C**	
20. Other NFBP & secure transaction techniques	**C**	
21. Special attention for higher risk countries	**PC**	• There is no requirement for financial institutions to give special attention to business with countries which do not sufficiently apply FATF Recommendations. MLR 28 only covers FATF countermeasures, and the

		guidance of JMLSG only covers part of the financial sector. • No specific requirement to examine as far as possible the background and purpose of such transactions, and make written findings available for authorities.
22. Foreign branches & subsidiaries	**NC**	• There are currently no requirements relating to foreign branches and subsidiaries.
23. Regulation, supervision and monitoring	**LC**	• The impact assessment method (to determine the level of supervision) does not adequately take into account AML/CFT risk, and therefore there are some concerns about the adequacy of supervision for small firms. • Consumer credit, financial leasing, guarantees and commitments, brokers, factoring, safe-keeping and administration are neither supervised nor expected to comply with professional guidance. • For most on-site assessments (high and medium impact firms), there is an over reliance on interview-based visits without sample testing, and for the medium firms the FSA does not receive any information related to the implementation of the AML/CFT between two on-site visits. • There are some minor concerns about the current on-going monitoring for MSBs.
24. DNFBP - regulation, supervision and monitoring	**PC**	• Currently no AML/CFT supervision for real estate agents or TCSPs that are not legal or accountancy professionals, or accountants that are not members of professional bodies (approximately 40,000). • Current sanctions for Gambling Commission are not yet adequate, although this will change once the Gambling Act comes into force in September 2007. • Notaries in England and Wales are not supervised for AML/CFT (unless they are also lawyers, or accountants that are members of professional bodies).
25. Guidelines & Feedback	**C**	
Institutional and other measures		
26. The FIU	**LC**	• There are concerns with regard to the effectiveness and workability of the current consent process, especially with regard to what is often interpreted as consent for follow-up transactions from the same customer. • The FIU does not conduct sufficient pro-active analysis on SARs; overly relying on individual LEAs to conduct their own analysis could reduce the importance of the UK FIU as the national center for receiving, analysing, and disseminating SARs; and could ultimately impede the FIU's analytical functions and its own ability to give guidance and to develop its expertise about ML/FT methods, trends and typologies. • The FIU does not publish periodic reports including SARs statistics, typologies and trends as well as information regarding its activities.
27. Law enforcement authorities	**C**	
28. Powers of competent authorities	**C**	
29. Supervisors	**LC**	• With regard to entities that are not subject to the FSA regime (such as consumer credit and leasing) there is not an authority with adequate powers of inspection and sanction for AML/CFT. • For MSBs, sanctions cannot generally be applied to directors and senior managers.
30. Resources, integrity and training	**LC**	• Overall, the allocation of HMRC's resources is a concern, as current resources are focused on the MSBs with the largest turnover which does not adequately address the smaller MSBs which might be of higher risk for ML/FT. • The FIU should increase resources in order to meet commitments made under recent government reviews.
31. National co-operation	**C**	

32. Statistics	**LC**	• MLA requests: There are no statistics on the breakdown of the offences concerned in each case (i.e., ML, predicate offences, or FT), nor on the number granted and refused, or the time required to respond. • No comprehensive statistics for CFT convictions. • The FIU does not have precise figures on the number of SARs analysed and disseminated. • The UK does not maintain comprehensive statistics on cross-border disclosures concerning suspected ML/FT.
33. Legal persons – beneficial owners	**PC**	• While the investigative powers are generally sound, there are not adequate measures in place to ensure that there is adequate, accurate and timely information on the beneficial ownership and control of legal persons that can be obtained or accessed in a timely fashion by competent authorities. • Information on the companies registrar pertains only to legal ownership/control (as opposed to beneficial ownership) and is not verified and is not necessarily reliable. • Although the use of share warrants to the bearer is reportedly rare in the UK, there are no specific measures taken to ensure that they are not misused for money laundering other than the inclusion of "cash" in the POCA description.
34. Legal arrangements – beneficial owners	**PC**	• While the investigative powers are generally sound, there are not adequate measures in place to ensure that there is adequate, accurate and timely information on the beneficial ownership and control of legal arrangements that can be obtained or accessed in a timely fashion by competent authorities. • There is no standardisation of beneficial ownership data held, and the nature of information collected will vary with the provision of any relevant guidance. • Providers of trust services who are not lawyers, or accountants that are members of professional bodies, are not monitored for their AML/CFT obligations and so it is not clear how reliable the information they maintain would be.
International Co-operation		
35. Conventions	**C**	
36. Mutual legal assistance (MLA)	**LC**	• There are concerns about the ability of the UK authorities (excluding Scotland) to handle mutual legal assistance requests in a timely and effective manner; the UK is presently unable to ensure timely and effective turnaround of all routine requests.
37. Dual criminality	**C**	
38. MLA on confiscation and freezing	**C**	
39. Extradition	**C**	
40. Other forms of co-operation	**C**	
Nine Special Recommendations	**Rating**	**Summary of factors underlying rating**
SR.I Implement UN instruments	**C**	
SR.II Criminalise terrorist financing	**C**	
SR.III Freeze and confiscate terrorist assets	**C**	
SR.IV Suspicious transaction reporting	**C**	
SR.V International co-operation	**C**	
SR VI AML requirements for money/value transfer services	**LC**	• Minor concerns about the effectiveness of the sector's supervision. • There are not adequate sanctions that can be used against directors and

		senior managers. • There are some concerns with regard to the extent that certain Recommendations apply: customer identification such as a lack of beneficial ownership requirements (R.5), PEPs (R. 6), and transaction monitoring (R.11, 21).
SR VII Wire transfer rules	**PC**	• The derogation set out in the EU regulation for wire transfers within the EU (classified as domestic transfers) is not in compliance with the FATF requirements under SR.VII. [32] • The sanctions regime is not effective or dissuasive; since no sanctions can currently be applied it is doubtful as to whether any "enforceable obligations" are in place before 15 December 2007. • In terms of effectiveness, there are doubts about the current implementation of the very recent EU requirements, including the requirement to have in place effective risk-based procedures for identifying and handling wire transfers that are not accompanied by complete originator information, and about the existence of an effective compliance monitoring of financial institutions.
SR.VIII Non-profit organisations	**LC**	• Northern Ireland not covered relating to registration, transparency and supervision of charities.
SR.IX Cross Border Declaration & Disclosure	**LC**	• UK authorities do not have the authority to detain cash or bearer negotiable instruments purely for a false disclosure. • Currently, there is no requirement to retain, at a minimum, the amount and identification of the bearer where there is a false disclosure or maintain this data in the event of a suspicion of ML/FT, although this is done in practice if the amount is £1,000 or more. • The system whereby detailed information on cross-border disclosures is available to the FIU is not fully comprehensive.

[32] The FATF decided at the June 2007 Plenary to further consider this subject.

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	
2.1 Criminalisation of Money Laundering (R.1 & 2)	
2.2 Criminalisation of Terrorist Financing (SR.I)	• It is recommended that the UK authorities make the link between the terrorist financing offences under the TACT and the Conventions and Protocols referred to in the Annex to the TF Convention more explicit to remove any doubt which there may be in this regard. • UK authorities should also improve their system for statistics for FT prosecutions and convictions.
2.3 Confiscation, freezing and seizing of proceeds of crime (R.3)	• The UK should consider enacting a broad stand-alone provision enabling seizure and confiscation of instrumentalities of crime, including in cases when there has been no conviction. • The UK authorities should review the current arrangements in civil recovery cases both at the legislative and operational level with a view to making the process more effective and timely, including the better facilitation of international cooperation. ARA is encouraged to take a more aggressive approach in pushing litigation forward to final forfeiture orders.
2.4 Freezing of funds used for terrorist financing (SR.III)	• Systematic outreach to DNFBPs should be made more proactive. The UK should enhance its communication, guidance and compliance monitoring efforts for DNFBPs.
2.5 The Financial Intelligence Unit and its functions (R.26)	• The UK FIU should increase its analytical capabilities, in order to maintain its role as the national center for receiving, analysing and disseminating SARS, as well as its expertise in analysing and developing ML/FT typologies. • The UK FIU should continue to increase its staff, especially its analytical staff in the Intelligence Team and other teams, in line with the objective set out in the SARs ("Lander") review. • The UK authorities should continue to work with the private sector to develop a more workable and efficient "consent" system. • The UK FIU should be given more timely and direct access to a number of databases. • The UK FIU should continue to ensure that its functions and authorities remain fully independent from the non-FIU functions carried out by the other parts of SOCA. • The FIU should keep more comprehensive statistics on the total number of SARs analysed and disseminated.
2.6 Law enforcement, prosecution and other competent authorities (R.27 & 28)	
2.7 Cross Border Declaration & Disclosure	• However, authorities should have a more direct power to detain cash purely for a false disclosure or declaration when transporting cash or monetary instruments into or out of the UK. • Authorities should retain, at a minimum, the amount and identification the bearer in amount of disclosures where there is a false disclosure and in the event of a suspicion of ML/FT (even if there is not a seizure).
3. Preventive Measures – Financial Institutions	
3.1 Risk of money laundering or terrorist financing	
3.2 Customer due diligence, including	• ***Recommendation 5:*** the UK should put the following obligations into law or

