Financial Action Task Force on Money Laundering

Groupe d'action financière sur le blanchiment de capitaux

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

NORWAY

10 JUNE 2005

TABLE OF CONTENTS

Preface - information and methodology used for the evaluation ... 3
EXECUTIVE SUMMARY ...
1 GENERAL ... 14
1.1 General information on Norway ... 14
1.2 General Situation of Money Laundering and Financing of Terrorism ... 15
1.3 Overview of the Financial Sector and DNFBP ... 17
1.4 Overview of commercial laws and mechanisms governing legal persons and arrangements 20
1.5 Overview of strategy to prevent money laundering and terrorist financing ... 21
2 LEGAL SYSTEM AND RELATED INSTITUTIONAL MEASURES ... 28
2.1 Criminalisation of Money Laundering (R.1 & 2) ... 28
2.2 Criminalisation of Terrorist Financing (SR.II) ... 35
2.3 Confiscation, freezing and seizing of proceeds of crime (R.3) ... 37
2.4 Freezing of funds used for terrorist financing (SR.III) ... 43
2.5 The Financial Intelligence Unit and its functions (R.26, 30 & 32) ... 47
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) ... 57
3 PREVENTIVE MEASURES - FINANCIAL INSTITUTIONS ... 65
3.1 Risk of money laundering or terrorist financing ... 65
3.2 Customer due diligence, including enhanced or reduced measures (R.5 to 8) ... 65
3.3 Third parties and introduced business (R.9) ... 77
3.4 Financial institution secrecy or confidentiality (R.4) ... 78
3.5 Record keeping and wire transfer rules (R.10 & SR.VII) ... 79
3.6 Monitoring of transactions and relationships (R.11 & 21) ... 83
3.7 Suspicious transaction reports and other reporting (R.13-14, 25 & SR.IV) ... 85
3.7A Large transaction and cross-border transaction reporting (R.19 & SR IX) ... 91
3.8 Internal controls, compliance, audit and foreign branches (R.15 & 22) ... 95
3.9 Shell banks (R.18) ... 98
3.10 The supervisory and oversight system - competent authorities and SROs: Role, functions, duties and powers (including sanctions) (R.17, 23, 29 & 30) ... 98
3.11 Financial institutions - market entry and ownership/control (R.23) ... 102
3.12 AML/CFT Guidelines (R.25) ... 104
3.13 Ongoing supervision and monitoring (R.23, 29 & 32) ... 105
3.14 Money or value transfer services (SR.VI) ... 107
4 PREVENTIVE MEASURES – DESIGNATED NON-FINANCIAL BUSINESSES AND PROFESSIONS ... 109
4.1 Customer due diligence and record-keeping (R.12) (applying R.5 to 10 to DNFBP) ... 109
4.2 Monitoring of transactions and relationships (R.12 & 16) (applying R.11 & 21 to DNFBP) 111
4.3 Suspicious transaction reporting (R.16) (applying R.13 & 14 to DNFBP) ... 112
4.4 Internal controls, compliance & audit (R.16) (applying R.15 to DNFBP) ... 113
4.5 Regulation, supervision and monitoring (Applying R.17 and 24-25 to DNFBP) ... 114
4.6 Other non-financial businesses and professions: Modern secure transaction techniques (R.20). 119
4 LEGAL PERSONS AND ARRANGEMENTS & NON-PROFIT ORGANISATIONS ... 120
5.1 Legal Persons – Access to beneficial ownership and control information (R.33) ... 120
5.2 Legal Arrangements – Access to beneficial ownership and control information (R.34) ... 123
5.3 Non-profit organisations (SR.VIII) ... 124
5 NATIONAL AND INTERNATIONAL CO-OPERATION ... 125
6.1 National co-operation and coordination (R.31) ... 125
6.2 The Conventions and UN Special Resolutions (R.35 & SR.I) ... 126
6.3 Mutual Legal Assistance (R.32, 36-38, SR.V) ... 128
6.4 Extradition (R.32, 37 & 39, & SR.V) ... 133
6.5 Other Forms of International Co-operation (R.32 & 40, & SR.V) ... 136
6 OTHER ISSUES ... 139

7.1 Other relevant AML/CFT measures or issues 139

Preface - information and methodology used for the evaluation

1. The evaluation of the anti-money laundering (AML)[1] and combating the financing of terrorism (CFT) regime of Norway was based on the Forty Recommendations 2003 and the Eight Special Recommendations on Terrorist Financing 2001 of the Financial Action Task Force (FATF), and was prepared using the AML/CFT Methodology 2004. The evaluation was based on the laws, regulations and other materials supplied by Norway, and information obtained by the evaluation team during its on-site visit to Norway from 17-28 January 2005, and subsequently. During the on-site the evaluation team met with officials and representatives of all relevant Norwegian 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. John Carlson and Ms. Valerie Schilling from the FATF Secretariat, Mr. Richard Berkhout, Senior Policy Advisor, Integrity Division, Financial Markets Policy Directorate, Ministry of Finance (the Netherlands) who participated as a financial expert; Mr. Eric Chan, Director (International & Regional Relations), External Department, Monetary Authority of Singapore (Singapore) who participated as a financial expert; Mr. Nils-Gunnar Danielsson, Detective Superintendent, Financial Unit, Finanspolisen/Rikspolisstyrelsen (NFIS) (Sweden) who participated as a law enforcement expert; Mr. Pieter Smit, Senior Manager, Strategic Research, Financial Intelligence Centre, National Treasury (South Africa) who participated as a legal expert. The assessment team reviewed the institutional framework, the relevant AML/CFT laws, regulations, guidelines and other requirements, and the regulatory and other systems in place to deter money laundering (ML) and the financing of terrorism (FT) through financial institutions and Designated Non-Financial Businesses and Professions (DNFBP), as well as examining the capacity, the implementation and the effectiveness of all these systems.[2]

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

[1] See Annex 1 for a complete list of abbreviations and acronyms.

[2] See Annex 2 for a detailed list of all bodies met during the on-site mission.

See Annex 3 for copies of the key laws, regulations and other measures.

See Annex 4 for a list of all laws, regulations and other material received and reviewed by the assessors.

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

EXECUTIVE SUMMARY

1 BACKGROUND INFORMATION

1. This report provides a summary of the AML/CFT measures in place in Norway 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 Norway's levels of compliance with the FATF 40+9 Recommendations (see the attached table on the Ratings of Compliance with the FATF Recommendations).[4] Recent AML/CFT priorities have been to increase the effectiveness of measures to detect, prosecute, and confiscate proceeds of crime; enhance international co-operation; competence building; comply with the current EU Money Laundering Directive; and train the 27 specialised economic crime units.

2. In the last 10 years, Norway has seen an increase in profit-motivated crime (especially drug-related and economic crime). Serious crime in Norway has been characterised by the following general trends: better organisation and increased flexibility; increased internationalisation, specialisation and professionalism; increased co-operation between criminal networks and links with legal business activity, and more use of advanced technologies. Recent threat assessments conclude that organised crime and criminal networks are gaining more of a foothold and that money laundering continues to be characterised by extensive use of cash. A recent attempt to analyse possible connection between terrorist financing and organised crime does not provide basis for any definitive conclusions.

3. The following types of financial institutions are authorised to operate in Norway: savings banks, commercial banks, finance companies and mortgage companies; life and non-life insurance companies, e-money institutions, investment firms, security funds management companies and branches of foreign financial institutions. All are supervised by the Financial Supervisory Authority of Norway (*Kredittilsynet*) (the FSA). Foreign exchange offices (i.e. bureaux de change) and money/value transfer service (MVTS) providers are formally not permitted to operate in Norway as separate entities, though banks, finance companies and EEA branches of such undertakings are allowed to carry out such financial activities.

4. The following types of non-financial businesses and professions operate in Norway: real estate agents, auditors and accountants (supervised by the FSA), lawyers (supervised by the Supervisory Council for Legal Practice (Supervisory Council), and dealers in precious metals and stones (not supervised for AML/CFT). Notaries do not exist in Norway. Casinos (including Internet casinos) are not allowed to operate in Norway, though Norwegians may gamble on Internet casinos that are operated from a server located in another country, and Norwegians may offer such a service in Norway from outside Norway. Trust and company services are normally provided by lawyers and auditors. Trust and company services providers are not recognised as separate businesses.

2 LEGAL SYSTEM AND RELATED INSTITUTIONAL MEASURES

5. Norway has criminalised money laundering under s.317 of the Penal Code. Charges can be brought for different types of money laundering, ranging in seriousness from drug-related money laundering to negligent money laundering. Overall, these offences are broad in scope and apply to all crimes. The offences have also been actively and successfully used, with the prosecuting authorities bringing 1 693 cases since 2000, and achieving a high conviction rate (about 85%), particularly considering that all convictions are for third party money laundering. Negligent money

[4] Also see the attached table on the Ratings of Compliance with the FATF Recommendations for an explanation of the compliance ratings (C, LC, PC and NC).

laundering is also criminalised. Some minor enhancements that could be made to an otherwise effective regime include extending the offence to self-laundering and conspiracy (which is currently only an offence if three or more people conspire in the context of an organised criminal group), increasing the use of more serious money laundering charges, and modifying the structuring/penalties of the different types of money laundering offences.

6. Terrorist financing is an autonomous offence under s.147b of the Penal Code, and covers obtaining or collecting funds or other assets with the intention that they are to be used to finance terrorist acts. This term "terrorist acts" refers to a range of existing criminal offences committed with certain specific intentions. Although Norway's criminalisation of terrorist financing is generally in line with the Terrorist Financing Convention, Norway should clarify its legislation to ensure that the offence covers collecting funds in the knowledge that they are to be used (for any purpose) by a terrorist organisation/individual terrorist. The offence is punishable by up to 10 years imprisonment. There has been one investigation but no prosecutions for terrorist financing in Norway.

7. In recent years, Norway has focused on measures that could enhance its ability to deprive criminals of the proceeds of crime, and the innovations adopted have been largely successful. The law provides for two types of provisional measures—charging and seizing (which in practice, operates like a freezing mechanism for certain types of assets, such as funds in a bank account) and these measures are sufficient in most cases. The police and the prosecution authorities have a full range of powers to identify and trace assets.

8. Confiscation of the proceeds from any criminal offence or property of corresponding value is mandatory. Proof on the criminal standard that a specific criminal offence generated the proceeds is required; however, the burden of proof is eased to the civil standard concerning the amount of the proceeds which may be confiscated. Extended confiscation measures are also possible in serious cases, meaning there is a presumption that all of the defendant's property is illegally acquired. Proceeds or instrumentalities of crime can be confiscated from a third party in a range of circumstances. Overall, Norway has implemented a comprehensive confiscation system that is achieving results. In 2003, over 900 confiscation orders totalling over NOK 140 million (€17 million) were issued.

9. United Nations Security Council Resolution (UNSCR) S/RES/1267(1999) and its successor resolutions are implemented by an enabling statute and regulations. These laws provide some of the necessary measures by creating an authority to freeze, automatically incorporating any changes to the lists into the legal system, prohibiting anyone from making any funds available to entities listed, and providing for penalties of fines or imprisonment. Freezing can be legally challenged using normal legal mechanisms for challenging government decisions. Despite this, there is a lack of guidance to institutions and persons holding targeted assets, and no measures to monitor compliance. Norway has frozen one bank account under S/RES/1267(1999), and the effectiveness of the regime is noticeably reduced by the absence of further policies and procedures to handle freezing cases.

10. Norway has implemented S/RES/1373(2001) by enacting special provisions in its criminal procedure law, thus allowing property to be frozen when a person is suspected of terrorist offences. The decision to freeze is not based on a national list, but on a case-by-case assessment based on evidence (to the "more than 50% likely" standard) that the person has/has attempted to obtain/collect funds and assets in respect of the commission of terrorist acts or made funds available to terrorists/terrorist organisations. However, because the scope of the terrorist financing offence is not quite broad enough, Norway would be unable to freeze the assets of a person who is considered to have collected funds in the knowledge that they are to be used generally (for any purpose) by a terrorist organisation/individual terrorist. Moreover, there are no clear channels for communicating freezing actions taken under S/RES/1373(2001), no guidance to entities that may

be holding assets covered by such a freezing action, and no system for monitoring compliance. With regards to S/RES/1373(2001), Norway has never found any funds/assets inside of Norway. Consequently, the freezing mechanisms that it has enacted in its criminal procedure law for this purpose has never been triggered. Overall, the freezing regime in Norway has implemented only some of the elements of Special Recommendation III. There is a lack of clear procedures for unfreezing and de-listing requests, authorising access to assets on humanitarian grounds, monitoring compliance and applying sanctions. An effective system for communication between government and the private sector needs to be established, and clear guidance provided to financial institutions.