enhanced or reduced measures (R.5 to 8)	regulation: (i) to identify the beneficial owner and take reasonable measures to verify the identity of the beneficial owner (for all customers); (ii) for legal persons, to determine who are the natural persons that ultimately own or control the customer; (iii) to verify that any person purporting to act on behalf of a customer is so authorised; and (iv) a general requirement for conducting ongoing due diligence. • The UK authorities should clarify that CDD is still required in the context of an on-going business relationship if money laundering/FT are suspected (rather than just for "one-off" transactions.) Also, any reduction or exemption of CDD requirements should be based on a specific analysis and identification of a proven low risk. • It should also be specifically required by law, regulation, or other directly enforceable means: (i) to verify the beneficial owner before or during the course of establishing the business relationship; (ii) once the business relationship has commenced, to terminate the business relationship if proper CDD cannot be conducted; and (iii) to apply CDD to existing customers on the basis of materiality and risk. • UK authorities should make more clearly enforceable obligations: to obtain information on the intended purpose and nature of the business relationship; to specify the procedures for on-going due diligence in compliance with the FATF Recommendations; to require that financial institutions maintain documents and other CDD data up-to-date and relevant by undertaking regular reviews. • ***Recommendation 6:*** Regarding PEPs, the UK authorities should create enforceable obligations in this regard as soon as possible. • ***Recommendation 7:*** The UK authorities should make enforceable obligations to cover correspondent banking.
3.3 Third parties and introduced business (R.9)	• UK authorities should make more explicit requirements for financial institutions to immediately obtain from the third party all the necessary information concerning certain elements of the CDD process, to take adequate steps to satisfy themselves that copies of identification data and other relevant documentation relating to CDD requirements will be made available from the third party upon request without delay, and for financial institutions to accept introducers pursuant to its assessment of AML/CFT adequacy.
3.4 Financial institution secrecy or confidentiality (R.4)	
3.5 Record keeping and wire transfer rules (R.10 & SR.VII)	• Credit institutions should adopt effective risk-based procedures for identifying and handling wire transfers that are not accompanied by complete originator information. • By December 2007, the UK authorities should adopt effective, proportionate and dissuasive sanctions applicable to infringements of the provision laid down on the EU Regulation.
3.6 Monitoring of transactions and relationships (R.11 & 21)	• UK authorities should adopt more specific requirements to monitor all complex, unusual large transactions, etc, and to make out findings in writing. • The UK authorities should adopt more specific requirements dealing with monitoring transactions involving certain countries and making findings in writing.
3.7 Suspicious transaction reports and other reporting (R.13-14, 19, 25 & SR.IV)	• The UK should continue to work with the private sector to make the consent process more efficient and effective.
3.8 Internal controls, compliance, audit and foreign branches (R.15 & 22)	• There should be a more direct requirement for firms to maintain an independent audit function. • The UK should also address other minor legal issues (coverage of all MLRO duties under MLR 7), coverage of the full range of training requirements under MLR 3 (1)(c); particularly related to those financial sector entities who are only subject to the MLRs, without further rules or guidance. • The UK should consider a general requirement to screen all employees. • The UK should also adopt more specific rules relating to foreign branches

	and subsidiaries in relation to the requirements of Recommendation 22.
3.9 Shell banks (R.18)	• Authorities should create more directly enforceable obligations for financial institutions not to enter into, or continue, correspondent banking relationships with shell banks and to require financial institutions to satisfy themselves that respondent financial institutions in a foreign country do not permit their accounts to be used by shell banks.
3.10 The supervisory and oversight system - competent authorities and SROs. Role, functions, duties and powers (including sanctions) (R.23, 29, 17 & 25)	• ***Recommendation 17***: authorities should consider targeting ML/FT more specifically. • HMRC should be given more direct powers to take against directors and senior management for AML/CFT breaches. • ***Recommendation 23:*** For smaller firms, the UK authorities should adjust their risk assessment basis for determining the level of supervision in order to take more into account the actual AML/CFT risks. • Supervision for certain entities currently categorised as "small firms" should be strengthened, especially small banks (even if they are supervised more closely than the other small firms), securities brokers/investment managers, and insurance firms which are Core Principles institutions. • It is recommended that consumer credit, financial leasing, guarantees and commitments, brokers, factoring, safe-keeping and administration) be brought into an appropriate AML/CFT supervisory framework. • When conducting on-site risk assessments, the FSA should more often and thoroughly review files and conduct more sample testing. In addition, the supervisory framework would be strengthened if ongoing monitoring required financial institutions to regularly send AML regulatory reports to the FSA so as to keep aware of the firm's AML/CFT issues and allow for some analysis of these reports. • To more effectively perform its tasks, HMRC should deploy a broader allocation of resources at all levels of ML /FT risk. • ***Recommendation 29***: The UK authorities should designate an authority (or authorities) with adequate powers of inspection, monitoring, and sanction with regard to those activities currently not supervised by FSA (i.e., consumer credit, leasing, etc).
3.11 Money value transfer services (SR.VI)	• It is recommended to increase the resources of the HMRC as well as its powers of sanction to enhance the supervision of MSBs.
4. Preventive Measures – Non-Financial Businesses and Professions	
4.1 Customer due diligence and record-keeping (R.12)	• The UK should adopt adequate measures for R.6., 9, 11 for DNFBPs. The UK should also require that the estate agents identify the buyer of real estate. • Similarly, the UK should adopt stronger CDD measures as described under Recommendation 5. • UK authorities should ensure that CDD in casinos is linked to transactions above EUR 3,000 as there is a risk that relying on current ad hoc arrangements by casinos to link identification on the door with transactions undertaken inside the casino could potentially give rise to a situation in which it might not be possible to trace a particular transaction to a particular individual.
4.2 Suspicious transaction reporting (R.16)	• The UK should strengthen the requirements for internal controls and for paying special attention to business and transactions involving jurisdictions that do not adequately apply the FATF Recommendations.
4.3 Regulation, supervision and monitoring (R.24-25)	• It is highly recommended that real estate agents and trust and company service providers become subject to adequate AML/CFT supervision. • Authorities should also bring the Gambling Act 2005 into full force so as to augment the range of sanctions available to the Gambling Commission. • UK authorities should ensure that accountants that are not part of professional bodies become subject to adequate monitoring for AML/CFT. • It is noted that a system for supervision of compliance by notaries public in England and Wales who are not also practicing as solicitors will be introduced; the UK authorities are encouraged to continue with this process

	at a steady pace.
4.4 Other non-financial businesses and professions (R.20)	
5. Legal Persons and Arrangements & Non-Profit Organisations	
5.1 Legal Persons – Access to beneficial ownership and control information (R.33)	• It is recommended that the UK authorities review the current system to determine ways in which adequate and accurate information on beneficial ownership may be available on a timely basis to law enforcement authorities • UK authorities should implement the provisions of the new Companies Act as soon as possible and are encouraged to implement the planned changes in practice at Companies House. • The UK authorities should consider the justification and need for the on-going existence of bearer shares given the apparent lack of demand and potential risk of abuse.
5.2 Legal Arrangements – Access to beneficial ownership and control information (R.34)	• The UK 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.
5.3 Non-profit organisations (SR.VIII)	• Authorities should develop appropriate procedures for registration, transparency, supervision and investigation of charities in Northern Ireland as soon as possible.
6. National and International Co-operation	
6.1 National co-operation and coordination (R.31)	
6.2 The Conventions and UN Special Resolutions (R.35 & SR.I)	
6.3 Mutual Legal Assistance (R.36-38 & SR.V)	• It is recommended that the UKCA institute a far more pro-active approach to monitoring progress on execution of requests and ensuring a timely and effective response. Case officers within the UKCA should assume overall responsibility for each request and the case officer should be centrally and actively engaged in dialogue between the allocated law enforcement agency and the requesting jurisdiction concerning execution of the request on a regular and unprompted basis. The focus should shift from a "case allocation" approach to a pro-active "case monitoring and completion" approach. • The UK authorities should improve mechanisms for overall co-ordination of execution of requests, both domestically with its own law enforcement agencies and externally with requesting jurisdictions. • The UKCA should ensure that clear lines of communication exist with established points of contact between itself and the law enforcement officer responsible for execution of the request, as well as between itself and the requesting jurisdiction. • The UK authorities are encouraged to continue their bilateral dialogue with certain partner countries to examine perceived problems and work towards resolution. • If deemed necessary to improve implementation issues identified, the Home Office should consider providing additional resources to the UKCA, particularly by way of additional manpower or case officers to support the workload, which continues to increase. The additional recruitment of lawyers to become more actively involved in execution the requests should be considered.
6.4 Extradition (R.39, 37 & SR.V)	• The UK authorities are encouraged to keep operation of procedures under the 2003 Act under active review to ensure that a proper balance is achieved between the interests of the requesting state in securing the fugitive's return and the rights of the fugitive in that process.
6.5 Other Forms of Co-operation (R.40 & SR.V)	

7. Other Issues	
7.1 Resources and statistics (R. 30 & 32)	• The UK authorities should continue to implement the recommendations of the various AML/CFT reviews.

ANNEXES

Annex 1: List of abbreviations and acronyms

ACPO	Association of Chief Police Officers
ARA	Assets Recovery Agency
ATCS	Anti-Terrorism Crime and Security Act 2001
BCEW	Bar Council of England and Wales
BCNI	Bar Council of Northern Ireland
Cash Controls Regulation	EC Regulation 1889/2005
CICFA	Concerted Inter-Agency Criminal Finances Action group (a.k.a. the Asset Recovery Working Group (ARWG))
CLC	Council for Licensed Conveyancers
COPFS	Scottish Crown Office and Procurator Fiscal Service
CPS	Crown Prosecution Service
CRU	Civil Recover Unit (Scotland)
FI	Financial Investigator
DPPNI	Department of Public Prosecutions Northern Ireland
FIN-NET	Financial Crime Information Network
FLA	Finance and Leasing Association
FSA	Financial Services Authority
FSMA	Financial Services and Markets Act 2000
JARD	Joint Asset Recovery Database
JMLSG	Joint Money Laundering Steering Group
HMRC	HM Revenue and Customs
HVDs	High Value Dealers
LEAs	Law Enforcement Authorities (generic term for police & other agencies)
LSEW	Law Society of England & Wales
LSNI	Law Society of Northern Ireland
LSS	Law Society of Scotland
MLRs	Money Laundering Regulations 2003
MLAC	Money Laundering Advisory Committee
MSB	Money Service Business
MTIC	Missing Trader Intercommunity Fraud
NCIS	National Criminal Intelligence Service
NTFIU	National Terrorist Finance Investigation Unit
OCTF	Organised Crime Task Force
OFT	Office of Fair Trading
OGCs / OCEs	Organised Crime Groups / Organised Crime Entities
OSCR	Office of the Scottish Charities Regulator
PPSNI	Public Prosecution Service Northern Ireland
PSNI	Police Service Northern Ireland
POCA	Proceeds of Crime Act 2002
RARTs	Regional Asset Recovery Teams
RCPO	Revenue and Customs Prosecution Office
SARs	Suspicious Activity Reports
SCDEA	Scottish Crime and Drug Enforcement Agency
SFO	Serious Fraud Office
SOCA	Serious and Organised Crime Agency
TACT	Terrorism Act 2000
TFAG	Terrorist Finance Action Group
"Third Money Laundering Directive" / "Third Directive"	Directive 2005/60/EC. EU led AML/CFT directive to be implemented into UK law by December 2007.
UNODC	United Nations Office of Drugs and Crime
UKCA	United Kingdom Central Authority (MLA and extradition)

Annex 2: Details of all bodies met on the on-site mission: Ministries, other government authorities or bodies, private sector representatives and others

Ministries

- Her Majesty's Treasury (HMT)
- Home Office
- Foreign and Commonwealth Office (FCO)
- Department for Trade and Industry (DTI)

Criminal justice and operational agencies

- Serious Organised Crime Agency (SOCA), including the UK Financial Intelligence Unit (UK FIU)
- Her Majesty's Revenue and Customs (HMRC)
- Crown Prosecution Service (CPS)
- Revenue and Customs Prosecution Office (RCPO)
- Public Prosecution Service Northern Ireland (PPSNI)
- Assets Recovery Agency (ARA)
- Scottish Crown Office and Procurator Fiscal Service (COPFS)
- City of London Police
- Association of Chief Police Officers (ACPO)
- Scottish Drug Enforcement Agency (SCDEA)
- UK Central Authority
- National Terrorist Finance Investigation Unit (NTFIU)

Financial Sector Bodies—government

- Financial Services Authority (FSA)
- Bank of England

Financial sector bodies, associations, and entities

- British Bankers Association (BBA)
- Joint Money Laundering Steering Group (JMLSG) (includes the BBA, Finance and Leasing Association (FLA), Association of British Insurers (ABI), and the Investment Management Association (IMA) amongst others)
- investment management firm
- large retail banking firm
- money service business
- private banking firm
- insurance firm
- wholesale banking/securities firm
- casino

Measures for legal persons and NPOs

- Companies House
- Charity Commission for England & Wales
- Office of the Scottish Charities Regulator (OSCR, by video link)
- Department for Social Development in Northern Ireland (DSDNI, by video link)

DNFBP and other matters

- Gambling Commission
- Casino Operators association
- British Casino association
- Royal Institute of Chartered Surveyors (RICS)
- Law Society England and Wales (LSEW)
- Law Society Northern Ireland (LSNI)
- Law Society Scotland (LSS)
- Bar Council England and Wales (BCEW)
- Faculty of Advocates (Scotland)
- Council for Licensed Conveyancers (CLC)
- Consultative Committee of Accountancy Bodies (CCAB): Includes the Institute of Chartered Accountants in England and Wales (ICAEW); the Chartered Institute of Management Accountants (CIMA).
- The Society of Trust and Estate Practitioners (STEP)
- Association of Company Registration Agents
- National Association of Goldsmiths
- Money Laundering Reporting Officer of a major high-value dealer

Annex 3: List of laws, regulations and other guidance received[33]

- Al-Qaida and Taliban (UN Measures) Order 2002
- Al-Qaida and Taliban (UN Measures) Order 2002 (Amendment)
- Al-Qaida and Taliban (UN Measures) Order 2006
- Anti-Terrorism Crime and Security Act 2001
- Anti-Terrorism Crime and Security Act 2001
- Bank Notice 11/08/2006
- BAR Council guidance
- Charities Act 1993
- Charities Act 2006
- Charities Trustee Investment (Scotland) Act 2005
- Council for Licensed Conveyancers guidance
- Crime (International Cooperation) Act 2003
- Criminal Justice (International Co-operation) Act 1990
- Criminal Justice (International Co-operation) Act 1990 (Enforcement of Overseas Forfeiture Orders) Order 2005 -- England and Wales
- Criminal Justice (International Co-operation) Act 1990 (Enforcement of Overseas Forfeiture Orders) Order 2005 -- Northern Ireland
- Criminal Justice (International Co-operation) Act 1990 (Enforcement of Overseas Forfeiture Orders) Order 2005 -- Scotland
- DNFBP and Police case studies
- EC Regulation 1889/2005 (Cross-border cash controls)
- Extradition Act 2003
- Financial Services and Markets Act 2000
- Financial Services and Markets Act 2000 (Disclosure of Confidential Information) Regulations 2001 ("Gateways Regulation")
- FSA Handbook: Market Conduct (MAR)
- FSA Handbook: Fit and Proper Test for Approved Persons (FIT)
- FSA Handbook: General Provisions (GEN)
- FSA Handbook: Principles for Business (PRIN)
- FSA Handbook: Senior Management Arrangements, Systems and Controls (SYSC)
- FSA Handbook: Supervision (SUP)
- FSA Handbook: Enforcement (ENF)
- Gambling Act 2005
- Gaming Act 1968
- Institute of Chartered Accountants guidance
- JMLSG Guidance: The assessment of AML/CFT standards in other countries January 2006
- JMLSG Guidance: The assessment of AML/CFT standards in other countries September 2006
- JMLSG Guidance Notes, Part I (Main text)
- JMLSG Guidance Notes, Part II (Sectoral Guidance)
- Law Society for Scotland guidance
- Law Society of England and Wales guidance
- Money Laundering Regulations 2003
- Notaries guidance
- Proceeds of Crime Act 2002
- Proceeds of Crime Act 2002 (External Requests and Orders) Order 2005
- Serious Organised Crime and Police Act 2005
- Terrorism (UN Measures) Order 2001

[33] This list is not exhaustive.

- Terrorism (UN Measures) Order 2006
- Terrorism Act 2000
- Terrorism Act 2006

Annex 4: Copies of key laws, regulations and other measures

Proceeds of Crime Act 2002 (money laundering offence)

327 Concealing etc

(1) A person commits an offence if he-

(a) conceals criminal property;

(b) disguises criminal property;

(c) converts criminal property;

(d) transfers criminal property;

(e) removes criminal property from England and Wales or from Scotland or from Northern Ireland.

(2) But a person does not commit such an offence if-

(a) he makes an authorised disclosure under section 338 and (if the disclosure is made before he does the act mentioned in subsection (1)) he has the appropriate consent;

(b) he intended to make such a disclosure but had a reasonable excuse for not doing so;

(c) the act he does is done in carrying out a function he has relating to the enforcement of any provision of this Act or of any other enactment relating to criminal conduct or benefit from criminal conduct.

(3) Concealing or disguising criminal property includes concealing or disguising its nature, source, location, disposition, movement or ownership or any rights with respect to it.

328 Arrangements

(1) A person commits an offence if he enters into or becomes concerned in an arrangement which he knows or suspects facilitates (by whatever means) the acquisition, retention, use or control of criminal property by or on behalf of another person.

(2) But a person does not commit such an offence if-

(a) he makes an authorised disclosure under section 338 and (if the disclosure is made before he does the act mentioned in subsection (1)) he has the appropriate consent;

(b) he intended to make such a disclosure but had a reasonable excuse for not doing so;

(c) the act he does is done in carrying out a function he has relating to the enforcement of any provision of this Act or of any other enactment relating to criminal conduct or benefit from criminal conduct.

329 Acquisition, use and possession

(1) A person commits an offence if he-

(a) acquires criminal property;

(b) uses criminal property;

(c) has possession of criminal property.

(2) But a person does not commit such an offence if-

(a) he makes an authorised disclosure under section 338 and (if the disclosure is made before he does the act mentioned in subsection (1)) he has the appropriate

consent;

(b) he intended to make such a disclosure but had a reasonable excuse for not doing so;

(c) he acquired or used or had possession of the property for adequate consideration;

(d) the act he does is done in carrying out a function he has relating to the enforcement of any provision of this Act or of any other enactment relating to criminal conduct or benefit from criminal conduct.

(3) For the purposes of this section-

(a) a person acquires property for inadequate consideration if the value of the consideration is significantly less than the value of the property;

(b) a person uses or has possession of property for inadequate consideration if the value of the consideration is significantly less than the value of the use or possession;

(c) the provision by a person of goods or services which he knows or suspects may help another to carry out criminal conduct is not consideration.

…….

334 Penalties

(1) A person guilty of an offence under section 327, 328 or 329 is liable-

(a) on summary conviction, to imprisonment for a term not exceeding six months or to a fine not exceeding the statutory maximum or to both, or

(b) on conviction on indictment, to imprisonment for a term not exceeding 14 years or to a fine or to both.

(2) A person guilty of an offence under section 330, 331, 332 or 333 is liable-

(a) on summary conviction, to imprisonment for a term not exceeding six months or to a fine not exceeding the statutory maximum or to both, or

(b) on conviction on indictment, to imprisonment for a term not exceeding five years or to a fine or to both.