11. Norway's financial intelligence unit, the Money Laundering Unit (MLU), is located within the National Authority for Investigation and Prosecution of Economic and Environmental Crime (ØKOKRIM) and has been a member of the Egmont Group since 1995. Suspicious transaction reporting in Norway takes place in two stages: (a) where a reporting entity suspects that a transaction is associated with the proceeds of crime, it must make further inquiries; (b) if those inquiries do not dispel the suspicion, then an STR has to be made to the MLU. The transaction can be temporarily frozen by the MLU: this power is exercised only a few times a year. In January 2005, the MLU had 11½ employees, seven of which analysed STRs. This level of staffing is inadequate to deal with the volume of STRs that the MLU currently receives (more than 5 000 in 2004). This is exacerbated by the MLU's manual processes such as an inability to receive STRs electronically and the lack of analytical software tools. An electronic reporting system and a new, improved STR database are due to be implemented. MLU staff have sufficient powers to obtain information from police, other government officials and foreign FIUs, can demand additional information from reporting entities, and has direct access to a wide range of databases. The MLU is subject to the oversight of the Control Committee; however, this oversight only extends to the protection of privacy and personal data. The Committee is an independent body that reports to the Ministry of Finance. While the Committee does not interfere with the MLU's independence; its intervention does impact the overall effectiveness of the MLU in that a disproportionate amount of the MLU's limited resources are now directed towards considering whether to delete or justify retaining old STR files. Information about an STR must be deleted if a suspicion is rebutted, or if after five years no investigation or legal measures have been initiated. Although, on paper, the MLU generally meets the literal requirements of Recommendation 26, its lack of effectiveness causes concerns and impedes the overall effectiveness of Norway's AML/CFT system. The MLU is understaffed, under-resourced and technologically ill-equipped, and though MLU staff are doing what they can given these limitations, the whole issue needs to be addressed. Norway should ring-fence the responsibilities and resources of the MLU.

12. The Norwegian police service is comprised of the Police Directorate, the Police Security Service (PST), the 27 police districts, and centralised institutions like ØKOKRIM, New Kripos and the Police College. They work closely with the Prosecution Authority. ØKOKRIM is responsible for investigating complex economic crime (including money laundering), while all police districts have established separate teams to combat economic crime. Money laundering offences and confiscation cases are investigated in every police district, and terrorist financing is investigated by the PST or by ØKOKRIM. Law enforcement has initiated 2 342 money laundering investigations. Police and prosecutors have all the normal search and seizure powers, as well as powers to use special investigative techniques such as secret search and seizure, though some powers can only be used for more serious offences, thus limiting their availability for use in money laundering. Other covert measures, such as undercover operations are available, but are not statutorily regulated. Training is provided to police and prosecutors on economic crime, however, this should be expanded to meet the needs in the area.

3 PREVENTIVE MEASURES - FINANCIAL INSTITUTIONS

13. The current Norwegian AML legislation was adopted in June 2003, but does not yet take into account the full obligations set out in the revised FATF Recommendations (2003). Norway's

customer identification measures are based on implementation of the 1st and 2nd EU Money Laundering Directives and the FATF Recommendations (1996). Norway reports that it has been waiting until the 3rd EU Money Laundering Directive (which was just adopted) was finalised before doing so. There are no higher risk categories of customers or products, and the lower risk categories have been implemented in line with the EU Directives. The AML measures under the Money Laundering Act (MLA) and Regulations (MLR) apply to all the financial institutions that must be covered under the FATF Recommendations (referred to as "Reporting FIs" in Norway).

14. Although Norway has implemented basic customer identification obligations, it has not implemented full customer due diligence (CDD) requirements. Reporting FIs are required to identify permanent and occasional customers (for large value transactions). A natural person's identity is normally verified by producing a document issued by a public authority, which normally contains full name, signature, photograph and personal identity number or D-number. (Non-residents liable to pay tax are registered with a unique D-number.) A legal person's identity is verified by checking certain Registers. Where the customer is unable to produce the required identity documents, the Reporting FI should generally refuse to establish a customer relationship. There are exemptions from the identification obligations if the customer is a Norwegian or EEA credit institution or investment firm, and for low value insurance contracts.[5] Overall, there are weaknesses regarding the implementation of Recommendation 5, as the only measure currently in place is a bare requirement to identify customers. Elements going beyond the initial establishment of the customer relationship such as beneficial ownership and other elements of CDD are not required. These deficiencies need to be addressed. In addition, specific identification requirements and procedures should be introduced that are tailored to the business practices of sectors other than banking. Norway should also implement the applicable measures for politically exposed persons (PEPs) and correspondent banking (R.6 & 7).

15. Normally, the establishment of non-face-to-face business relationships is not allowed and the customer must physically appear either at the Reporting FI or at an agent or outsourcee, where identification and verification is performed. Where there is outsourcing, the Reporting FI must ensure that the outsourcee conducts the customer identification and verification properly, maintains proper records, and properly trains its employees. Reporting FIs cannot rely on verification performed by another Reporting FI, even those that are part of the same financial group, and introductory business is generally not permitted. A legal duty of confidentiality requires employees of financial institutions to keep customer information confidential, but does not inhibit disclosure of information to the MLU, nor impede the FSA in performing its supervisory role. Indeed, banks, finance companies and insurance companies are allowed to exchange customer data when investigating suspicious transactions. It is recommended this authority be extended to other types of financial institutions. Record keeping requirements are generally satisfactory, with Reporting FIs being obligated to retain copies of any documents used to verify the customer's identity for five years after termination of the customer relationship, and to keep transaction records for ten years. The MLA requires relevant originator information to be kept for all permanent customers and the Currency Register Act and Regulations effectively extend this to occasional customers conducting any cross border wire transfer. However, in other respects, SR VII has not been implemented and this should be rectified.

16. Banks and finance companies were legally obliged to establish electronic monitoring systems before the end of 2004. Norway's initial experience with its new electronic monitoring system for banks and finance companies is a pattern of reporting that focuses more on the nature of the transaction, and not just the nationality of the customer and cash transactions. Monitoring of unusual transactions is conducted, the NCCT list is published and additional NCCT

[5] In the context of Recommendation 5, the Norwegian regime exempts their financial institutions from certain AML/CFT obligations in relation to financial institutions that are located in countries belonging to the European Economic Area. The FATF decided at the June 2005 Plenary to further consider this subject.

countermeasures applied. Reporting FIs are required to report transactions to the MLU when there is a suspicion that the transaction is related to money laundering or terrorist financing, and are exempt from liability when they report to the FIU in good faith. "Tipping off" a customer or any third party in connection with reporting a STR to the MLU is prohibited. Banks and MVTS providers report the largest number of STRs, though none of them were related to terrorist financing. It is a concern that the number of STRs being reported by other non-bank financial institutions is very small, and the number of STRs from banks is also decreasing.

17. Norway has recently revised its declaration system and also its systems for monitoring cross-border transportations of currency (cash). The declaration system is now administered by the customs authorities and is regulated in the customs legislation. A new Currency Register Act provides for storing declaration information in a Currency Transaction Register. The police have direct access to the Register when a criminal investigation has been initiated. The declaration system applies to all incoming and outgoing cross-border transportations of currency equal to or exceeding NOK 25 000 (€ 3 000) or the equivalent value in a foreign currency. Name, date of birth, personal identification number or passport number, the amount/value transported and the date are recorded as is for amounts above NOK 100 000 (€ 12 100), the purpose of the transportation. The legal measures are broadly adequate, and allow the police to stop smuggled money when it is detected, giving the police time to investigate the money in question. There is no obligation to declare bearer negotiable instruments when entering or leaving Norway. However, when foreign negotiable instruments are cashed, this is reported to the Currency Transaction Register. Norway indicates that the reason for this is that the transaction occurs when the instrument is cashed, and also avoids the double reporting of transactions in the Register.

18. All Reporting FIs must establish certain internal control and communications procedures, and appoint an AML officer. Reporting FIs must have an internal audit function and designate an AML/CFT compliance officer person within senior management. Special training programmes for employees and other relevant persons on AML/CFT obligations are required. While these measures are generally satisfactory regarding checking the existing laws, they do not implement the full range of measures required under the Recommendations and it appears that institutions have not voluntarily implemented higher standards. Foreign branches of Norwegian institutions are obligated to observe AML/CFT measures consistent with Norwegian requirements and the FATF Recommendations to the extent that the host country's laws permit. Norway has not yet had any cases of foreign subsidiaries of Norwegian institutions being established abroad in countries that are considered to have lesser AML/CFT measures than Norway. Norway should implement an obligation to inform the FSA if a foreign branch or subsidiary is unable to observe appropriate AML/CFT measures. Shell banks are indirectly prohibited in Norway. However, there are no provisions prohibiting financial institutions from entering correspondent banking relationships with shell banks or obligating institutions to satisfy themselves that their foreign respondent institutions do not permit their accounts to be used by shell banks. All these measures should be introduced as soon as possible.

19. The FSA is an independent government agency, responsible for supervising the Norwegian financial sector. The licensing function is divided between the Ministry of Finance and the FSA. When a financial institution is granted a licence, checks are conducted to ensure that the general manager and directors meet fit and proper requirements. This includes a criminal records check. Supervisory resources are allocated on a risk sensitive basis and the FSA looks to co-ordinate its prudential approach with its AML/CFT supervision. The FSA has adequate powers to supervise and inspect the policies, practices and internal controls of Reporting FIs. It is also authorised to impose a broad range of administrative sanctions for non-compliance, from letters requesting corrective action, orders through to fines or de-licensing. Sanctions can be applied against both institutions and officers/employees, though its powers to do the latter should be clarified. To date the FSA has imposed sanctions for breaches of AML/CFT obligations in the form of issuing letters requesting that corrective action be taken.

20. At the end of 2003, the FSA had 183 employees responsible for supervising 2 518 separate entities, including designated non-financial businesses and professions (DNFBPs) (except lawyers and dealers). Considering the number of entities that the FSA is responsible for supervising, this seems to be an inadequate number of staff. In the past six years, the FSA has conducted between 100-120 on-site inspections per year, in addition to off-site reviews. Although AML/CFT assessments are integral part of the FSA's regular visits, they seem to be limited in scope and not conducted frequently enough. For smaller financial institutions, AML/CFT assessments are not held annually, but only when there are indications that an assessment would be necessary. Only 12 thematic inspections focusing solely on AML issues have been conducted. The assessors found that some of these institutions (deemed to be high risk) had just been assessed for the first time in seven years, and the assessment found some major shortcomings. This situation needs to be reviewed. The FSA should consider how it can best enhance focus on AML/CFT issues, for example, by having a team of examiners that checks compliance with AML/CFT on an ongoing basis for all supervised entities.

21. Some steps have been taken concerning guidance. The FSA has issued Circular 9/2004 to reporting entities on how to comply with their obligations, while the MLU has also given some sporadic guidance and participates in seminars for the private sector. However, the guidance seems to have been insufficient, and reporting entities (both financial institutions and DNFBPs) met by the assessment team asked for additional and more sector-specific guidance (particularly in the area of typologies). Additionally, the MLU should enhance its general and specific feedback concerning the status of particular STRs and the outcome of certain specific cases.

22. Unauthorised MVTS providers are illegal, and Norway has detected some underground banking. Two cases have been successfully prosecuted. Regulated MVTS providers (banks) are subject to the FATF Recommendations, albeit not adequately. This negatively impacts on the effectiveness of AML/CFT measures in the MVTS and other financial institution sectors. Norway should take steps to properly implement Recommendations 5-7, 15 and 22, and SR VII overall. The FSA is responsible for licensing and monitoring MVTS operators, however, there are concerns about the effectiveness of this supervision. The FSA is taking action to correct these problems.

4 PREVENTIVE MEASURES – DESIGNATED NON-FINANCIAL BUSINESSES AND PROFESSIONS

23. The following DNFBP are subject to AML/CFT obligations: real estate agents, dealers in objects, including precious metals/stones, in connection with cash transactions of NOK 40 000 (€ 4 800) or more, lawyers and other independent legal professionals, auditors and accountants (collectively referred to as Reporting BPs). Land-based casinos, notaries and trust/company service providers (as a separate defined business sector) do not exist in Norway. Although the large majority of company services are handled by lawyers and accountants, there is no legal prohibition from other persons establishing such businesses in Norway. Norway should clarify the law to ensure that anyone providing such service is covered. This may include amending the law to restrict the provision of company services to only accountants and lawyers to reflect the current practice.

24. For the most part, AML/CFT obligations for Reporting FIs/BPs are the same. Consequently, the same deficiencies in the implementation of customer identification requirements (Rec.5) exist. Customer identification requirements have been implemented, but full CDD requirements have not. Nor have any measures concerning PEPs (Rec.6) been implemented in the DNFBP sectors. Norway should correct these deficiencies as a matter of priority. All dealers in objects, including dealers in precious metals/stones, auctioneering firms, commission agents and the like, are obligated to identify their customers when carrying out cash transactions involving NOK 100 000 (€ 12 100) or more, or suspicious transactions involving NOK 40 000 (€ 4 800) or more. In the latter case, an STR must be filed with the MLU. However, overall it is unclear how effectively dealers in precious metals/stones

are complying with AML/CFT requirements because they are not monitored or supervised in this regard. Norway should designate an authority responsible for doing so. Occasional customer rules do not apply to lawyers, independent legal professionals, real estate agents, accountants or auditors since, due to the nature of their work, they do not have occasional customers.