….

Interpretation

340 Interpretation

(1) This section applies for the purposes of this Part.

(2) Criminal conduct is conduct which-

(a) constitutes an offence in any part of the United Kingdom, or

(b) would constitute an offence in any part of the United Kingdom if it occurred there.

(3) Property is criminal property if-

(a) it constitutes a person's benefit from criminal conduct or it represents such a benefit (in whole or part and whether directly or indirectly), and

(b) the alleged offender knows or suspects that it constitutes or represents such a benefit.

(4) It is immaterial-

(a) who carried out the conduct;

(b) who benefited from it;

(c) whether the conduct occurred before or after the passing of this Act.

(5) A person benefits from conduct if he obtains property as a result of or in connection with the conduct.

(6) If a person obtains a pecuniary advantage as a result of or in connection with conduct, he is to be taken to obtain as a result of or in connection with the conduct a sum of money equal to the value of the pecuniary advantage.

(7) References to property or a pecuniary advantage obtained in connection with conduct include references to property or a pecuniary advantage obtained in both that connection and some other.

(8) If a person benefits from conduct his benefit is the property obtained as a result of or in connection with the conduct.

(9) Property is all property wherever situated and includes-

(a) money;

(b) all forms of property, real or personal, heritable or moveable;

(c) things in action and other intangible or incorporeal property.

(10) The following rules apply in relation to property-

(a) property is obtained by a person if he obtains an interest in it;

(b) references to an interest, in relation to land in England and Wales or Northern Ireland, are to any legal estate or equitable interest or power;

(c) references to an interest, in relation to land in Scotland, are to any estate, interest, servitude or other heritable right in or over land, including a heritable security;

(d) references to an interest, in relation to property other than land, include references to a right (including a right to possession).

(11) Money laundering is an act which-

(a) constitutes an offence under section 327, 328 or 329,

(b) constitutes an attempt, conspiracy or incitement to commit an offence specified in paragraph (a),

(c) constitutes aiding, abetting, counselling or procuring the commission of an offence specified in paragraph (a), or

(d) would constitute an offence specified in paragraph (a), (b) or (c) if done in the United Kingdom.

(12) For the purposes of a disclosure to a nominated officer-

(a) references to a person's employer include any body, association or organisation (including a voluntary organisation) in connection with whose activities the person exercises a function (whether or not for gain or reward), and

(b) references to employment must be construed accordingly.

(13) References to a constable include references to a person authorised for the purposes of this Part by the Director General of the National Criminal Intelligence Service.

Fund-raising.

15. - (1) A person commits an offence if he-

(a) invites another to provide money or other property, and

(b) intends that it should be used, or has reasonable cause to suspect that it may be used, for the purposes of terrorism.

(2) A person commits an offence if he-

(a) receives money or other property, and

(b) intends that it should be used, or has reasonable cause to suspect that it may be used, for the purposes of terrorism.

(3) A person commits an offence if he-

(a) provides money or other property, and

(b) knows or has reasonable cause to suspect that it will or may be used for the purposes of terrorism.

(4) In this section a reference to the provision of money or other property is a reference to its being given, lent or otherwise made available, whether or not for consideration.

Use and possession.

16. - (1) A person commits an offence if he uses money or other property for the purposes of terrorism.

(2) A person commits an offence if he-

(a) possesses money or other property, and

(b) intends that it should be used, or has reasonable cause to suspect that it may be used, for the purposes of terrorism.

Funding arrangements.

17. A person commits an offence if-

(a) he enters into or becomes concerned in an arrangement as a result of which money or other property is made available or is to be made available to another, and

(b) he knows or has reasonable cause to suspect that it will or may be used for the purposes of terrorism.

Money laundering.

18. - (1) A person commits an offence if he enters into or becomes concerned in an arrangement which facilitates the retention or control by or on behalf of another person of terrorist property-

(a) by concealment,

(b) by removal from the jurisdiction,

(c) by transfer to nominees, or

(d) in any other way.

(2) It is a defence for a person charged with an offence under subsection (1) to prove that he did not know and had no reasonable cause to suspect that the arrangement related to terrorist property.

Statutory Instrument
2003 No. 3075

The Money Laundering Regulations 2003

Made *28th November 2003*

Laid before Parliament *28th November 2003*

Coming into force in accordance with regulation 1(2)

ARRANGEMENT OF REGULATIONS

PART I:

GENERAL

1. Citation, commencement etc.
2. Interpretation

PART II:

OBLIGATIONS ON PERSONS WHO CARRY ON RELEVANT BUSINESS

3. Systems and training etc. to prevent money laundering
4. Identification procedures
5. Exceptions
6. Record-keeping procedures
7. Internal reporting procedures
8. Casinos

PART III:

MONEY SERVICE OPERATORS AND HIGH VALUE DEALERS

Registration

9. Registers of money service operators and high value dealers
10. Requirement to be registered
11. Supplementary information
12. Determination of application to register
13. Cancellation of registration
14. Fees

Powers of the Commissioners

15. Entry, inspection etc.
16. Order for access to recorded information
17. Procedure where recorded information is removed
18. Failure to comply with requirements under regulation 17
19. Entry, search etc.

Penalties, review and appeals

20. Power to impose penalties
21. Review procedure
22. Appeals to a VAT and duties tribunal

Miscellaneous

23. Prosecution of offences by the Commissioners
24. Recovery of fees and penalties through the court
25. Authorised persons operating a bureau de change

PART IV:

MISCELLANEOUS

26. Supervisory authorities etc. to report evidence of money laundering
27. Offences by bodies corporate etc.
28. Prohibitions in relation to certain countries
29. Minor and consequential amendments
30. Transitional provisions

SCHEDULES

1. Activities Listed in Annex 1 to the Banking Consolidation Directive
2. Minor and Consequential Amendments

Whereas the Treasury are a government department designated[1] for the purposes of section 2(2) of the European Communities Act 1972[2] in relation to measures relating to preventing the use of the financial system for the purpose of money laundering;

Now therefore the Treasury, in exercise of the powers conferred on them by -

(i) section 2(2) of the European Communities Act 1972, and
(ii) sections 168(4)(b), 402(1)(b), 417(1)[3] and 428(3) of the Financial Services and Markets Act 2000[4],

hereby make the following Regulations:

PART I

GENERAL

Citation, commencement etc.

1. - (1) These Regulations may be cited as the Money Laundering Regulations 2003.

(2) These Regulations come into force -

(a) for the purposes of regulation 10 in so far as it relates to a person who acts as a high value dealer, on 1st April 2004;
(b) for the purposes of regulation 2(3)(h), on 31st October 2004;
(c) for the purposes of regulation 2(3)(i), on 14th January 2005;
(d) for all other purposes, on 1st March 2004

(3) These Regulations are prescribed for the purposes of sections 168(4)(b) and 402(1)(b) of the 2000 Act.

(4) The following Regulations are revoked -

(a) the Money Laundering Regulations 1993[5];
(b) the Financial Services and Markets Act 2000 (Regulations Relating to Money Laundering)

Regulations 2001[6];
(c) the Money Laundering Regulations 2001[7].

Interpretation

2. - (1) In these Regulations -

"the 2000 Act" means the Financial Services and Markets Act 2000;
"applicant for business" means a person seeking to form a business relationship, or carry out a one-off transaction, with another person acting in the course of relevant business carried on by that other person in the United Kingdom;
"applicant for registration" means an applicant for registration as a money service operator, or as a high value dealer;
"the appropriate judicial authority" means -
(a) in England and Wales, a magistrates' court,

(b) in Scotland, the sheriff,

(c) in Northern Ireland, a court of summary jurisdiction;

"authorised person" has the meaning given by section 31(2) of the 2000 Act;
"the Authority" means the Financial Services Authority;
"the Banking Consolidation Directive" means Directive 2000/12/EC of the European Parliament and of the Council of 20th March 2000 relating to the taking up and pursuit of the business of credit institutions as last amended by Directive 2002/87/EC of the European Parliament and of the Council of 16th December 2002[8];
"business relationship" means any arrangement the purpose of which is to facilitate the carrying out of transactions on a frequent, habitual or regular basis where the total amount of any payments to be made by any person to any other in the course of the arrangement is not known or capable of being ascertained at the outset;
"cash" means notes, coins or travellers' cheques in any currency;
"the Commissioners" means the Commissioners of Customs and Excise;
"constable" includes a person commissioned by the Commissioners and a person authorised for the purposes of these Regulations by the Director General of the National Criminal Intelligence Service;
"EEA State" means a State which is a contracting party to the agreement on the European Economic Area signed at Oporto on 2nd May 1992 as it has effect for the time being;
"estate agency work" has the meaning given by section 1 of the Estate Agents Act 1979[9] save for the omission of the words "(including a business in which he is employed)" in subsection (1) and includes a case where, in relation to a disposal or acquisition, the person acts as principal;
"high value dealer" means a person who carries on the activity mentioned in paragraph (2)(n);
"the Life Assurance Consolidation Directive" means Directive 2002/83/EC of the European Parliament and of the Council of 5th November 2002 concerning life assurance[10];
"justice" means a justice of the peace or, in relation to Scotland, a justice within the meaning of section 307 of the Criminal Procedure (Scotland) Act 1995[11];
"money laundering" means an act which falls within section 340(11) of the Proceeds of Crime Act 2002[12] or an offence under section 18 of the Terrorism Act 2000[13];
"the Money Laundering Directive" means Council Directive 91/308/EEC of 10th June 1991 on prevention of the use of the financial system for the purpose of money laundering as amended by Directive 2001/97/EC of the European Parliament and of the Council of 4th December 2001[14];
"money service business" means any of the activities mentioned in paragraph (2)(d) (so far as not excluded by paragraph (3)) when carried on by way of business;

"money service operator" means a person who carries on money service business other than a person who carries on relevant business falling within any of sub-paragraphs (a) to (c) of paragraph (2);
"nominated officer" has the meaning given by regulation 7;
"officer" (except in regulations 7, 10 and 27) has the meaning given by section 1(1) of the Customs and Excise Management Act 1979[15];
"officer in overall charge of the investigation" means the person whose name and address are endorsed on the order concerned as being the officer so in charge;
"one-off transaction" means any transaction other than one carried out in the course of an existing business relationship;
"operator" means a money service operator;
"recorded information" includes information recorded in any form and any document of any nature whatsoever;
"registered number" has the meaning given by regulation 9(2);
"relevant business" has the meaning given by paragraph (2);
"the review procedure" means the procedure under regulation 21;
"satisfactory evidence of identity" has the meaning given by paragraphs (5) and (6);
"supervisory authority" has the meaning given by paragraphs (7) and (8);
"tribunal" means a VAT and duties tribunal.