25. In general, Reporting BPs have satisfactorily implemented record keeping requirements. Although Reporting BP are not allowed to establish non-face-to-face business (customers must physically appear at the Reporting BP or its agent/outsourcee for identification and verification), there are some concerns about the effectiveness of this system in practice. All of the Reporting BP met with had established internal AML/CFT controls and communication routines as required. Reporting BP must monitor their accounts and report suspicious activity to the MLU. Lawyers are only obliged to report suspicious transactions when assisting or acting on behalf of clients in planning or carrying out financial transactions, with certain exceptions. So far, only lawyers, accountants, auditors and real estate agents have filed STRs; dealers in precious metals/stones have not. However, this obligation is quite new for most Reporting BPs. Nevertheless, there are preliminary concerns about effectiveness because most of the DNFBP sectors met with during the on-site visit (particularly real estate agents, accountants, auditors, and dealers in precious metals/stones) requested more sector-specific guidance (particularly typologies). Although the FSA has issued general AML/CFT guidelines to real estate agents, accountants and auditors (Circular 9/2004), more tailored and sector-specific guidance should be issued to the Reporting BPs as soon as possible to address these concerns. Currently, two working groups are set up in order to propose such guidelines for lawyers and auditors/accountants. The NARF (Norway's major professional body for authorised external accountants) is currently developing a quality control programme for external accountants.

26. Real estate agents, accountants and auditors must be licensed by the FSA in order to be authorised to carry out their business. The FSA supervises these entities, issues guidance to them on an ad hoc basis and is empowered to apply administrative sanctions. However, the FSA does not appear to have sufficient resources to do so effectively. The FSA has not started inspecting accountants/auditors because the scope of their reporting obligation has not been fully clarified. The Supervisory Council licenses, supervises, audits and sanctions the legal professionals. The Supervisory Council conducts between 50-70 audits per year of law firms, including checks on AML/CFT compliance. The Supervisory Council has only uncovered one case of money laundering by a lawyer. The Norwegian Bar Association (NBA) has issued binding ethical guidelines for lawyers (which specifically refer to ML) and has compiled a template for internal controls and communication routines. It is also in the process of participating in a Ministry of Justice & Police committee to draft AML/CFT guidelines for legal professionals. Dealers in precious metals/stones are obliged to register their activity or company, but do not need to be licensed or authorised to conduct business. This sector is not supervised or monitored by any agency for compliance with AML/CFT obligations, although industrial associations play a role in helping members to understand and apply new legal requirements, including those related to AML/CFT. The MLU has taken the initiative, passing on information about Norway's new AML/CFT legislation to industry organisations such as NHO and HSH. Nevertheless, without any supervision or monitoring, there is no way of assessing how effectively AML/CFT measures are being implemented in this sector. Norway should designate an authority to fulfil this role.

27. Although there are no land-based casinos in Norway, limited and closely regulated internet gaming does exist. Although having an ownership interest in an internet casino is not expressly prohibited, Norway reports that such activity could be stopped pursuant to existing gaming legislation. However, Norway has not taken any measures to identify whether any Norwegian residents/citizens currently own or operate an internet casino, a company that runs an internet casino or a server located in Norway which hosts an internet casino. Nor has any guidance been issued to Reporting FIs/BPs alerting them to the possible existence of such entities and how to treat them. Norway should be aware of issues relating to the illicit operation of internet casinos in

Norway, and should be prepared to address these problems.[6] Additionally, Norway's efforts to encourage the development and use of modern, secure techniques for conducting financial transactions that are less vulnerable to money laundering should continue.

5 LEGAL PERSONS AND ARRANGEMENTS & NON-PROFIT ORGANISATIONS

28. Norway has several registries for legal persons. All Norwegian legal persons, and Norwegian and foreign companies or other legal persons conducting business activities in Norway are obligated to register with one or more registers. Registered information concerning a particular legal person can be readily retrieved by virtue of Norway's single number identification system. Norway has also implemented measures to ensure that this information is updated. Additionally, Norway obligates all Norwegian private and public limited companies to establish and maintain a register of all shareholders that must be kept up-to-date and must be made available to anyone who asks. Foreign companies are allowed to own shares of Norwegian companies and, in such cases, the register of shareholders will identify the foreign company. Norwegian authorities are entitled to ask the foreign company for that information. However, the information accessible will depend on home state requirements.

29. These measures ensure that accurate, adequate and reasonably current information concerning the ownership and control of Norwegian legal persons is readily accessible to competent authorities in a timely fashion. However, it should be noted that these measures do not expressly relate to information concerning beneficial ownership (as that term is used in the FATF Recommendations). Nevertheless, Norway has implemented additional measures that go some way to ensuring that the person who exercises ultimate effective control over a legal person can be identified. First, listed public companies are subject to shareholder disclosure rules. Second, Norwegian law prohibits the buying/selling of shares through a nominee, except as regards foreign investors, and then only with safeguards to ensure transparency. Third, bearer shares do not exist in Norway. Nevertheless, concerning beneficial ownership, additional steps could be taken to provide more timely access to this sort of information.

30. Charitable organisations are not obligated to register; however, their bank accounts must be opened in the name of a natural person who is a member. The FSA specifically advises Reporting FIs/BPs that collection accounts for charitable organisations should not be exempt from the requirements to produce identity documents. Nevertheless, this situation is unsatisfactory because it hinders the bank's ability to identify the actual owners of funds in an account and leaves the natural person (in whose name the account is registered) subject to tax on the funds concerned. The system is further weakened by the fact that Recommendation 5 has not been implemented with regards to beneficial ownership. Norway has not reviewed its laws/regulations relating to non-profit organisations (NPOs) as required by Special Recommendation VIII. Norway should do so, and implement appropriate CFT measures in this sector. Norwegian law does not recognise the legal concept of a trust or similar legal arrangements, including trusts created in other countries.

6 NATIONAL AND INTERNATIONAL CO-OPERATION

31. With a few exceptions, Norway has fully implemented the elements of the Vienna, Palermo and Terrorist Financing Conventions that are relevant to the FATF Recommendations. Norway has largely implemented the basic legal provisions of S/RES/1267(1999), but should implement measures to monitor or supervise for compliance with these requirements. Norway's implementation of S/RES/1373(2001) should be improved.

[6] These observations have not affected Norway's rating on compliance with the FATF Recommendations (in particular, Recommendations 12, 16 or 24). The FATF decided at the June 2005 Plenary to study the issue of internet casinos to clarify AML/CFT obligations in relation to this activity.

32. On an operational level, the FSA is authorised to co-operate with other domestic supervisors, law enforcement authorities and foreign supervisors for AML/CFT purposes. Several informal mechanisms, including regular contact meetings and forums exist to improve interagency co-operation between the police, Prosecution Authority, MLU, customs and tax authorities and supervisors with regards to AML/CFT. There is still room for improvement in more effective interagency co-operation.

33. Mutual legal assistance and extradition measures apply equally to money laundering and terrorist financing matters. Norway can respond to both mutual legal assistance and extradition requests in the absence of an applicable treaty. Extradition to Nordic countries is regulated by the Nordic Extradition Act (NEA). Extradition to other countries is regulated by the Extradition Act (EA). Mutual legal assistance is regulated by a separate chapter of the EA. Norway is party to international agreements facilitating mutual legal assistance within the Nordic region, the EU and between Schengen countries. Mutual legal assistance requests from non-Nordic countries seeking coercive measures are subject to the requirement of dual criminality. Although in general, there are no legal or practical impediments to rendering assistance, provided that both Norway and the requesting country criminalise the conduct underlying the offence, the application of dual criminality may create obstacles to both mutual legal assistance and extradition where the underlying offence relates to the following types of money laundering/terrorist financing activity that have not been properly criminalised in Norway: (i) self-laundering; (ii) conspiracy of 2 people to commit money laundering; and (ii) obtaining or collecting funds/assets to be used by a terrorist organisation/individual terrorist (for any purpose) where those funds have not yet been provided to the terrorist organisation/individual terrorist . Norway should take measures to address this problem, in particular, by properly criminalising these activities. Requests from non-Nordic countries (other than Nordic and Schengen countries) must also meet some of the requirements for extradition. Neither dual criminality nor the requirement that the underlying offence be extraditable apply to mutual legal assistance requests from Nordic countries.

34. Generally, mutual legal assistance requests are forwarded through the Ministry of Justice & Police. Norway reports that requests are given priority; however, there are no statistics concerning the length of processing times for either mutual legal assistance or extradition requests. Procedures for processing mutual legal assistance requests from Nordic and Schengen countries (which, given Norway's geographical location, would usually account for the majority of requests) are streamlined and can be sent directly between judicial authorities. Mutual legal assistance requests from other countries must always proceed by letters rogatory (which is not efficient). Duties of confidentiality do not impede mutual legal assistance. Assistance can be provided even where the offence is considered to involve fiscal matters. A wide range of mutual legal assistance can be provided, including compelling witness testimony, order the production of documents and seizing evidence. Norway co-operates closely on a global and region level to avoid conflicts regarding investigation/prosecution of cases concerning transnational crime.

35. Where a foreign state (that is not a signatory to the Vienna or Strasbourg Conventions) requests Norway to execute a foreign freezing/seizing/confiscation order, Norway can only recognise the order, but cannot give effect to it without starting its own proceedings. A procedure that requires a case to be made out before a local (Norwegian) court on the basis of foreign evidence is inherently less effective than one where the Norwegian court satisfies itself that a foreign court has made a freezing/seizing/confiscation order, and then simply gives effect to that order. Norway should enhance the effectiveness of its system by enacting legislation that would clearly allow for confiscation in situations other than those covered by the Vienna and Strasbourg Conventions, and should consider enacting measures that would allow it to give effect to a foreign freezing/seizing/confiscation order without the necessity of starting its own domestic proceedings. Although, to the best of Norway's recollection, no such requests have been made, Norway recognises that this issue will have to be addressed as it goes forward and as requests for international co-operation increase. Although there are no special permanent arrangements for co-ordinating seizure/confiscation actions with other countries, Norway does co-ordinate on a case-to-case basis. No asset forfeiture fund exists.

36. Both money laundering and terrorist financing are extraditable offences. Norwegian nationals may not be extradited (except to Nordic countries). When extradition is refused on this basis, the case will be forwarded upon request to the Prosecution Authority for a determination of whether domestic proceedings should be initiated. Extradition must be refused if there is a grave danger that the person concerned will suffer persecution directed against his life/liberty for reasons of race, religion, nationality, political convictions or other political circumstances. Proceedings may be transferred in the absence of an international convention. Dual criminality is applied to extradition requests (except those to Nordic countries). Norway collects statistics (which are not always reliable) on the number of requests for mutual legal assistance, extradition, freezing/seizing/confiscation and requests from foreign FIUs. However, Norway should keep additional statistics, including those relating to the nature of mutual legal assistance/extradition requests, whether the request was granted/refused, and how much time was required to respond. Norwegian law enforcement authorities are authorised to conduct investigations on behalf of foreign counterparts. They also have well-functioning systems of electronically stored information that is easy to find and easy to forward to other countries. Information is exchanged with foreign counterparts on the condition that it only be used for professional purposes, and is not made subject to disproportionate or unduly restrictive conditions. Generally, the attitude of Norwegian law enforcement is to respond rapidly to requests from co-operating agencies abroad.

37. The MLU can exchange information with foreign FIUs (both police/prosecution-based FIUs and administrative FIUs), both spontaneously and upon request, without an MOU. The MLU has an MOU with the Belgian FIU and requests from nine other foreign FIUs are pending. Norway should finalise these MOU as soon as possible to avoid the negative impact created by a situation where the foreign FIU needs to have an MOU in order to be able to co-operate. When responding to requests from foreign counterparts, the MLU can use the information from its own database and others that it has access to (including law enforcement and public databases). However, last year, due to a technical failure, connectivity with the Egmont Secure Web System, the MLU was lost for about three months. The technical problem was resolved and the MLU has designated staff to deal with international requests; however, it is too early to assess how effective these new measures will be**.** Norway should ensure that these new systems are working effectively.

38. Norway is a party to a number of international agreements and participates in working groups that are targeted at facilitating co-operation within the EU in various sectors, including insurance and securities. Norway has negotiated MOUs with foreign supervisory authorities in the banking and investment sector. Norwegian supervisory authorities may co-operate spontaneously with foreign supervisory authorities, even in the absence of any applicable agreement or statutory provision provided that the execution of the request is not contrary to Norwegian law. For instance, the FSA has co-operated with its foreign counterparts in relation to on-site inspections of Nordic banking groups. As a general rule, the Customs Directorate co-operates with its foreign counterparts on the basis of MOUs. However, the Norwegian customs authorities also may exchange information with other countries according to the customs legislation. Information may be exchanged provided that information can be shared on a mutual basis and the recipient stores and protects the information properly.

MUTUAL EVALUATION REPORT

1 GENERAL

1.1 General information on Norway

1. Fully independent since 7 June 1905, the Kingdom of Norway covers an area of 385 155 square kilometres, including the islands of Jan Mayen and Svalbard.[7] The capital of Norway is Oslo. The population of Norway is approximately 4.6 million persons with a literacy level of virtually 100% (as of 1 January 2004). Listed as one the richest countries in the world, Norway's population enjoys a high standard of living. Life expectancy averages 78.7 years (as of 2001). The official languages are Norwegian (99.5%) and Sami (0.5%). The age of majority is 18.

2. Norway is not a member of the European Union (EU), but participates in the EU common market as a signatory of the European Economic Area Agreement (EEA Agreement) and therefore is bound to implement some EU legislation. For instance, according to the EEA Agreement, the 1ST and 2nd EU Money Laundering Directive is binding on Norway. Norway has also participated in Schengen since 25 March 2001. Norway is a developed, industrial country with an open, export-oriented economy. In the last century, Norway enjoyed a period of continuous economic growth. Since the 1970s, the offshore oil industry has played a dominant role in the Norwegian economy, securing stable growth. Throughout this development Norway has maintained a mixed economy, with considerable participation of state-owned companies and banks.

3. Norway is a constitutional monarchy with a parliamentary democratic system of governance. Election turnout is usually about 77-78%. The executive branch of government is comprised of the King (the head of state), the Prime Minister (the head of Cabinet) and the Council of Ministers (the Cabinet). The legislative branch of government is the *Storting* (a modified unicameral parliament of elected representatives). The judicial branch of government is comprised of the Supreme Court, the Interlocutory Appeals Committee of the Supreme Court, the Courts of Appeal and the District Courts. Political power is geographically divided into state, county and municipal levels. Norway is administratively divided into 19 counties.

4. The Norwegian Constitution of 1814 builds on principles similar to those found in the French and American Constitutions. Norway's legal system combines customary law, common law traditions and a civil law system. Primary legislation is in the form of laws. Secondary legislation is in the form of regulations. Both may be further explained in "preparatory works", the purpose of which is to give explanations to the Parliament prior to the adoption of new legislation and to give guidance to the users of the legislation after the adoption of the bill.

5. The explanations contained in preparatory works are regarded as clarification of vague legal texts, very much in the same way as case law. According to established principles of legal interpretation, there is an undisputable duty on courts and other professional interpreters of statutory law to take into consideration what is said in the preparatory works. The circumstances determine what weight should be attached to such explanations. For instance, no weight will be attached to them if they contradict the wording in the legislation. However, Norwegian courts will normally respect directions given in the preparatory works regarding the interpretation of statutory provisions, especially when the legislation is new and there is a lack of case law.

[7] Jan Mayen is, except for a scientific base, uninhabited. Svalbard is sparsely inhabited (in 1999, 2 333 persons, most of whom were Norwegian or Russian citizens) and subject to a special treaty that limits the full exercise of Norwegian sovereignty (application of Norwegian laws). The business community in Svalbard is focused on activities for the local mining and tourism industries and not on international financial services. Bordering on Sweden, Finland and Russia, Norway forms the western part of the Scandinavian Peninsula in northwestern Europe.

6. All case documents of public administrations are public, unless an exception is made by or pursuant to statute. The Public Administration Act (PAA) (supplemented by unwritten principles) governs public access to information and how public administrative bodies handle their cases. The activities of public administrative bodies are controlled by the Parliament, the Parliamentary Ombudsman and the Auditor General. Access to courts is guaranteed.

1.2 General Situation of Money Laundering and Financing of Terrorism[8]

7. In general, serious crime in Norway has been characterised by the following general trends: better organisation and increased flexibility; increased specialisation and professionalism; increased co-operation between criminal networks; increased use of advanced technologies; more links between crime and legal business activities; and increased internationalisation.

8. Norwegian authorities state that money laundering (ML) continues to be primarily characterised by extensive use of cash. Money from the predicate offence is placed in the registered economy, where its origin is concealed or blurred. In many instances, cash-based activities such as dealings in second-hand cars, fruit and vegetable, kiosk, building and construction and restaurant activities are suspected of being used for this purpose. The National Authority for Investigation and Prosecution of Economic and Environmental Crime (ØKOKRIM) has observed an increasing trend in the use of cash proceeds of crime to purchase assets such as cars, houses/flats or in investments in shares/securities.

9. In the last 10 years, Norway has seen an increase in profit-motivated crime (especially drug-related and economic crime). Although reports on drug-related crimes (particularly cases relating to drug use) have decreased in number since 2001, the most serious cases of drug related crimes have increased every year from 39 cases (in 1999) to 136 cases (in 2003). Norway reports that this is due to a shift in the priorities within the police, from focusing on the users to concentrating on the organised groups smuggling and dealing in narcotics.

10. Economic crimes, including various types of fraud against the state or against public and private business entities, are generating large amounts of illegal proceeds which are subject to money laundering. The incidence of economic crime almost doubled to 14 880 in 2003—up from approximately 8 000 cases in each of previous four years. This extraordinary increase is due to one single complex catalogue fraud which alone generated 8 000 separate reports. In the last two years alone, several persons in Norway have been convicted for fraud amounting to more than 100 million Norwegian Kroner (NOK) (12 million Euros (EUR)/15.8 million United States dollars (USD)).[9] Some of these cases have had international links, particularly in relation to the laundering of the illegal gains. In tax evasion cases, there is a growing trend of transporting and depositing proceeds abroad, using fictitious invoicing by companies that are registered and operating abroad, but still controlled by those responsible for the predicate offence. Recent developments also show an increase in prostitution, with an ever-greater number of women from Eastern Europe, Asia and Africa participating, causing concern about the possibility of trafficking and illegal transporting of proceeds abroad. There is also reason to believe higher activity in the areas of international fraud, and tax and duty evasion.

11. Another trend in Norway appears to be towards an increasing number of serious and more brutal crimes for profit. Although Norway still has a low number of armed robberies (compared to other countries). Robberies against post offices doubled in 2003 from 2002 (5 cases in 2002 and 10 cases in 2003), but the number of bank robberies decreased from 16 cases to 10 during the same period. In 2002 and 2003, there were 10 robberies each year against the transport of money and other valuables. The number of aggravated robberies remained fairly stable in 2002 and 2003 (333 and 325 cases respectively). The number of severe thefts increased considerably from 2001 to 2002, but was much

[8] The information in this section was provided by Norway and was not evaluated by the assessors.

[9] The exchange rates quoted in the report are based on the rates that were effective on 29 January 2005: NOK 1 = EUR 0.12121 / USD 0.15812.

lower again in 2003 (especially in the case of theft from vehicles). The number of blackmail and robbery cases decreased by 13.5 % from 2002 to 2003 (1 864 reported cases to 1 612 reported cases), and is now on a low level compared with previous years. Recently, highly professional and violent groups have successfully attacked post offices, banks and premises for deposits, without being caught. In many of these cases, serious robberies that had the character of military commando raids were committed on banks and armoured cars. Traditionally, the perpetrators of such crimes in Norway have been Norwegian citizens. However, during the last few years, more foreign criminals are organising and participating in such crimes. Recruitment to these hard-core robbery environments appears to take place across national borders. Many serious armed robbery cases have involved participation by persons with military backgrounds from Eastern Europe. Norway suspects that much of the proceeds from these robberies are laundered through registered companies that are formally or informally controlled by the criminals.

12. No statistics are available concerning the extent of organised crime within Norway. However, recent threat assessments conclude that organised crime or criminal networks are gaining more of a foothold. The Police Directorate is currently carrying out a national survey regarding the extent of organised crime. Norway intends to use the results of this survey to form the basis of a more structured fight against organised crime. In most cases, these organisations are led by criminals who live and operate abroad, while co-operating with criminals or criminal groups in Norway. This is especially true for crimes related to trafficking in human beings, smuggling and dealing in drugs and legal commodities (including cigarettes and alcohol which are very expensive commodities in Norway—compared with the price levels in neighbouring countries—due to heavy taxation). These types of crime likely generate huge profits for the criminals. Organised multi-criminal groups from Central and Eastern European countries are likely to continue to set up their activities in Norway, with smuggling and drug trafficking as their main activities.

13. In 2003, the Oslo police district conducted an analysis of possible terrorist financing (FT) activities to determine whether there were connections between organised crime and terrorist financing in the Oslo area. The analysis indicates that persons from different environments and groups—Kurds, Iraqi, Islamic, Iranian, Somali, Ethnic Albanian and Hezbollah—are involved in hawala-banking, couriering, or using direct bank transactions and/or money or value transfer services (MVTS) (such as Western Union and/or Money Gram). The sources of their funds are mainly criminal activity, in particular, drugs, fraud, trafficking, legal/illegal business, forced taxes/fees and money collecting. However, this analysis does not provide a basis for conclusions about possible connections between organised crime and terrorist financing.

14. Criminal statistics show that ethnic minority groups within Norwegian society are neither under-represented nor over-represented in the criminal activities that take place in Norway. However, members of some ethnic groups do dominate in certain types of serious crime, such as smuggling of drugs and trafficking in human beings. Their ethnic background makes it highly probable that some of the illegal proceeds are being transferred out of Norway through a traditional remittance system or by cash couriers. Non-ethnic Norwegians (such as immigrants, asylum-seekers/refugees) are represented in about 70% of the suspicious transaction reports (STRs) received.

15. The globalisation of economies has made it is easier for international criminal organisations operating towards and inside Norway to channel their illegal financial gains out of reach of the national authorities in the country where the crimes have been committed towards safe havens abroad. Norway states that it has reason to believe that a larger proportion of the illicit gains is transferred to deposits that are located outside of Norway. This may occur through private cash intensive companies, and then onwards through other companies within Norway and abroad by means of fictitious invoicing, fictitious loan agreements, transfer pricing and other means.

1.3 Overview of the Financial Sector and DNFBP

a. Overview of the Financial Institutions sectors[10]

16. The following types of financial institutions are authorised to operate in Norway: savings banks[11], commercial banks, finance companies and mortgage companies; life and non-life insurance companies, e-money institutions, investment firms, security funds management companies and branches of foreign financial institutions. All are supervised by the Financial Supervisory Authority of Norway (*Kredittilsynet*) (the FSA). Twelve institutions are authorised to provide credit card services. Foreign exchange offices (i.e. bureaux de change) and money transfer companies are formally not permitted to operate in Norway. However, banks, finance companies licensed by the Ministry of Finance and EU/European Economic Area (EEA) branches of such undertakings are allowed to carry out foreign exchange activity or international money transfers (Financial Institutions Act (FIA) chapter 4a).

17. The number of Norwegian-owned savings banks, commercial banks, finance companies and mortgage companies has decreased over the past ten years, while the number of foreign-owned institutions and branches has risen. The foreign share of the banking market has risen to 27% (most of which are branches and subsidiaries of Swedish and Danish banks). By the end of 2003, the five largest financial groups controlled as much as 74% of the market. Still, there has been a steep fall in banks' interest spreads, suggesting that competition has been intense and that structural and technological changes have benefited the customers.

18. Most insurance services (both life and non-life) are offered in Norway. Norway also has several e-money issuers. E-money issuers provide the possibility to pay through a mobile phone for goods or services that are delivered to the mobile phone and with Internet merchants such as online stores, net auctions, services, etcetera. In the retail environment, account holders can make purchases in street shops, restaurants and service stations. E-money users can also send or receive money through their e-money account, or deposit and withdraw cash (as e-money can be redeemed for real money). Mobile e-cash is funded by the user from his/her bank account or by receiving a payment from another user, and is stored in an extra electronic account available for the customer at any time, anywhere. The mobile e-cash is linked to the user's mobile phone number, but the transactions are not charged to the person's mobile phone bill. Instead, it is deducted electronically from the separate account. After e-money has been purchased and stored in the user's e-money account, the user's mobile phone can serve the same function as traditional payment forms (payment cards or cash).

19. The following chart sets out the types of financial institutions that are authorised to carry out the financial activities that are listed in the Glossary of the FATF 40 Recommendations.

TYPES OF FINANCIAL INSTITUTIONS AUTHORISED TO CARRY OUT FINANCIAL ACTIVITIES LISTED IN THE GLOSSARY OF THE FATF 40 RECOMMENDATIONS	
Type of financial activity (See the Glossary of the 40 Recommendations)	Type of financial institution that is authorised to perform this activity in Norway[12]
Acceptance of deposits and other repayable funds from	Banks (Savings Banks Act (SBA) ss.1, 22 and 24; Commercial

[10] See Annex 5 for further details on financial institutions in Norway, including how many of each type of financial institution exists.

[11] Savings banks differ from commercial banks with regards to their ownership; however, there are no formal differences in relation to their obligations under AML/CFT legislation. Commercial banks are ordinary limited companies that are owned by their shareholders. Savings banks have no shareholders or other owners; however, they may issue negotiable primary capital certificates which confer rights of representation in the main body. The owners of these certificates may also (under certain conditions) receive an annual interest based on the previous year's profit.