(2) For the purposes of these Regulations, "relevant business" means -

(a) the regulated activity of -

(i) accepting deposits;
(ii) effecting or carrying out contracts of long-term insurance when carried on by a person who has received official authorisation pursuant to Article 4 or 51 of the Life Assurance Consolidation Directive;
(iii) dealing in investments as principal or as agent;
(iv) arranging deals in investments;
(v) managing investments;
(vi) safeguarding and administering investments;
(vii) sending dematerialised instructions;
(viii) establishing (and taking other steps in relation to) collective investment schemes;
(ix) advising on investments; or
(x) issuing electronic money;

(b) the activities of the National Savings Bank;

(c) any activity carried on for the purpose of raising money authorised to be raised under the National Loans Act 1968[16] under the auspices of the Director of Savings;

(d) the business of operating a bureau de change, transmitting money (or any representation of monetary value) by any means or cashing cheques which are made payable to customers;

(e) any of the activities in points 1 to 12 or 14 of Annex 1 to the Banking Consolidation Directive (which activities are, for convenience, set out in Schedule 1 to these Regulations) when carried on by way of business, ignoring an activity falling within any of sub-paragraphs (a) to (d);

(f) estate agency work;

(g) operating a casino by way of business;

(h) the activities of a person appointed to act as an insolvency practitioner within the meaning of section 388 of the Insolvency Act 1986[17] or Article 3 of the Insolvency (Northern Ireland) Order 1989[18];

(i) the provision by way of business of advice about the tax affairs of another person by a body corporate or unincorporate or, in the case of a sole practitioner, by an individual;

(j) the provision by way of business of accountancy services by a body corporate or unincorporate or, in the case of a sole practitioner, by an individual;

(k) the provision by way of business of audit services by a person who is eligible for appointment as a company auditor under section 25 of the Companies Act 1989[19] or Article 28 of the Companies (Northern Ireland) Order 1990[20];

(l) the provision by way of business of legal services by a body corporate or unincorporate or, in the case of a sole practitioner, by an individual and which involves participation in a financial or real property transaction (whether by assisting in the planning or execution of any such transaction or otherwise by acting for, or on behalf of, a client in any such transaction);

(m) the provision by way of business of services in relation to the formation, operation or management of a company or a trust; or

(n) the activity of dealing in goods of any description by way of business (including dealing as an auctioneer) whenever a transaction involves accepting a total cash payment of 15,000 euro or more.

(3) Paragraph (2) does not apply to -

(a) the issue of withdrawable share capital within the limit set by section 6 of the Industrial and Provident Societies Act 1965[21] by a society registered under that Act;

(b) the acceptance of deposits from the public within the limit set by section 7(3) of that Act by such a society;

(c) the issue of withdrawable share capital within the limit set by section 6 of the Industrial and Provident Societies Act (Northern Ireland) 1969[22] by a society registered under that Act;

(d) the acceptance of deposits from the public within the limit set by section 7(3) of that Act by such a society;

(e) activities carried on by the Bank of England;

(f) any activity in respect of which an exemption order under section 38 of the 2000 Act has effect if it is carried on by a person who is for the time being specified in the order or falls within a class of persons so specified;

(g) any activity (other than one falling within sub-paragraph (f)) in respect of which a person was an exempted person for the purposes of section 45 of the Financial Services Act 1986[23] immediately before its repeal;

(h) the regulated activities of arranging deals in investments or advising on investments, in so far as the investment consists of rights under a regulated mortgage contract;

(i) the regulated activities of dealing in investments as agent, arranging deals in investments,

managing investments or advising on investments, in so far as the investment consists of rights under, or any right to or interest in, a contract of insurance which is not a qualifying contract of insurance; or

(j) the Official Solicitor to the Supreme Court when acting as trustee in his official capacity.

(4) The following must be read with section 22 of the 2000 Act, any relevant order under that section and Schedule 2 to that Act -

(a) paragraphs (2)(a) and (3)(h) and (i);

(b) regulation 25 (authorised persons operating a bureau de change);

(c) references in these Regulations to a contract of long-term insurance.

(5) For the purposes of these Regulations, and subject to paragraph (6), "satisfactory evidence of identity" is evidence which is reasonably capable of establishing (and does in fact establish to the satisfaction of the person who obtains it) that the applicant for business is the person he claims to be.

(6) Where the person who obtains the evidence mentioned in paragraph (5) knows or has reasonable grounds for believing that the applicant for business is a money service operator, satisfactory evidence of identity must also include the applicant's registered number (if any).

(7) For the purposes of these Regulations, each of the following is a supervisory authority -

(a) the Bank of England;

(b) the Authority;

(c) the Council of Lloyd's;

(d) the Office of Fair Trading;

(e) the Occupational Pensions Regulatory Authority;

(f) a body which is a designated professional body for the purposes of Part 20 of the 2000 Act;

(g) the Gaming Board for Great Britain.

(8) The Secretary of State and the Treasury are each a supervisory authority in the exercise, in relation to a person carrying on relevant business, of their respective functions under the enactments relating to companies or insolvency or under the 2000 Act.

(9) In these Regulations, references to amounts in euro include references to equivalent amounts in another currency.

(10) For the purpose of the application of these Regulations to Scotland, "real property" means "heritable property".

PART II

OBLIGATIONS ON PERSONS WHO CARRY ON RELEVANT BUSINESS

Systems and training etc. to prevent money laundering

3. - (1) Every person must in the course of relevant business carried on by him in the United Kingdom -

(a) comply with the requirements of regulations 4 (identification procedures), 6 (record-keeping procedures) and 7 (internal reporting procedures);

(b) establish such other procedures of internal control and communication as may be appropriate for the purposes of forestalling and preventing money laundering; and

(c) take appropriate measures so that relevant employees are -

(i) made aware of the provisions of these Regulations, Part 7 of the Proceeds of Crime Act 2002 (money laundering) and sections 18 and 21A of the Terrorism Act 2000[24]; and
(ii) given training in how to recognise and deal with transactions which may be related to money laundering.

(2) A person who contravenes this regulation is guilty of an offence and liable -

(a) on conviction on indictment, to imprisonment for a term not exceeding 2 years, to a fine or to both;

(b) on summary conviction, to a fine not exceeding the statutory maximum.

(3) In deciding whether a person has committed an offence under this regulation, the court must consider whether he followed any relevant guidance which was at the time concerned -

(a) issued by a supervisory authority or any other appropriate body;

(b) approved by the Treasury; and

(c) published in a manner approved by the Treasury as appropriate in their opinion to bring the guidance to the attention of persons likely to be affected by it.

(4) An appropriate body is any body which regulates or is representative of any trade, profession, business or employment carried on by the alleged offender.

(5) In proceedings against any person for an offence under this regulation, it is a defence for that person to show that he took all reasonable steps and exercised all due diligence to avoid committing the offence.

(6) Where a person is convicted of an offence under this regulation, he shall not also be liable to a penalty under regulation 20 (power to impose penalties).

Identification procedures

4. - (1) In this regulation and in regulations 5 to 7 -

(a) "A" means a person who carries on relevant business in the United Kingdom; and

(b) "B" means an applicant for business.

(2) This regulation applies if -

(a) A and B form, or agree to form, a business relationship;

(b) in respect of any one-off transaction -

(i) A knows or suspects that the transaction involves money laundering; or

(ii) payment of 15,000 euro or more is to be made by or to B; or

(c) in respect of two or more one-off transactions, it appears to A (whether at the outset or subsequently) that the transactions are linked and involve, in total, the payment of 15,000 euro or more by or to B.

(3) A must maintain identification procedures which -

(a) require that as soon as is reasonably practicable after contact is first made between A and B -

(i) B must produce satisfactory evidence of his identity; or
(ii) such measures specified in the procedures must be taken in order to produce satisfactory evidence of B's identity;

(b) take into account the greater potential for money laundering which arises when B is not physically present when being identified;

(c) require that where satisfactory evidence of identity is not obtained, the business relationship or one-off transaction must not proceed any further; and

(d) require that where B acts or appears to act for another person, reasonable measures must be taken for the purpose of establishing the identity of that person.

Exceptions

5. - (1) Except in circumstances falling within regulation 4(2)(b)(i), identification procedures under regulation 4 do not require A to take steps to obtain evidence of any person's identity in any of the following circumstances.