[12] Including EU/EEA branches of such undertakings.

the public (including private banking)	Banks Act (CBA) ss.1, 19 and 20).
Lending (including consumer credit; mortgage credit; factoring, with or without recourse; and finance of commercial transactions (including forfaiting))	Banks, finance companies, insurance companies, investment firms (purchase of securities) (SBA s.24; CBA s.19; Financial Institutions Act (FIA) s.3-16; Securities Trading Act (STA) s.1-2).
Financial leasing (other than financial leasing arrangements in relation to consumer products)	Banks, finance companies (SBA s.24; CBA s.19; FIA s.3-16).
The transfer of money or value (including financial activity in both the formal or informal sector (e.g. alternative remittance activity), but not including any natural or legal person that provides financial institutions solely with message or other support systems for transmitting funds)	Domestic: Not regulated (The activities of financial institutions are regulated as indicated above). Cross-border: Banks, finance companies (FIA s.4a-1).
Issuing and managing means of payment (e.g. credit and debit cards, cheques, traveller's cheques, money orders and bankers' drafts, electronic money)	Banks, finance companies, e-money issuers (SBA s.24; CBA s.19; FIA s.3-16; E-money Institutions Act §1-1, 1-2 and 2-1).
Financial guarantees and commitments	Banks, finance companies (SBA s.24; CBA ss.19; FIA s.3-16).
Trading in: (a) money market instruments (cheques, bills, CDs, derivatives etc.); (b) foreign exchange; (c) exchange, interest rate and index instruments; (d) transferable securities; (e) commodity futures trading	(a) Banks and investment firms (intermediaries) (b) Banks and investment firms (intermediaries) (c) Banks and investment firms (intermediaries) (d) Investment firms (intermediaries) (e) Not regulated (The exchange Nord Pool and the authorised marketplace Imarex are licensed and regulated) (SBA s.24; CBA s.19; STA s.1-2).
Participation in securities issues and the provision of financial services related to such issues	Investment firms, banks with an authorisation to provide investment services (STA s.1-2).
Individual and collective portfolio management	Individual portfolio management: Investment firms and management companies for securities funds (STA s.1-2; Securities Funds Act (SFA) s.2-1). Collective portfolio management: Management companies for securities funds (SFA s.2-1).
Safekeeping and administration of cash or liquid securities on behalf of other persons	Banks and investment firms (SBA s.24; CBA s.19; STA s.1-2).
Otherwise investing, administering or managing funds or money on behalf of other persons	Not regulated. (Securities business regulated as described above).
Underwriting and placement of life insurance and other investment related insurance (including insurance undertakings and to insurance intermediaries (agents and brokers))	Life-insurance companies (Insurance Act (IA) s.7-1).
Money and currency changing	Banks and finance companies (SBA s.24; CBA s.19, FIA s. 4a-1).

b. Overview of the Non-financial Businesses and Professions sectors[13]

20. ***Casinos:*** Casinos (including Internet casinos) are not allowed to operate in Norway. However, it is not prohibited for Norwegian nationals to gamble on Internet casinos that are operated from a server located in another country, nor is it prohibited for Norwegians to offer such a service in Norway

[13] See Annex 6 for further details on designated non-financial businesses and professions in Norway, including how many of each type of business/profession exist.

from outside Norway. It is assumed that the number of Norwegians gambling in such casinos is increasing. Norway has no information about Norwegian ownership or control of such casinos.

21. Although casinos are prohibited in Norway, the following gambling activities are allowed:

(a) Ten different humanitarian organisations (such as the Norwegian Red Cross, Save the Children, etc.) hold a license for an internet lottery (tivoli.no). This lottery is operated by Norskespill.no AS, which is owned by the same organisations. Tivolo.no is subject to strict rules regarding registration, accounts, maximum bets and size of winnings.

(b) SMS Jackpot is a mobile phone lottery that is owned and operated by Sports and Environmental organisations (among others). It operates under requirements which are similar to tivoli.no.

(c) Norsk Tipping is Norway's leading betting company and is wholly owned by the Norwegian state. It operates betting relating to soccer games, etcetera. A number of their games are now accessible via the internet through a registration procedure, smart card and card reader.

(d) Norsk Rikstoto operates mainly games related to horse betting. It is owned by a foundation and is closely regulated.

22. ***Real estate agents:*** Real estate services are provided by licensed real estate agency firms, lawyers who have provided security for real estate agency and housing co-operatives which are in the business of brokering co-operative flats. Real estate agents (including lawyers who are acting as real estate agents) are licensed and supervised by the FSA.

23. ***Dealers in precious metals and dealers in precious stones:*** According to Statistics Norway (SSB) 673 businesses deal in precious metals and stones. All dealers in high value goods (including precious metals and stones) are subject to obligations under the Money Laundering Act (MLA) when performing transactions in cash exceeding a value of NOK 40 000 (EUR 5 800/USD 6 300). However, these businesses are not supervised by any agency for AML/CFT purposes.

24. ***Lawyers:*** Licensed lawyers may give legal assistance to others, and conduct cases in the lower court (*tingretten*), the appeal court (*lagmannsretten*) and the Supreme Court (after passing a required examination). Lawyers are licensed by the Supervisory Council for Legal Practice (Supervisory Council). All are supervised by the Supervisory Council for AML/CFT purposes. Additionally, the Norwegian Bar Association (NBA) supervises its members. There are approximately 4 900 lawyers operating in Norway. A significant number operate as personal undertakings (*enkeltpersonforetak)* and about 1 040 work as in-house lawyers.

25. ***Notaries:*** Notaries do not exist in Norway. Many of the services that would otherwise be provided by notaries (like legalising the title for transferring ownership of registered property or establishing a will) are part of normal civil contracts.

26. ***Other independent legal professionals:*** Approximately 1 662 Graduates in Law work as assistant advocates to licensed lawyers. Additionally, the Supervisory Council has issued 51 allowances authorising persons who have sufficient education within special fields of law to give legal assistance within such areas. Many work as tax advisors. The Supervisory Council has also granted eight permissions allowing persons to provide special forms of legal assistance under special circumstances. These permissions are granted to organisations that give free legal advice and obtain financial support from the authorities. These independent legal professionals are all authorised and supervised by the Supervisory Council. There is also a group of 48 persons with law degrees that have activated their right to exercise general legal assistance (cf.Courts of Law Act s.218).

27. ***Accountants:*** As of 31 December 2003, there were 9 164 natural persons and firms registered in the register of external accountants. The FSA is responsible for licensing, registering and supervising external accountants (both natural and legal persons).

28. ***Auditors:*** State authorised auditors and registered auditors may be authorised to provide statutory auditing services in Norway in accordance with the Eighth Council Directive of the European Communities 84/253/EEC of 10 April 1984 based on Article 54 (3)(g) of the Treaty on the approval of persons responsible for carrying out the statutory audits of accounting documents. Both are also entitled to provide audit services to any company (with the exception of listed companies, which are subject to auditing by state authorised auditors only). In 2003, there were 2 177 state authorised auditors, 2 977 registered auditors and 514 audit firms. Of these, approximately 1 800 auditors were qualified and authorised to audit a company's annual accounts (i.e. have furnished security and comply with the post-qualifying training requirements). The FSA is responsible for authorising, registering and supervising auditors (both natural and legal persons). Auditors are also supervised by the Norwegian Institute of Public Auditors (NIPA).

29. ***Trust and company service providers:*** In Norway, trust and company services providers are not recognised as separate businesses or professions. Lawyers and auditors normally provide trust and company services.

1.4 Overview of commercial laws and mechanisms governing legal persons and arrangements[14]

30. A wide variety of legal persons exist in Norway: (a) Companies – limited companies and public limited companies (shareholders have limited liability); (b) Partnerships - general partnerships and general partnerships with shared liability (partners have unlimited liability), and limited partnerships (some partners have unlimited liability, others have limited liability); (c) Societies - house building co-operatives, housing co-operatives and co-operative societies; and (d) Organisations – Foundations, savings banks and associations. All have legal persona and can hold a bank account or own property in their name.

31. Limited companies and public limited companies must have memorandum and articles of association that identify (among other things) the name, address and type of business of the company and the board members. For a limited company, the minimum start up capital is NOK 100 000 (EUR 12 000/USD 15 800). The managing director and at least 50% of the board must be either residents of Norway or citizens of an EEA state. All directors must be natural persons. There must be at least one shareholder, and both natural and legal persons can own shares. An auditor must be retained. It is common practice in Norway for lawyers or accountants to incorporate "shelf companies" for sale. Where required, the lawyers/accountants could remain as directors of these companies, if requested by the shareholders.

32. All forms of partnership must have a partnership agreement that, inter alia, identifies the name and address of the partners (the partners are the owners of the assets of the partnership), the municipality where the company has its main office and the purpose of the partnership. There are no residency/nationality requirements concerning the partners, and partners can be either natural or legal persons. For a limited partnership, if the general partner is a legal person, an auditor must be appointed. All types of partnership (general partnerships, general partnerships with shared liability and limited partnerships) have their own legal personality, both with respect to procedural law and substantive law.

[14] See Annex 7 for more information concerning the characteristics of the legal persons and arrangements that exist in Norway, including the requirements for establishing them. "Legal arrangements" as defined in the FATF Recommendations do not exist under Norwegian law.

33. Societies are required to have a board of directors and to appoint an auditor. The members of the society are generally the persons that have an ownership interest in the assets of the society. Organisations are required to have a board of directors, and foundations and savings banks must also appoint an auditor. Foundations are private entities that hold the assets donated to them for the purposes set out in the documents establishing the foundation (commercial and non-commercial purposes). Associations are bodies formed by several natural or legal persons for a common non-profit purpose.

34. Norwegian law does not clearly prohibit foreign legal entities from having their main seat in Norway or from conducting business in Norway. Concerning legal persons from the EEA area, Norwegian law is interpreted in accordance with EU case law regarding cross-border transfers of a registered office (free movement of legal entities cf. C 212/97 Centros Ltd., amongst others).

35. Norway has not signed the Convention on the Law Applicable to Trusts and on their Recognition (1 July 1985, The Hague).

1.5 Overview of strategy to prevent money laundering and terrorist financing

a. AML/CFT Strategies and Priorities

36. Norway's key anti-money laundering (AML) / counter-terrorist financing (CFT) strategies and policies for the coming three years are set out in the Norwegian Government's Action Plan for Combating Economic Crime (the Action Plan 2004). The Action Plan 2004 comprehensively reviews the state of economic and profit motivated crime in Norway, and sets out proposed measures for addressing these issues.

37. Norway bases its AML control policies and objectives primarily on international initiatives such as the FATF 40 Recommendations, the EU Money Laundering Directives, the United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances 1988 (the Vienna Convention) and the Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime 1990 (the Strasbourg Convention). Additionally, the Norwegian Minister of Justice formally expressed Norway's support for the revised FATF Forty Recommendations in a letter to the Financial Action Task Force (FATF) President dated 18 September 2003. Norway's ratification of international conventions—such as the OECD Bribery Convention, the COE Corruption Convention and the United Nations Convention against Transnational Organised Crime (2000) (the Palermo Convention)—has also impacted on its AML regime.

38. Norway's CFT control policies and objectives policy are based primarily on the United Nations Security Council Resolutions, the United Nations Convention for the Suppression of the Financing of Terrorism (1999) (the Terrorist Financing Convention) and, to a certain extent, the FATF 8 Special Recommendations (SRs).

39. In particular, Norway has prioritised AML measures relating to (a) increasing the risk of detection and prosecution for everyone involved with the proceeds of crime; (b) improving the process of tracing and confiscating illegal proceeds; and (c) facilitating international co-operation. The proposed measures set out in the Action Plan 2004 include creating multi disciplinary teams to combat economic crime in all police districts (scheduled for completion by the 1 July 2005) and teaching financial investigation as a separate subject at the National Police College (Police College) (scheduled to begin in the 2005/2006 session). Additionally, the Action Plan 2004 states that it will be necessary to review relevant Norwegian legislation in order to ensure that Norway complies with the revised FATF Recommendations (including the 8 SRs) and the third EU Money Laundering Directive (Action Plan 2004 p.38). The third EU Money Laundering Directive is near adoption. Norway plans to start preparing its implementation as soon as the Directive is finalised; however, some new initiatives have already been taken. For example, a proposal is currently pending before Parliament to amend section 37(d) of the Penal Code (PC) to allow for the sharing of confiscated assets with other countries. Issues

relating to the enhanced confiscation of proceeds from crime are another subject which has been a priority of the Norwegian government for many years. The implementation period for the measures set out in the Action Plan 2004 is three years—although implementation of some measures is already underway.

40. Representatives from the Anti-Corruption/Anti-Money Laundering Project (AC/AML Project) (which developed the Action Plan 2004) cite the most important priorities in the Action Plan 2004 as being: (i) competence building (i.e. learning how to implement the new legislation); (ii) amending the new legislation to comply with the 3rd EU Money Laundering Directive (when that directive is adopted); (iii) making vulnerable sectors, such as the oil industry, more transparent; (iv) creating a new team at ØKOKRIM to work on state support schemes;[15] and (v) training each of the specialized economic crime units in the 27 police districts in Norway on confiscation issues.

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

(i) Ministries

41. Three ministries have responsibilities that are related to AML/CFT: the Ministry of Finance, the Ministry of Justice & Police, and the Ministry of Foreign Affairs.

Ministry of Finance[16]

42. The Ministry of Finance is responsible for planning and implementing economic policy; co-ordinating the preparation of the budget; ensuring government revenues by maintaining and developing the system of taxes and duties and monitoring financial markets; and drawing up regulations. It is organised into six departments, of which the Financial Markets Department and the Tax Law Department have responsibilities that are specifically relevant to AML/CFT issues. The Money Laundering Act is the responsibility of the Ministry of Finance.

43. *Control Committee for Measures to Combat Money Laundering (Control Committee):* The Control Committee is an independent body that was established in 1995 under section 14 of the Money Laundering Act and which reports to the Ministry of Finance. It is headed by a High Court Judge and supervises parts of the activities of Norway's financial intelligence unit, the Money Laundering Unit (MLU). The Ministry of Finance provides the secretary of the Control Committee.

44. *Directorate of Customs and Excise (Customs Directorate)[17]:* The Customs Directorate is an operational agency that is subordinated to the Ministry of Finance. It is the administrative authority for the Customs administration. It does not have investigative powers. The Customs Directorate is responsible for the Currency Transaction Register established under the Currency Register Act (CRA) which entered into force on 1 January 2005.

45. *Directorate of Taxes (Tax Directorate):* The Tax Directorate is an operational agency that is subordinated to the Ministry of Finance. Its responsibilities include conducting tax audits. It does not have investigative powers. An internal instruction issued in 2003, gave the tax authorities' the possibility to report to the police and Prosecution Authority about serious crime outside of the tax area, including money laundering (for a full explanation, see paragraphs 437 to 439 of this report).