(2) Where A has reasonable grounds for believing that B -

(a) carries on in the United Kingdom relevant business falling within any of sub-paragraphs (a) to (e) of regulation 2(2), is not a money service operator and, if carrying on an activity falling within regulation 2(2)(a), is an authorised person with permission under the 2000 Act to carry on that activity;

(b) does not carry on relevant business in the United Kingdom but does carry on comparable activities to those falling within sub-paragraph (a) and is covered by the Money Laundering Directive; or

(c) is regulated by an overseas regulatory authority (within the meaning given by section 82 of the Companies Act 1989) and is based or incorporated in a country (other than an EEA State) whose law contains comparable provisions to those contained in the Money Laundering Directive.

(3) Where -

(a) A carries out a one-off transaction with or for a third party pursuant to an introduction effected by a person who has provided a written assurance that evidence of the identity of all

third parties introduced by him will have been obtained and recorded under procedures maintained by him;

(b) that person identifies the third party; and

(c) A has reasonable grounds for believing that that person falls within any of sub-paragraphs (a) to (c) of paragraph (2).

(4) In relation to a contract of long-term insurance -

(a) in connection with a pension scheme taken out by virtue of a person's contract of employment or occupation where the contract of long-term insurance -

(i) contains no surrender clause; and
(ii) may not be used as collateral for a loan; or

(b) in respect of which a premium is payable -

(i) in one instalment of an amount not exceeding 2,500 euro; or
(ii) periodically and where the total payable in respect of any calendar year does not exceed 1,000 euro.

(5) Where the proceeds of a one-off transaction are payable to B but are instead directly reinvested on his behalf in another transaction -

(a) of which a record is kept; and

(b) which can result only in another reinvestment made on B's behalf or in a payment made directly to B.

Record-keeping procedures

6. - (1) A must maintain procedures which require the retention of the records prescribed in paragraph (2) for the period prescribed in paragraph (3).

(2) The records are -

(a) where evidence of identity has been obtained under the procedures stipulated by regulation 4 (identification procedures) or pursuant to regulation 8 (casinos) -

(i) a copy of that evidence;
(ii) information as to where a copy of that evidence may be obtained; or
(iii) information enabling the evidence of identity to be re-obtained, but only where it is not reasonably practicable for A to comply with paragraph (i) or (ii); and

(b) a record containing details relating to all transactions carried out by A in the course of relevant business.

(3) In relation to the records mentioned in paragraph (2)(a), the period is -

(a) where A and B have formed a business relationship, at least five years commencing with the date on which the relationship ends; or

(b) in the case of a one-off transaction (or a series of such transactions), at least five years commencing with the date of the completion of all activities taking place in the course of that transaction (or, as the case may be, the last of the transactions).

(4) In relation to the records mentioned in paragraph (2)(b), the period is at least five years commencing with the date on which all activities taking place in the course of the transaction in question were completed.

(5) Where A is an appointed representative, his principal must ensure that A complies with this regulation in respect of any relevant business carried out by A for which the principal has accepted responsibility pursuant to section 39(1) of the 2000 Act.

(6) Where the principal fails to do so, he is to be treated as having contravened regulation 3 and he, as well as A, is guilty of an offence.

(7) "Appointed representative" has the meaning given by section 39(2) of the 2000 Act and "principal" has the meaning given by section 39(1) of that Act.

Internal reporting procedures

7. - (1) A must maintain internal reporting procedures which require that -

(a) a person in A's organisation is nominated to receive disclosures under this regulation ("the nominated officer");

(b) anyone in A's organisation to whom information or other matter comes in the course of relevant business as a result of which he knows or suspects or has reasonable grounds for knowing or suspecting that a person is engaged in money laundering must, as soon as is practicable after the information or other matter comes to him, disclose it to the nominated officer or a person authorised for the purposes of these Regulations by the Director General of the National Criminal Intelligence Service;

(c) where a disclosure is made to the nominated officer, he must consider it in the light of any relevant information which is available to A and determine whether it gives rise to such knowledge or suspicion or such reasonable grounds for knowledge or suspicion; and

(d) where the nominated officer does so determine, the information or other matter must be disclosed to a person authorised for the purposes of these Regulations by the Director General of the National Criminal Intelligence Service.

(2) Paragraph (1) does not apply where A is an individual who neither employs nor acts in association with any other person.

(3) Paragraph (1)(b) does not apply in relation to a professional legal adviser where the information or other matter comes to him in privileged circumstances.

(4) Information or other matter comes to a professional legal adviser in privileged circumstances if it is communicated or given to him -

(a) by (or by a representative of) a client of his in connection with the giving by the adviser of legal advice to the client;

(b) by (or by a representative of) a person seeking legal advice from the adviser; or

(c) by a person in connection with legal proceedings or contemplated legal proceedings.

(5) But paragraph (4) does not apply to information or other matter which is communicated or given with the intention of furthering a criminal purpose.

(6) "Professional legal adviser" includes any person in whose hands information or other matter

may come in privileged circumstances.

Casinos

8. - (1) A person who operates a casino by way of business in the United Kingdom must obtain satisfactory evidence of identity of any person before allowing that person to use the casino's gaming facilities.

(2) A person who fails to do so is to be treated as having contravened regulation 3.

PART III

MONEY SERVICE OPERATORS AND HIGH VALUE DEALERS

Registration

Registers of money service operators and high value dealers

9. - (1) The Commissioners must maintain a register of operators.

(2) The Commissioners must allocate to every registered operator a number, which is to be known as his registered number.

(3) The Commissioners must maintain a register of high value dealers.

(4) The Commissioners may keep the registers in any form they think fit.

Requirement to be registered

10. - (1) A person who acts as an operator or as a high value dealer must first be registered by the Commissioners.

(2) An applicant for registration must -

(a) make an application to be registered in such manner as the Commissioners may direct; and

(b) furnish the following information to the Commissioners -

(i) his name and (if different) the name of the business;

(ii) his VAT registration number or, if he is not registered for VAT, any other reference number issued to him by the Commissioners;

(iii) the nature of the business;

(iv) the address of each of the premises at which he proposes to carry on the business;

(v) any agency or franchise agreement relating to the business, and the names and addresses of all relevant principals, agents, franchisors or franchisees;

(vi) the name of the nominated officer (if any); and

(vii) whether any person concerned (or proposed to be concerned) in the management, control or operation of the business has been convicted of money laundering or an offence under these Regulations.

(3) At any time after receiving an application for registration and before determining it, the Commissioners may require the applicant for registration to furnish them, within 21 days beginning with the date of being requested to do so, with such further information as they reasonably consider necessary to enable them to determine the application.

(4) Any information to be furnished to the Commissioners under this regulation must be in such form or verified in such manner as they may specify.

(5) In this regulation, "the business" means money service business (or, in the case of a high value dealer, the business of dealing in goods) which the applicant for registration carries on or proposes to carry on.

(6) In paragraph (2)(b)(vii), the reference to "money laundering or an offence under these Regulations" includes an offence referred to in regulation 2(3) of the Money Laundering Regulations 1993 or an offence under regulation 5 of those Regulations.

Supplementary information

11. - (1) If at any time after a person has furnished the Commissioners with any information under regulation 10 -

(a) there is a change affecting any matter contained in that information; or

(b) it becomes apparent to that person that the information contains an inaccuracy;

he must supply the Commissioners with details of the change or, as the case may be, a correction of the inaccuracy (hereafter "supplementary information") within 30 days beginning with the date of the occurrence of the change (or the discovery of the inaccuracy) or within such later time as may be agreed with the Commissioners.

(2) The supplementary information must be supplied in such manner as the Commissioners may direct.

(3) The obligation in paragraph (1) applies also to changes affecting any matter contained in any supplementary information supplied pursuant to this regulation.

Determination of application to register

12. - (1) The Commissioners may refuse to register an applicant for registration if, and only if -

(a) any requirement of -

(i) paragraphs (2) to (4) of regulation 10 (requirement to be registered);
(ii) regulation 11 (supplementary information); or
(iii) regulation 14 (fees);

has not been complied with; or

(b) it appears to them that any information furnished pursuant to regulation 10 or 11 is false or misleading in a material particular.

(2) The Commissioners must, by the end of the period of 45 days beginning with the date on which they receive the application or, where applicable, the date on which they receive any further information required under regulation 10(3), give notice in writing to the applicant for registration of -

(a) their decision to register him and, in the case of an applicant for registration as an operator, his registered number; or

(b) the following matters -

(i) their decision not to register him;
(ii) the reasons for their decision;
(iii) the review procedure; and
(iv) the right to appeal to a tribunal.

Cancellation of registration

13. - (1) The Commissioners may cancel the registration of an operator or high value dealer if, at any time after registration, it appears to them that they would have had grounds to refuse registration under paragraph (1) of regulation 12 (determination of application to register).

(2) Where the Commissioners decide to cancel the registration of an operator or high value dealer, they must forthwith inform him, in writing, of -

(a) their decision and the date from which the cancellation takes effect;

(b) the reasons for their decision;

(c) the review procedure; and

(d) the right to appeal to a tribunal.

Fees

14. - (1) The Commissioners may charge a fee -

(a) to an applicant for registration; and

(b) to an operator or high value dealer annually on the anniversary of his registration by them under these Regulations.

(2) The Commissioners may charge under paragraph (1) such fees as they consider will enable them to meet any expenses incurred by them in carrying out any of their functions under these Regulations or for any incidental purpose.

(3) Without prejudice to the generality of paragraph (2), a fee may be charged in respect of each of the premises at which the operator, high value dealer or applicant for registration carries on (or proposes to carry on) money service business or relevant business falling within regulation 2(2)(n).

Powers of the Commissioners

Entry, inspection etc.

15. - (1) Where an officer has reasonable cause to believe that any premises are used in connection with money service business or relevant business falling within regulation 2(2)(n), he may at any reasonable time enter and inspect the premises and inspect any recorded information or currency found on the premises.