---

[15] Abuse of state support schemes (such as government subsidy arrangements and social services) is increasing. For instance, Norway recently had cases where doctors were helping patients to defraud the social services network by systematically reporting that patients were medically unable to work. Norway recognizes that its current control systems are trust-based and designed for a small community where everyone knows each other. Such controls are no longer working as Norway grows.

[16] See Annex 8 for additional details concerning the organisation and AML/CFT responsibilities of the Ministry of Finance.

[17] See Annex 13 for additional details concerning the organisation of the Customs Directorate.

The Directorate of Taxes is now building its institutional capacity to cope with this change. The Directorate of Taxes is divided into regional teams. Three of these County revenue offices (Oslo City, Oslo County and, Akershus County) have established a Tax Crime Unit (*Skattekrimenheten for Oslo og Akershus*). The main duty of this body is to detect and make inquiries on serious tax crime in the Oslo area, and to co-operate with the police and Prosecution Authority (including ØKOKRIM) with a view to maximising the effect of their combined powers.[18]

Ministry of Justice & Police[19]

46. Law enforcement and prosecution are very heavily interconnected in Norway. The Ministry of Justice and Police is responsible for the recourses of the National Police Directorate (Police Directorate), the Director General of the Public Prosecution and the Police Security Service (PST). The Police Directorate is responsible for the resources and the non-prosecution tasks of the police and bodies like ØKOKRIM. The Director General of the Public Prosecution is responsible for the Prosecution Authority and the prosecution tasks of the police, the PST and bodies like ØKOKRIM. This means that both have shared responsibilities for many bodies. The resources made available by the Ministry have to be used in accordance with the principal priorities and guidelines given in budgetary documents issued by the Government and the Parliament. A more detailed description of the priorities and the most important steps to be taken is found in the annual letter of assignment from the Ministry of Justice to the respective services when the resources are handed out.

47. *Anti-Corruption and Money Laundering Project (the AC/AML Project):* The AC/AML Project was established in May 2002 within the Ministry of Justice & Police and will conclude in 2005. The AC/AML Project has five members, including the head. The AC/AML Project was responsible for preparing the Action Plan 2004. Its members lecture at the Police College and offer courses and seminars on money laundering issues. The AC/AML Project has also developed a textbook concerning how to work with confiscation cases[20] and worked on issues relating to the enhanced confiscation of proceeds from crime.

48. *EMØK:* EMØK is an intergovernmental committee on economic crime which consists of senior government officials and is contained within the Ministry of Justice & Police. The EMØK consists of representatives from the Ministry of Justice & Police (leadership), Ministry of Finance, Ministry of Trade & Industry, Ministry of Labour & Social Affairs, Ministry of Modernisation, and ØKOKRIM. EMØK was established in 1999 and was responsible for preparing the Governmental Action Plan against Economic Crime (2000) (Action Plan 2000). Some of its members also assisted the AC/AML Project in preparing the Action Plan 2004 and EMØK will systematically follow-up on its implementation.

49. *National Police Directorate (Police Directorate):* The Police Directorate was established in 2001 as part of a comprehensive reform of the entire Norwegian police force. It is organised under the Ministry of Justice & Police and acts under the Minister of Justice's constitutional responsibility. The Police Directorate plays a key role in the co-ordination of efforts to combat international and organised crime. In particular, it co-ordinates international police co-operation, administratively manages those Norwegian liaison officers serving with Interpol and Europol (the liaison officers serving with Norwegian embassies are, as of 1 January 2005, administratively managed by the Ministry of Foreign Affairs) and provides Norway's operative police services with accurate analysis and threat assessments ("intelligence-led policing"). It also manages and co-ordinates the Norwegian police, including three central police institutions which have AML/CFT responsibilities: ØKOKRIM,

[18] Four new similar units will be established in other parts of Norway by 1 July 2005.

[19] See Annex 9 for additional details concerning the organisation and AML/CFT responsibilities of the Ministry of Justice and Police.

[20] This book, entitled *Confiscation – what must be done?,* was authored by Anne-Mette Dyrnes and is available in Norwegian.

KRIPOS, and the Police College. ØKOKRIM, KRIPOS and the Police College report directly to the Police Directorate. The PST reports directly to the Ministry of Justice & Police.

50. *The National Council for Co-ordinated Combating of Organised Crime (ROK):* ROK is a council that was established by the Ministry of Justice & Police in November 2000 for the purpose of improving co-ordination in the fight against organised crime that is committed across the borders of several police districts.

51. *CATCH*: CATCH is the name of a special project that was established by the Ministry of Justice & Police in 2001 and administered by the Police Directorate. The project was an operational unit with a total of 36 employees. Its objective was to investigate serious organised crime by focusing on the principals of that crime. Its mandate was from the ROK.[21]

52. *National Authority for Investigation and Prosecution of Economic and Environmental Crime (ØKOKRIM):* ØKOKRIM is both a special police institution and prosecution authority that is organised (for administrative and budgetary purposes) under the Police Directorate. In respect of its handling of criminal cases, ØKOKRIM reports to the Director General of Public Prosecutions. ØKOKRIM is responsible for investigating and prosecuting serious and complicated economic and environmental crime. Several multidisciplinary specialised investigation teams (most headed by a chief state prosecutor) are located there, including the Assets Confiscation team. The MLU is also located at ØKOKRIM.

53. *Money Laundering Unit (MLU):* The MLU is the Norwegian financial intelligence unit (FIU). It is part of the ØKOKRIM and is headed by a police prosecutor. The MLU receives, records, analyses, disseminates and deletes (as required by law) suspicious transaction reports received from financial institutions and non-financial businesses and professionals that have reporting obligations under Norway's AML/CFT legislation. The MLU also receives and analyses other information, such as information from the customs authorities and other intelligence. It also conducts training courses and seminars.

54. *National Criminal Investigation Service (New KRIPOS):* KRIPOS was a central agency that rendered expert assistance to the Norwegian police districts relating to technical and tactical investigation services, and international police co-operation. In 2004, the Ministry of Justice & Police decided to establish a new police institution based upon KRIPOS effective from 1 January 2005—the National Authority for Investigation and Combating Organised and other Serious Crime (New Kripos). This new agency will be responsible for combating serious organised crime, providing assistance to the police districts and investigating its own cases related to organised crime. Both the CATCH project and the Police Computer Crime Centre (PCCC) (formerly part of ØKOKRIM) is part of the new agency. The Interpol and Sirene offices are located at New Kripos.

55. *National Police College (Police College):* The Police College offers a basic three-year training programme in police subjects. The basic course is a bachelor program, mandatory for all police officers. The Police College also gives some post-graduate courses focused on organised and financial crime. The Police College is responsible to the Police Directorate.

56. *Director General of Public Prosecutions (Prosecution Authority):* The Director General of Public Prosecutions is head of the Prosecution Authority and is responsible for handling criminal investigations and prosecutions, including money laundering and terrorist financing investigations and prosecutions.

[21] As of 1 April 2005, the functions of CATCH are implemented in the regular structure of the National Criminal Investigation Service (New KRIPOS).

57. *Police Security Service (PST):* The PST is the Norwegian security service responsible for preventing and investigating crimes related to terrorism, including terrorist financing, espionage and the spread of weapons of mass destruction. It is also responsible for preventing the spread of violent extremism and fulfils an advisory function for the Norwegian authorities.

Ministry of Foreign Affairs[22]

58. The Ministry of Foreign Affairs plays a legislative and informative role in relation to domestic efforts to combat terrorist financing. In particular, the Ministry of Foreign Affairs is responsible for implementing the United Nations Security Council Resolutions related to terrorist financing. The Ministry of Foreign Affairs is also the focal point for the relations with the United Nations Counter Terrorism Committee (UNCTC). Furthermore, the Ministry of Foreign Affairs is negotiating new binding instruments relating to the fight against terrorism both within the United Nations and the Council of Europe.

(ii) Financial sector bodies

59. *Association of Norwegian Stockbrokers Companies (ANSC):* ANSC is a national trade organisation for investment services companies operating in Norway. The ANSC sets standards in the investment services industry and sanctions members that violate those standards or other applicable laws and regulations, including those related to money laundering.

60. *Federation of Norwegian Commercial and Service Enterprises (HSH):* HSH is Norway's leading organisation for employers who work in the trade and services sector. It has approximately 9 300 member companies, among them dealers in precious stones and metals. Membership is voluntary and the HSH has no monitoring or supervisory role concerning the AML/CFT obligations of dealers in high-value goods.

61. *Financial Supervisory Authority of Norway* (*Kredittilsynet) (FSA):*[23] The FSA is an administrative agency which acts under the general responsibilities of the Ministry of Finance. The FSA is responsible for licensing finance companies, investment firms, management companies for securities funds, insurance brokers, debt collecting agencies, state authorised and registered public accountants, authorised external accountants and real estate agencies. The FSA is also responsible for supervising banks (including money exchange and MVTS), finance companies, mortgage companies, insurance companies and brokers, pension funds, investment firms, securities fund management and market conduct in the securities market, stock exchanges and authorised market places, settlement centres and securities registers, real estate agents, debt collection agencies, external accountants and auditors. The responsibility for following-up on relevant legislation, including AML/CFT legislation lies with the FSA. In short, the FSA is the supervisor for all industries under AML/CFT obligations, except for dealers in high value goods and lawyers.

62. *Norges Bank:* Norges Bank is the Central Bank in Norway. It is a separate legal entity owned by the state and is obligated to comply with Norway's AML/CFT legislation. The Bank's activities are regulated by Act no.28 of 24 May 1985 relating to Norges Bank and the Monetary System.

63. *Norwegian Financial Services Association (FNH):* FNH is the Norwegian banking and insurance association. It represents about 45 commercial banks, financial services institutions and insurance companies (but not savings banks). It is responsible for safeguarding the interests of its members towards the government, other organisations and the mass media. The FNH was formed in 2000 as a result of the merger between the Norwegian Bankers' Association and the Norwegian

[22] See Annex 10 for additional details concerning the organisation and AML/CFT responsibilities of the Ministry of Foreign Affairs.

[23] See Annex 14 for additional details concerning the organisation of the FSA, including its key relations and stakeholders.

Insurance Association. The main reasons behind this merger were the structural trends in the financial services industry, greater international competition, and the emergence of common international regulations governing competition.

64. *Norwegian Mutual Fund Association (NMFA):* The NMFA is an industry organisation for mutual fund investment companies and mutual distributors in Norway. NMFA establishes standards in the mutual fund industry. It also sanctions members who fail to comply with those standards or other applicable laws and regulations (including those related to money laundering).

65. *Oslo Børs:* Oslo Børs is a Norwegian Stock Exchange. It provides a regulated market for securities trading and is supervised by the FSA.

(iii) DNFBPs

66. *Confederation of Norwegian Business and Industry (NHO):* The NHO is the main organisation for Norwegian employers. It promotes business-friendly legislation and policy, represents employers in collective bargaining, and gives advice to the members on a wide range of issues. The NHO has more than 16 000 members, ranging from small family-owned businesses to large industrial enterprises. All belong to one of 22 nation-wide sectored federations and one of 15 regional associations. The sectored federations handle branch-related interests, while the regional associations offer a local point of contact between companies and authorities.

67. *Norges Autoriserte Regnskapsføreres Forening (NARF):* The NARF is the major professional body for authorised external accountants. There are 6 598 authorised external accountants in Norway (as of the end of 2003). Of these, 2 856 are members of NARF.

68. *Norwegian Bar Association (NBA)*: About 90 percent of Norwegian lawyers (over 6 000 persons) are members of the NBA. The NBA handles cases concerning possible contraventions of the professional duties and ethical guidelines applicable to lawyers, including cases that may lead to the loss or suspension of a lawyer's license. Cases are handles through local disciplinary committees, an appointed Disciplinary Committee (to handle appeals) and an Advocate License Committee.

69. *Norwegian Institute of Public Accountants (DnR):* The DnR is the professional body for registered auditors and state authorised auditors in Norway. There are 2 980 registered and 2 180 state authorised auditors in Norway. Of these, 1 560 registered and 1 910 state authorised auditors are members of the DnR.

70. *Supervisory Council for Legal Practice (Supervisory Council):* The Supervisory Council is the supervisory body for lawyers and other independent legal professionals.

(iv) Other matters

71. Norway has a comprehensive registry system for natural persons. At birth, each Norwegian citizen is registered and assigned a unique 11-digit identification number. Norwegian residents are also assigned a unique 11-digit identification number. Non-residents who are liable to pay tax in Norway are assigned a unique D-number. These identification numbers are recorded in the Norwegian Population and Employer Register (Population Register) which also contains information concerning the person's name, address, spouse, siblings, children, parents and past/present employers. These numbers are commonly requested for the purpose of identifying natural persons. Consequently, when opening a bank account or applying for a bank card, the customer (if a natural person) must provide his/her identification or D-number.

72. Norway also has a comprehensive registry system for legal persons. There are various registers for legal persons, depending on their characteristics and types of activity. Norwegian legal persons or foreign legal persons doing business in Norway are required to register and will be assigned a unique identification number which is then used for all subsequent registrations in any applicable government registry. When

opening a bank account or establishing a business relationship, the customer (if a legal person) must provide their identification number. (Additional details concerning identification numbers for both natural and legal persons, and the registry system in general, are set out in paragraphs 206, 208 and 375 to 382 below.)

c. Approach concerning risk

73. Norwegian anti-money laundering legislation and measures were adopted before the 2003 revision of the FATF 40 Recommendations. Consequently, Norwegian legislation is not based on risk-assessments conducted in the manner or to the extent provided for in the revised FATF Recommendations. However, the overall philosophy of the Norwegian government is that laws and regulations that create new burdens on citizens and businesses and also limit the right to privacy should only be adopted if a serious need is observed. If such a need is observed, then it must be compared to the economic and other costs of implementing the proposed measures.

d. Progress since the last mutual evaluation

74. The main deficiencies identified in the second FATF Mutual Evaluation Report of Norway dated 6 August 1998 were: insufficient resources in the FIU; weaknesses in the confiscation regime; lack of statistics; problems with insured letters (*verdibrev*) that could be a loophole in the AML regime; problems with international co-operation with other FIUs; and the lack of sufficient measures to address organised crime. Since then, the following measures that partially address the identified deficiencies have been taken:

(a) The FIU's number of staff has been increased from 4 staff in 1998 to 11½ staff in January 2005.

(b) The legislation was amended to make confiscation of the proceeds from crime mandatory. A new provision on extended confiscation with a reversed burden of proof was also adopted. The number of confiscation orders and the total amount of the confiscated assets has increased: NOK 430.2 million (EUR 52.1 million/USD 68 million) in the seven-year period from 1997 to 2003, as compared with NOK 153 million (EUR 18.5 million/USD 24.1 million) in the five-year period from 1990 to 1995.

(c) Statistics collection has improved. Distinction is now made between the different kinds of money laundering in section 317 of the Penal Code, and between extended and normal confiscation.

(d) A provision was introduced to apply Norway's AML/CFT legislation to insured letters (*verdibrev*); however, it is not yet in force.

(e) The FIU's ability to co-operate domestically and internationally has been improved by repealing the strict confidentiality provision that existed in the previous legislation. Information can be exchanged with foreign FIUs, both spontaneously and upon request, regardless of whether the FIU is organised within the police or prosecution authority or within the administration.

(f) The following special departments and units were established to fight organised crime: The CATCH project (which focuses on the principals); a new police institution (New Kripos) to replace the National Criminal Investigation Service (NCIS) (which was established on 1 January 2004 to investigate serious organised crime cases and which incorporates the CATCH project and the PCCC); the Organised Crime Department of the Oslo Police District (established in 2004); the Police Directorate (which co-ordinates operative police efforts to combat international and organised crime); and the ROK (which co-ordinates the fight against organised crime which is committed across the borders of several police districts).

(g) In 2003, the government adopted the Plan of Action for Combating Trafficking in Women and Children for the years 2003–2005. This plan launched measures to protect and assist victims, prevent human trafficking and prosecute those who organise human trafficking.

(h) It is now prohibited to enter into an agreement to commit serious crime as part of the activity of an organised group or network, and the penalty for doing so has been raised.

(i) The Criminal Procedure Act (CPA) was amended to allow the following coercive measures to be used: secret search; video surveillance and technological tracking; concealed video surveillance of a public place; technological tracking when a person with just cause suspected of an act or attempt of an act punishable by imprisonment for five years or more; break-in in order to place a technical direction finder, or place such finders in clothes or bags that the suspect wears or carries, when a person with just cause is suspected of an act or attempt at an act punishable for 10 years or more. The government is also considering a proposal to statutorily regulate other coercive measures, such as infiltration (undercover) operations and provocation.

(j) A witness protection program was adopted and legislative amendments were made, making it possible to give a person a totally new identity. Additional measures to protect witnesses were also adopted, including procedures: (i) to allow the use of anonymous witness statements as evidence in court in certain cases of serious crime; (ii) to allow witnesses to remain anonymous during an investigation; and (iii) to interrogate witnesses by use of telecommunication.

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

75. ***Recommendation 1:*** Overall, Norway has implemented a very broad money laundering offence that is being actively and successfully used. Norway first criminalised money laundering in 1989 and broadened the scope of the offence in 1993.[24] Norway's money laundering offence meets almost all of the requirements of the Vienna Convention and Palermo Convention which obligate countries to make it a criminal offence to intentionally conceal or disguise, or convert or transfer property knowing that it is derived from a list of enumerated drug offences (in the Vienna Convention) or serious crime (in the Palermo Convention). Section 317 of the Penal Code makes it an offence to receive or obtain or assist in the securing, for oneself or another person, "any part of the proceeds of a criminal act". The term *proceeds* has been interpreted very broadly and thoroughly covers any type of property (including services) that directly or indirectly represents the proceeds of crime, regardless of its value. Although the law itself does not define the term *proceeds,* the preparatory works define *proceeds* as something that has been obtained by a criminal offence or is otherwise closely connected with a criminal offence.

76. For prosecutors, the money laundering offence is easy to use. The Prosecution Authority must prove that the proceeds stem from a criminal offence(s); however, it is not necessary that a person be convicted of a predicate offence. Moreover, Norway's implementation of the money laundering offence goes further in that the prosecutor does not have to prove: (i) who committed the predicate offence; (ii) that the proceeds stem from a specific criminal offence or a specific type of crime; or (iii) that the perpetrator of the money laundering offence knew or should have known who committed the

[24] In 1989, Norway enacted section 162(a) of the Penal Code which made it a criminal offence to receive or obtain any part of the proceeds from a drug crime. On 11 June 1993, section 162(a) was repealed and section 317 was amended to broaden the scope of the offence. Previously, section 317 of the Penal Code made it an offence to receive or obtain any part of the proceeds derived from other persons by criminal acts such as theft, embezzlement, fraud, etcetera. This amendment broadens the scope of section 317 to cover all kinds of criminal offences, including tax offences.

predicate offence. Moreover, a conviction for money laundering may be obtained even before the predicate offence has taken place.[25] This does not mean that the burden of proof is reversed; the prosecution still bears the burden of proving to the criminal standard of proof that the proceeds have no legal origin. In practice, the evidence must show that the money does not stem from legal income, an inheritance, a loan, a gift, etc.

77. Norway has adopted an all-crimes approach to the criminalisation of money laundering. It is an offence to receive or obtain or to assist in securing "any part of the proceeds of a *criminal act"*. Acts of assisting in securing the proceeds of crime includes (but are not limited to) collecting, storing, concealing, transporting, sending, transferring, converting, disposing of, pledging or mortgaging, or investing the proceeds. There is no requirement that the act of securing the proceeds be successful. For example, if a perpetrator invests proceeds in shares which ultimately drop in value, this is still money laundering even though additional proceeds were not generated. No limitations or thresholds have been placed on the term *criminal act* and, in practice, the term is applied very broadly to include the proceeds of misdemeanours and tax offences, as well as serious crimes. Consequently, any criminal act mentioned in the Penal Code (including terrorist financing which is a criminal offence pursuant to section 147(b) of the Penal Code) could constitute a predicate offence, as could any criminal act mentioned in other legislation (i.e. tax offences, serious offences and misdemeanours). The money laundering offence is considered to be a felony (i.e. a serious crime). All of the offences set out in the *designated categories of offences* (as defined in the Glossary of the FATF 40 Recommendations) are *criminal acts* and are, therefore, predicate offences for money laundering. For most of the designated categories there is a range of such offences.

78. Norway has successfully used its money laundering offence to prosecute the laundering of proceeds that were generated from a predicate offence which occurred in another country.[26] Although section 317 itself is silent in this regard, the preparatory works expressly provide that if the predicate offence is committed abroad, laundering the proceeds in Norway is a criminal offence provided that the predicate offence would have been a criminal offence if committed in Norway.

79. In addition, Norwegian law confers criminal law jurisdiction over a wide range of offences committed abroad by (i) a Norwegian national and (ii) any person domiciled in Norway (PC s.12.3). Norwegian criminal law also gives criminal law jurisdiction over to a less extensive range of offences committed abroad by a foreigner (PC s.12.4). The Preparatory Works expressly state that laundering the proceeds of a foreign predicate offence can be prosecuted in Norway.

80. Overall, Norway's money laundering offence is very comprehensive; however, it does not apply to persons who commit the predicate offence (i.e. self-laundering is not a criminal offence). The proceeds must stem from crime committed by a person(s) other than the money launderer. However, self-laundering is often characterised as being "harmful to society" and is considered to be an aggravating circumstance at sentencing. For instance, if the predicate offence is theft (PC s.258 para.2), an element of self-laundering could be considered an aggravating circumstance at sentencing, resulting in the maximum penalty being raised from three to six years. Nevertheless, there is no fundamental principle of Norwegian law that would preclude self-laundering from being an offence. A Ministry of Justice & Police committee constituted in 1994 conducted an assessment of whether the money laundering offence should extend to self-laundering. A minority of the committee proposed to

[25] This was the result in two Supreme Court cases (Case citations Rt. 1991/1018 and Rt. 1997/1637). In the first of these cases, a third party kept money that was intended to be used to buy drugs (heroin) that had not yet been smuggled into the country. Although the predicate offence (purchasing the drugs) had not yet taken place, the third party was convicted of money laundering.

[26] This was the result in a 1997 Supreme Court ruling (Case citation: Rt. 1997/1637). This case involved Russian nationals who committed tax evasion in Russia. The proceeds from the tax evasion were hidden in the bank account of a Norwegian national and a false rental contract for an apartment was produced. The Norwegian national was convicted of money laundering.

extend the offence to self-laundering. The committee's discussion did not raise any constitutional or other fundamental principle of Norwegian law that would bar the offence from being extended in this manner. The discussion was focused on traditional legal policy concerns, suggesting that the non-criminalisation of self-laundering is not based on a fundamental principle of Norwegian law. This view was confirmed by the Norwegian authorities during the on-site visit. The committee's report had a general hearing, and the Ministry of Justice & Police is still assessing whether a new provision on money laundering will include self-laundering.[27]

81. Norway's money laundering regime is also enhanced by the implementation of a number of ancillary offences to the offence of money laundering:

(a) Attempt: Attempted money laundering is a criminal offence (PC s.49). An attempt is defined as circumstances in which "the felony is not completed, but an act has been done whereby the commission of the felony is intended to begin". The offence of attempted money laundering even extends to circumstances in which the attempt itself was useless.[28]

(b) Aiding and abetting: Section 317 of the Penal Code expressly makes it an offence to aid and abet the securing of proceeds for another person (third party money laundering). Aiding and abetting means to carry out acts that may help to secure the proceeds of crime.

(c) Facilitation and counselling: Norway interprets acts of assisting in securing the proceeds to include facilitation and counselling. The MLA Prep. Works specifically mention that setting up a mailbox company that will be used to receive proceeds of crime could be an act of money laundering (facilitating). As well, a lawyer who advises the client on ways to launder the proceeds of crime may be punished for money laundering (counselling).

82. Conspiracy to commit money laundering is also an offence if the conspiracy is entered into as part of the activity of an organised criminal group (PC s.162c). An "organised criminal group" refers to "an organised group of three or more persons whose main purpose is to commit an act that is punishable by imprisonment for a term of not less than three years, or whose activity largely consists of committing such acts". However, the scope of the conspiracy offence does not extend quite far enough in that a conspiracy involving only two people is not covered. However, there is no clear fundamental principle of domestic law that would preclude such conduct being criminalised. To the contrary, section 147a of the Penal Code (for instance) expressly criminalises a conspiracy involving two people conspiring to commit a terrorist act.

83. Section 317 contains two exceptions whereby a person receiving proceeds of crime is not subject to punishment. First, a person who receives proceeds for his/her ordinary maintenance (or the maintenance of another person) from someone who is obliged to provide such maintenance is not subject to penalties for money laundering. The basis for the obligation to provide maintenance may be legal (i.e. a marriage or child-parent relationship) or contractual (i.e. the receiver of the proceeds is the common law wife of the criminal). In this context *maintenance* only includes things that are required for support (i.e. food, clothes, shelter, etcetera). *Ordinary maintenance* means that luxurious goods are not included. Second, a person who receives proceeds as normal payment for ordinary (not luxury) consumer goods, articles for everyday use or services is not subject to penalties for money laundering. This exemption is intended to limit the scope of the money laundering offence so as not to require a supplier of ordinary consumer goods to ask about the origin of the money used to buy the goods in question.

[27] The Ministry of Justice & Police intends to propose a new Penal Code in a couple of years.

[28] This was the result of a recent Supreme Court case (Case citation Rt. 2004/598). In that case, it turned out that the money to be laundered (NOK 17 million / EUR 2.1 million / USD 2.7 million) that Nigerian nationals had obtained assistance from Norwegian nationals to secure) did not exist.

84. Norway has been very active and successful in pursuing cases of money laundering. The Prosecution Authority may proceed with a case in one of two ways. First, in minor cases, the Prosecution Authority may offer the accused person the option of "accepting a writ". Accepting a writ means that a criminal conviction is registered and a fine is paid, but no term of imprisonment is imposed. Alternatively, the Prosecution Authority may proceed by way of issuing an indictment. Between 2000 and the end of June 2004, the prosecuting authorities decided to proceed with 1 693 cases in the following four categories of money laundering offence (all of which involve assisting in securing the proceeds of crime for another person): ordinary money laundering, aggravated money laundering, drug-related money laundering and negligent money laundering. The ordinary money laundering offence applies if the defendant knowingly laundered less than NOK 75 000 (EUR 9 100 / USD 11 900). The aggravated money laundering offence applies if the defendant knowingly laundered NOK 75 000 (EUR 9 100 / USD 11 900) or more—a notably low threshold for the application of an aggravated offence. The drug-related money laundering offence applies when the proceeds being laundered were the proceeds of a drug offence. The negligent money laundering offence applies when the defendant negligently laundered the proceeds. The following chart sets out how many cases were proceeded with (either through writ or indictment) in each of those four categories. (It should be noted that not all of these cases originated from STRs.)