(2) An operator or high value dealer must -

(a) furnish to an officer, within such time and in such form as the officer may reasonably require, such information relating to the business as the officer may reasonably specify; and

(b) upon demand made by the officer, produce or cause to be produced for inspection by the

officer at such place, and at such time, as the officer may reasonably require, any recorded information relating to the business.

(3) An officer may take copies of, or make extracts from, any recorded information produced under paragraph (2).

Order for access to recorded information

16. - (1) Where, on an application by an officer, a justice is satisfied that there are reasonable grounds for believing -

(a) that an offence under these Regulations is being, has been or is about to be committed by an operator or high value dealer; and

(b) that any recorded information which may be required as evidence for the purpose of any proceedings in respect of such an offence is in the possession of any person;

he may make an order under this regulation.

(2) An order under this regulation is an order that the person who appears to the justice to be in possession of the recorded information to which the application relates must -

(a) give an officer access to it;

(b) permit an officer to take copies of, or make extracts from, any information produced; or

(c) permit an officer to remove and take away any of it which he reasonably considers necessary;

not later than the end of the period of 7 days beginning with the date of the order or the end of such longer period as the order may specify.

(3) Where the recorded information consists of information stored in any electronic form, an order under this regulation has effect as an order to produce the information in a form in which it is visible and legible, or from which it can readily be produced in a visible and legible form, and, if the officer wishes to remove it, in a form in which it can be removed.

Procedure where recorded information is removed

17. - (1) An officer who removes any recorded information in the exercise of a power conferred by regulation 16 must, if so requested by a person showing himself -

(a) to be the occupier of premises from which the information was removed; or

(b) to have had custody or control of the information immediately before the removal;

provide that person with a record of what he has removed.

(2) The officer must provide the record within a reasonable time from the making of the request for it.

(3) Subject to paragraph (7), if a request for permission to be granted access to anything which -

(a) has been removed by an officer; and

(b) is retained by the Commissioners for the purposes of investigating an offence;

is made to the officer in overall charge of the investigation by a person who had custody or control of the thing immediately before it was so removed or by someone acting on behalf of such a person, that officer must allow the person who made the request access to it under the supervision of an officer.

(4) Subject to paragraph (7), if a request for a photograph or copy of any such thing is made to the officer in overall charge of the investigation by a person who had custody or control of the thing immediately before it was so removed, or by someone acting on behalf of such a person, that officer must -

(a) allow the person who made the request access to it under the supervision of an officer for the purpose of photographing it or copying it; or

(b) photograph or copy it, or cause it to be photographed or copied.

(5) Where anything is photographed or copied under paragraph (4)(b), the photograph or copy must be supplied to the person who made the request.

(6) The photograph or copy must be supplied within a reasonable time from the making of the request.

(7) There is no duty under this regulation to grant access to, or supply a photograph or a copy of, anything if the officer in overall charge of the investigation for the purposes of which it was removed has reasonable grounds for believing that to do so would prejudice -

(a) that investigation;

(b) the investigation of an offence other than the offence for the purposes of the investigation of which the recorded information was removed; or

(c) any criminal proceedings which may be brought as a result of -

(i) the investigation of which he is in charge; or
(ii) any such investigation as is mentioned in sub-paragraph (b).

Failure to comply with requirements under regulation 17

18. - (1) Where, on an application made as mentioned in paragraph (2), the appropriate judicial authority is satisfied that a person has failed to comply with a requirement imposed by regulation 17, the authority may order that person to comply with the requirement within such time and in such manner as may be specified in the order.

(2) An application under paragraph (1) may only be made -

(a) in the case of a failure to comply with any of the requirements imposed by regulation 17(1) and (2), by the occupier of the premises from which the thing in question was removed or by the person who had custody or control of it immediately before it was so removed;

(b) in any other case, by the person who had such custody or control.

(3) In England and Wales and Northern Ireland, an application for an order under this regulation is to be made by complaint; and sections 21 and 42(2) of the Interpretation Act (Northern Ireland) 1954[25] apply as if any reference in those provisions to any enactment included a reference to this regulation.

Entry, search etc.

19. - (1) Where a justice is satisfied on information on oath that there is reasonable ground for

suspecting that an offence under these Regulations is being, has been or is about to be committed by an operator or high value dealer on any premises or that evidence of the commission of such an offence is to be found there, he may issue a warrant in writing authorising any officer to enter those premises, if necessary by force, at any time within one month from the time of the issue of the warrant and search them.

(2) A person who enters the premises under the authority of the warrant may -

(a) take with him such other persons as appear to him to be necessary;

(b) seize and remove any documents or other things whatsoever found on the premises which he has reasonable cause to believe may be required as evidence for the purpose of proceedings in respect of an offence under these Regulations; and

(c) search or cause to be searched any person found on the premises whom he has reasonable cause to believe to be in possession of any such documents or other things; but no woman or girl may be searched except by a woman.

(3) The powers conferred by a warrant under this regulation may not be exercised -

(a) outside such times of day as may be specified in the warrant; or

(b) if the warrant so provides, otherwise than in the presence of a constable in uniform.

(4) An officer seeking to exercise the powers conferred by a warrant under this regulation or, if there is more than one such officer, that one of them who is in charge of the search must provide a copy of the warrant endorsed with his name as follows -

(a) if the occupier of the premises concerned is present at the time the search is to begin, the copy must be supplied to the occupier;

(b) if at that time the occupier is not present but a person who appears to the officer to be in charge of the premises is present, the copy must be supplied to that person;

(c) if neither sub-paragraph (a) nor (b) applies, the copy must be left in a prominent place on the premises.

Penalties, review and appeals

Power to impose penalties

20. - (1) The Commissioners may impose a penalty of such amount as they consider appropriate, not exceeding £5,000, on a person to whom regulation 10 (requirement to be registered) applies, where that person fails to comply with any requirement in regulation 3 (systems and training etc. to prevent money laundering), 10, 11 (supplementary information), 14 (fees) or 15 (entry, inspection etc.).

(2) The Commissioners must not impose a penalty on a person where there are reasonable grounds for them to be satisfied that the person took all reasonable steps for securing that the requirement would be complied with.

(3) Where the Commissioners decide to impose a penalty under this regulation, they must forthwith inform the person, in writing, of -

(a) their decision to impose the penalty and its amount;

(b) their reasons for imposing the penalty;

(c) the review procedure; and

(d) the right to appeal to a tribunal.

(4) Where a person is liable to a penalty under this regulation, the Commissioners may reduce the penalty to such amount (including nil) as they think proper.

Review procedure

21. - (1) This regulation applies to the following decisions of the Commissioners -

(a) a decision under regulation 12 to refuse to register an applicant;

(b) a decision under regulation 13 to cancel the registration of an operator or high value dealer;

(c) a decision under regulation 20 to impose a penalty.

(2) Any person who is the subject of a decision as mentioned in paragraph (1) may by notice in writing to the Commissioners require them to review that decision.

(3) The Commissioners need not review any decision unless the notice requiring the review is given before the end of the period of 45 days beginning with the date on which written notification of the decision was first given to the person requiring the review.

(4) A person may give a notice under this regulation to require a decision to be reviewed for a second or subsequent time only if -

(a) the grounds on which he requires the further review are that the Commissioners did not, on any previous review, have the opportunity to consider certain facts or other matters; and

(b) he does not, on the further review, require the Commissioners to consider any facts or matters which were considered on a previous review except in so far as they are relevant to any issue to which the facts or matters not previously considered relate.

(5) Where the Commissioners are required under this regulation to review any decision they must either -

(a) confirm the decision; or

(b) withdraw or vary the decision and take such further steps (if any) in consequence of the withdrawal or variation as they consider appropriate.

(6) Where the Commissioners do not, within 45 days beginning with the date on which the review was required by a person, give notice to that person of their determination of the review, they are to be assumed for the purposes of these Regulations to have confirmed the decision.

Appeals to a VAT and duties tribunal

22. On an appeal from any decision by the Commissioners on a review under regulation 21, the tribunal have the power to -

(a) quash or vary any decision of the Commissioners, including the power to reduce any penalty to such amount (including nil) as they think proper; and

(b) substitute their own decision for any decision quashed on appeal.

Miscellaneous

Prosecution of offences by the Commissioners

23. - (1) Proceedings for an offence under these Regulations may be instituted by order of the Commissioners.

(2) Such proceedings may be instituted only against an operator or high value dealer or, where such a person is a body corporate, a partnership or an unincorporated association, against any person who is liable to be proceeded against under regulation 27 (offences by bodies corporate etc.).

(3) Any such proceedings which are so instituted must be commenced in the name of an officer.

(4) In the case of the death, removal, discharge or absence of the officer in whose name any such proceedings were commenced, those proceedings may be continued by another officer.

(5) Where the Commissioners investigate, or propose to investigate, any matter with a view to determining -

(a) whether there are grounds for believing that an offence under these Regulations has been committed by any person mentioned in paragraph (2); or

(b) whether such a person should be prosecuted for such an offence;

that matter is to be treated as an assigned matter within the meaning of the Customs and Excise Management Act 1979.

(6) In exercising their power to institute proceedings for an offence under these Regulations, the Commissioners must comply with any conditions or restrictions imposed in writing by the Treasury.

(7) Conditions or restrictions may be imposed under paragraph (6) in relation to -

(a) proceedings generally; or

(b) such proceedings, or categories of proceedings, as the Treasury may direct.

Recovery of fees and penalties through the court

24. Where any fee is charged, or any penalty is imposed, by virtue of these Regulations -

(a) if the person from whom it is recoverable resides in England and Wales or Northern Ireland, it is recoverable as a civil debt; and

(b) if that person resides in Scotland, it may be enforced in the same manner as an extract registered decree arbitral bearing a warrant for execution issued by the sheriff court of any sheriffdom in Scotland.

Authorised persons operating a bureau de change

25. - (1) No authorised person may, as from 1st April 2004, carry on the business of operating a bureau de change unless he has first informed the Authority that he proposes to do so.

(2) Where an authorised person ceases to carry on that business, he must inform the Authority forthwith.

(3) Any information to be supplied to the Authority under this regulation must be in such form or verified in such manner as the Authority may specify.

(4) Any requirement imposed by this regulation is to be treated as if it were a requirement imposed by or under the 2000 Act.

(5) Any function of the Authority under this regulation is to be treated as if it were a function of the Authority under the 2000 Act.

PART IV

MISCELLANEOUS

Supervisory authorities etc. to report evidence of money laundering

26. - (1) Where a supervisory authority, in the light of any information obtained by it, knows or suspects, or has reasonable grounds for knowing or suspecting, that someone has or may have been engaged in money laundering, the supervisory authority must disclose the information to a constable as soon as is reasonably practicable.

(2) Where a supervisory authority passes the information to any other person who has such knowledge or suspicion or such reasonable grounds for knowledge or suspicion as is mentioned in paragraph (1), he may disclose the information to a constable.

(3) Where any person within paragraph (6), in the light of any information obtained by him, knows or suspects or has reasonable grounds for knowing or suspecting that someone has or may have been engaged in money laundering, he must, as soon as is reasonably practicable, disclose that information either to a constable or to the supervisory authority by whom he was appointed or authorised.

(4) Where information has been disclosed to a constable under this regulation, he (or any person obtaining the information from him) may disclose it in connection with the investigation of any criminal offence or for the purpose of any criminal proceedings, but not otherwise.

(5) A disclosure made under this regulation is not to be taken to breach any restriction on the disclosure of information (however imposed).

(6) Persons within this paragraph are -

(a) a person or inspector appointed under section 65 or 66 of the Friendly Societies Act 1992[26];

(b) an inspector appointed under section 49 of the Industrial and Provident Societies Act 1965 or section 18 of the Credit Unions Act 1979[27];

(c) an inspector appointed under section 431, 432, 442 or 446 of the Companies Act 1985[28] or under Article 424, 425, 435 or 439 of the Companies (Northern Ireland) Order 1986[29];

(d) a person or inspector appointed under section 55 or 56 of the Building Societies Act 1986[30];

(e) a person appointed under section 167, 168(3) or (5), 169(1)(b) or 284 of the 2000 Act, or under regulations made as a result of section 262(2)(k) of that Act, to conduct an investigation; and

(f) a person authorised to require the production of documents under section 447 of the Companies Act 1985, Article 440 of the Companies (Northern Ireland) Order 1986 or section 84 of the Companies Act 1989.

Offences by bodies corporate etc.

27. - (1) If an offence under regulation 3 committed by a body corporate is shown -

(a) to have been committed with the consent or the connivance of an officer; or

(b) to be attributable to any neglect on his part;

the officer as well as the body corporate is guilty of an offence and liable to be proceeded against and punished accordingly.

(2) If an offence under regulation 3 committed by a partnership is shown -

(a) to have been committed with the consent or the connivance of a partner; or

(b) to be attributable to any neglect on his part;

the partner as well as the partnership is guilty of an offence and liable to be proceeded against and punished accordingly.

(3) If an offence under regulation 3 committed by an unincorporated association (other than a partnership) is shown -

(a) to have been committed with the consent or the connivance of an officer of the association or a member of its governing body; or

(b) to be attributable to any neglect on the part of such an officer or member;

that officer or member as well as the association is guilty of an offence and liable to be proceeded against and punished accordingly.

(4) If the affairs of a body corporate are managed by its members, paragraph (1) applies in relation to the acts and defaults of a member in connection with his functions of management as if he were a director of the body.

(5) In this regulation -

(a) "partner" includes a person purporting to act as a partner; and

(b) "officer", in relation to a body corporate, means a director, manager, secretary, chief executive, member of the committee of management, or a person purporting to act in such a capacity.

Prohibitions in relation to certain countries

28. - (1) The Treasury may direct any person who carries on relevant business -

(a) not to enter a business relationship;

(b) not to carry out any one-off transaction; or

(c) not to proceed any further with a business relationship or one-off transaction;

in relation to a person who is based or incorporated in a country (other than an EEA State) to which the Financial Action Task Force has decided to apply counter-measures.

(2) A person who fails to comply with a Treasury direction is to be treated as having contravened regulation 3.

Minor and consequential amendments

29. The provisions mentioned in Schedule 2 to these Regulations have effect subject to the amendments there specified, being minor amendments and amendments consequential on the provisions of these Regulations.

Transitional provisions

30. - (1) Nothing in these Regulations obliges any person who carries on relevant business falling within any of sub-paragraphs (a) to (e) of regulation 2(2) to maintain identification procedures which require evidence to be obtained in respect of any business relationship formed by him before 1st April 1994.

(2) Nothing in these Regulations obliges any person who carries on relevant business falling within any of sub-paragraphs (f) to (n) of regulation 2(2) -

(a) to maintain identification procedures which require evidence to be obtained in respect of any business relationship formed by him before 1st March 2004; or

(b) to maintain internal reporting procedures which require any action to be taken in respect of any knowledge, suspicion or reasonable grounds for knowledge or suspicion which came to that person before 1st March 2004.

John Heppell
Nick Ainger
Two of the Lords Commissioners of Her Majesty's Treasury
28th November 2003

SCHEDULE 1

Regulation 2(2)(e)

ACTIVITIES LISTED IN ANNEX 1 TO THE BANKING CONSOLIDATION DIRECTIVE

1. Acceptance of deposits and other repayable funds.
2. Lending.
3. Financial leasing.
4. Money transmission services.
5. Issuing and administering means of payment (eg credit cards, travellers' cheques and bankers' drafts).
6. Guarantees and commitments.
7. Trading for own account or for account of customers in -

(a) money market instruments (cheques, bills, certificates of deposit, etc.);
(b) foreign exchange;
(c) financial futures and options;
(d) exchange and interest-rate instruments;
(e) transferable securities.

8. Participation in securities issues and the provision of services related to such issues.
9. Advice to undertakings on capital structure, industrial strategy and related questions and advice as well as services relating to mergers and the purchase of undertakings.
10. Money broking.
11. Portfolio management and advice.
12. Safekeeping and administration of securities.
13. Credit reference services.
14. Safe custody services.

SCHEDULE 2

Regulation 29

MINOR AND CONSEQUENTIAL AMENDMENTS

PART I

Primary Legislation

Value Added Tax Act 1994 (c. 23)

1. - (1) Section 83 of the Value Added Tax Act 1994 is amended as follows.

(2) In paragraph (zz), for "regulation 16 of the Money Laundering Regulations 2001", substitute "regulation 21 of the Money Laundering Regulations 2003".

Northern Ireland Act 1998 (c. 47)

2. - (1) Paragraph 25 of Schedule 3 (reserved matters) to the Northern Ireland Act 1998 is amended as follows.

(2) For "1993" substitute "2003".

PART II

Secondary Legislation

The Cross-Border Credit Transfers Regulations 1999 (S.I. 1999/1876)

3. - (1) Regulation 12 of the Cross-Border Credit Transfers Regulations 1999 is amended as follows.

(2) For paragraph (2) substitute -

" (2) In this regulation "enactments relating to money laundering" means section 18 of the Terrorism Act 2000, section 340(11) of the Proceeds of Crime Act 2002 and the Money Laundering Regulations 2003.".

The Terrorism Act 2000 (Crown Servants and Regulators) Regulations 2001 (S.I. 2001/192)

4. - (1) The Terrorism Act 2000 (Crown Servants and Regulators) Regulations 2001 are amended as follows.

(2) In regulation 2, for the definition of "relevant financial business" substitute -

" "relevant business" has the meaning given by regulation 2(2) of the Money Laundering Regulations 2003.".

(3) In regulation 3, for "relevant financial business" substitute "relevant business".

The Representation of the People (England and Wales) Regulations 2001 (S.I. 2001/341)

5. - (1) The Representation of the People (England and Wales) Regulations 2001 are amended as follows.

(2) In regulation 114(3)(b)[31] -

(i) for "1993" substitute "2003"; and

(ii) omit ", the Money Laundering Regulations 2001".

The Representation of the People (Northern Ireland) Regulations 2001 (S.I. 2001/400)

6. - (1) The Representation of the People (Northern Ireland) Regulations 2001 are amended as follows.

(2) In regulation 107(3)(b)[32] -

(i) in paragraph (i), for "1993" substitute "2003";

(ii) omit paragraph (ii); and

(iii) in paragraph (iii), omit the words "either of" and "sets of".

The Representation of the People (Scotland) Regulations 2001 (S.I. 2001/497)

7. - (1) The Representation of the People (Scotland) Regulations 2001 are amended as follows.

(2) In regulation 113(3)(b)[33] -

(i) for "1993" substitute "2003"; and

(ii) omit ", the Money Laundering Regulations 2001".

The Proceeds of Crime Act 2002 (Failure to Disclose Money Laundering: Specified Training)Order 2003 (S.I. 2003/171)

8. - (1) The Proceeds of Crime Act 2002 (Failure to Disclose Money Laundering: Specified Training) Order 2003 is amended as follows.

(2) In article 2, for "regulation 5(1)(c) of the Money Laundering Regulations 1993" substitute "regulation 3(1)(c)(ii) of the Money Laundering Regulations 2003".