NUMBER OF MONEY LAUNDERING CASES PROCEEDED WITH BY THE PROSECUTION AUTHORITY					
TYPE OF OFFENCE *(Statistics provided by STRASAK)*	2000	2001	2002	2003	2004
Ordinary money laundering: Assisting in securing proceeds of crime less than NOK 75 000 (EUR 9 100 / USD 11 900) for another person	51	48	32	98	236
Aggravated money laundering: Assisting in securing proceeds of crime greater than NOK 75 000 (EUR 9 100 / USD 11 900) for another person	24	35	19	15	32
Drug-related money laundering: Assisting in securing the proceeds of drug trafficking for another person	-	1	1	3	1
Negligent money laundering: Negligently assisting in securing the proceeds of crime for another person	105	302	310	404	284
TOTAL NUMBER OF MONEY LAUNDERING CASES	180	386	362	520	553

85. Overall, there is a strong upward trend in the number of money laundering prosecutions being pursued. In fact, the number of money laundering prosecutions has increased by almost 300% in the four-year period from 2000 to 2004—mostly in the area of negligent money laundering.

86. A very positive indicator of the success of the Norwegian system is the particularly high conviction rate for those money laundering cases that are proceeded with by way of indictment. Overall, during the 4½ year period between 2000 and the first half of 2004, the Prosecution Authority obtained convictions in just over 85% of the money laundering cases that went before the courts. The following chart sets out the total number of convictions that were obtained in all money laundering cases that went before a court. The conviction rate appears as a percentage in brackets after the number of convictions.

CONVICTION RATE IN MONEY LAUNDERING CASES[29]					
TYPE OF OFFENCE *(Statistics provided by STRASAK)*	2000	2001	2002	2003	2004 (up to 30.06.2004)
Ordinary money laundering: Assisting in securing proceeds of	30	27	17	78	7

[29] These statistics do not include convictions for money laundering offences related to receiving the proceeds of crime.

crime less than NOK 75 000 (EUR 9 100 / USD 11 900) for another person	(94%)	(73%)	(84%)	(96%)	(70%)
Aggravated money laundering: Assisting in securing proceeds of crime greater than NOK 75 000 (EUR 9 100 / USD 11 900) for another person	11 (85%)	8 (92%)	27 (87%)	10 (83%)	7 (88%)
Drug-related money laundering: Assisting in securing the proceeds of drug trafficking for another person	-	-	-	-	-
Negligent money laundering: Negligently assisting in securing the proceeds of crime for another person	20 (91%)	61 (85%)	96 (91%)	151 (83%)	86 (84%)
ANNUAL TOTALS	61 (90%)	96 (83%)	140 (87%)	239 (87%)	100 (80%)

87. The Norwegian authorities also report that, having detected money laundering activity, they are sometimes able to detect the predicate offence(s) as well.

88. ***Recommendation 2:*** The offence of money laundering applies to natural persons that knowingly engage in money laundering activity (intentional money laundering), as required by the FATF Recommendations. However, section 317 goes farther than this by also expressly criminalising negligent money laundering (i.e. where the perpetrator should have known that the proceeds in question were generated from a crime). Intent in respect of section 317 also includes situations where an accused acknowledged the possibility that property could be the proceeds of crime and reconciled himself/herself with that possibility ("*dolus eventualis"*). This means that a perpetrator is unable to avoid liability by turning a blind eye to the fact that property is the proceeds of crime (i.e. wilful blindness). Although the concept of *dolus eventualis* does exist in Norwegian law, it is not known how frequently such cases are pursued. Although the law does not expressly say so, case law and legal tradition permit the mental element of the offence to be inferred from objective factual circumstances.

89. Criminal liability for money laundering applies to both natural and legal persons, including companies, societies or other associations, one-man enterprises, foundations and public entities (PC s.48a para.2). When a natural person who has acted on behalf of a legal person commits money laundering, the legal person may also be criminally liable—even if no natural person may be punished for the offence (i.e. when a director or employee acting within the scope of his/her authority acts on behalf of the legal person) (PC s.48a). There is no express bar to pursuing parallel criminal, civil and administrative proceedings against a legal person. However, in deciding whether to penalise a legal person for money laundering, the court shall take into account whether other sanctions have already been imposed on the legal person or on a natural person who was acting on its behalf (PC s.48b). Parallel criminal and administrative sanctions may not be imposed if to do so would violate the Strasbourg Human Rights Convention (Norwegian Act 30/1999 on Human Rights).

90. Norway has implemented an effectively dissuasive range of penalties in the case of legal persons found guilty of money laundering. Legal persons found guilty of money laundering are punishable by a fine (PC ss.26a, 27, 48a, 48b and 317; MLA s.16). There is no limit on the size of the fine that could be imposed; and in a case in January 2005 a fine of NOK one million, and a confiscation order for NOK one million was imposed on a company that committed a money laundering offence involving the proceeds of an offence against competition law. Additionally, the legal person may be deprived of the right to carry on business or may be prohibited from carrying it on in certain forms (PC s.48a para.3). In deciding whether to impose a penalty on a legal person and in assessing the penalty itself, the court must consider the following factors (PC s.48b):

(a) The preventative effect of the penalty;

(b) The seriousness of the offence;

(c) Whether the legal person could have prevented the offence by guidelines, instruction, training, control or other measures;

(d) Whether the offence was committed for the purpose of promoting the legal person's interests;

(e) Whether the legal person has or could have obtained any advantage by the offence;

(f) The economic capacity of the legal person; and

(g) Whether, as a consequence of the offence, other sanctions have been imposed on the legal person or on a natural person who has acted on its behalf (PC 48b).

91. Natural persons found guilty of the ordinary ML offence (i.e. where the amount involved is less than NOK 75 000/EUR 9 100/USD 11 900) are punishable by (unlimited) fines or a term of imprisonment not exceeding three years. The penalty of three years is consistent with other Nordic countries, but somewhat lower than the lowest maximum threshold of four years that is prescribed by European Union countries (Council of Framework Decision of 26 June 2001, 2001/500/JHA)with respect to money laundering offences. However, this is ameliorated by the fact that the penalty for aggravated ML is (unlimited) fines or a term of imprisonment not exceeding six years (cf. PC s.317 para.3) or 11 years if committed as part of the activity of an organised criminal group (PC s.60a), and the threshold for aggravated money laundering is quite low. Indications of an aggravated offence include: (i) the amount involved exceeds about NOK 75 000 (EUR 9 100/USD 11 900); (ii) the type of predicate offence; (iii) the way in which the laundering was carried out; (iv) whether the offender habitually engaged in that offence; and (v) the state of mind of defendant. The prosecuting authorities can charge an accused with aggravated ML or the court can independently find that aggravating circumstances exist. A person who commits ordinary ML as part of the activity of an organised criminal group or network is liable to six years imprisonment (double the length of what would otherwise have been imposed).[30] Negligent ML is punishable with a (unlimited) fine or a term of imprisonment not exceeding two years (PC s.317 para.5).

92. In general, repeat offenders are subject to double the term of imprisonment (up to the maximum term of imprisonment allowable for the offence) (PC s.61). Consequently, persons convicted more than once of negligent, ordinary and aggravated ML are subject to a maximum penalty of four years, six years and 12 years respectively. Even though the offence of money laundering is still considered to have taken place, the perpetrator cannot be punished if it is proven that he/she committed the offence while psychotic, unconscious, very mentally retarded, intoxicated or under 15 years of age (PC ss. 44-46, cf.317). In practice, the penalties imposed for money laundering are generally lower than the maximum penalty allowable for the offence.[31] In sentencing, the court takes into account (among other things) the level of punishment for the predicate offence. The following are some specific examples of the range of sentences imposed in money laundering cases:

(a) 7 years imprisonment for laundering NOK 6.5 million (EUR 788 000/USD 1 million) of proceeds from drug trafficking offences;

(b) 2.5 years imprisonment (of which 1 year was suspended) for attempted laundering of NOK 108 million (EUR 13 million/USD 17 million);

[30] An organised criminal group is three or more persons that have, as their main objective, the commission of a criminal offence which may be punished with imprisonment of at least three years, or a considerable part of its activity consists of the commitment of such criminal offences (PC s.60a).

[31] Additionally, a prisoner may be released on parole after two thirds (and no less than 60 days) of the punishment is served. If the punishment is less than 14 days, the prisoner may only be released on parole if there are weighty reasons to do so.

(c) 6 months imprisonment (of which 2 months was suspended) for negligent money laundering of about NOK 1.1 million (EUR 133 000/USD 174 000) that probably stemmed from extortion;

93. Overall, Norway has implemented a wide range of penalties (some of which are very dissuasive) for both natural and legal persons found guilty of money laundering. Norway has also proven itself effective in sanctioning money laundering activity, given the very high conviction rate in those cases that go before the courts. Nevertheless, given the very low threshold (any cases involving NOK 75 000/EUR 9 100/USD 11 900) or more), there is a much smaller number of aggravated ML cases than one might expect. It is not known why this is the case; however, as Norway goes forward, this is an issue that should be explored to ensure that the penalties which can be applied are effective, proportionate and dissuasive having regard to both the amount of money being laundered and the mental culpability of the accused—particularly if negligent ML cases are involving large amounts of proceeds. Of course, in considering this issue, it should also be remembered that all of Norway's ML convictions are for third party ML (since self-laundering is not an offence). This is significant because it will almost always be more difficult to prove the mental element of the offence to the standard of intentional ML in a third party ML case than it would be in a case of self-laundering (where the perpetrator also committed the predicate offence).

2.1.2 Recommendations and Comments

94. Norway's money laundering offences are broad in their scope and, given the number and ratio of successful prosecutions to convictions, the offence seems easy for prosecutors to use. Statistics show a significant number of prosecutions and convictions overall, with a particularly high conviction rate (in the region of 85%) However, some minor enhancements could be made to an otherwise effective regime, including extending the offence to self-laundering and to conspiracies involving two people.

95. Norway should also ascertain why the number of aggravated ML cases remains small (even though the threshold for the offence is very low). Depending on the underlying reasons, Norway should consider whether additional legislative measures need to be taken such as: (i) increasing the maximum penalties for all ML offences (including negligent ML); (ii) prescribing a single higher maximum penalty for all forms of money laundering (except drug-related ML if Norway wants to maintain the high maximum for this form of ML); (iii) combining the intentional and negligent ML offences into a single offence, but then allow for a finding of negligence to be considered a mitigating factor at sentencing; or (iv) providing for a higher penalty for negligent ML where circumstances would otherwise constitute aggravated ML (e.g. 4 years which is the penalty that currently applies to repeat offenders convicted of negligent ML). The latter two approaches would ensure that in cases of negligent ML where the amounts involved are particularly high (i.e. what would otherwise be an aggravated offence), a higher maximum penalty would be possible. Any of these proposed legislative solutions would leave the courts more room to take into account all factors (such as the amounts involved, the seriousness of the predicate offence, the offender's state of mind, extenuating circumstances, etc.) when deciding an appropriate penalty. Alternatively, further training measures may be appropriate such as providing additional training to prosecutors on how to prove the mental element of the ML offence, or to judges for the purposes of enhancing their ability to manage the complexities of a money laundering case.

96. Concerning the two exceptions in section 317 whereby a person receiving proceeds of crime is not subject to punishment, Norway is of the view that it is preferable to articulate these exceptions (which are very narrow) within the offence itself so that it is very clear when they apply, rather than repealing the exceptions and leaving it entirely as a matter for prosecutorial discretion. However, in practice, both of these exceptions are rarely used; prosecutors cannot charge persons who fall within these exceptions. The assessors are concerned that articulating these exceptions for third parties, along side the exception in respect of self-laundering, creates an opportunity for criminals to use their

criminal proceeds for the support (in part at least) of their ordinary lifestyle with impunity. Moreover, it may create inflexibility by precluding a prosecutor from pursuing appropriate cases that, technically speaking, fall within the scope of the exceptions. However, as there is no indication that these concerns have been realised, this point is raised for Norway's consideration only and does not affect its compliance rating

2.1.3 Compliance with Recommendations **1 & 2**

	Rating	Summary of factors underlying rating
R.1	LC	• Self-laundering is not a criminal offence and there is no fundamental principle of Norwegian law that would preclude self-laundering from being an offence. • The conspiracy offence would not extend to a conspiracy involving only two people, the requirement for an "organised criminal group" with a particular purpose would only apply to certain ML scenarios and there is no fundamental principle of domestic law that would preclude such conduct being criminalised.
R.2	C	• Recommendation 2 is fully observed.

2.2 Criminalisation of Terrorist Financing (SR.II)

2.2.1 Description and Analysis

97. ***Special Recommendation II:*** Terrorist financing has been an independent criminal offence in Norway since 28 June 2002 (PC s.147b). Section 147b criminalises two types of terrorist financing activities. The first is to obtain or collect funds or other assets with the intention that they should be used (in full or in part) to finance terrorist acts (PC s.147b para.1). The term *terrorist acts* refers to a range of criminal offences[32] (including those types of conduct set out in Articles 1(a) and (b) of the Terrorist Financing Convention) that are considered to be terrorist acts if it is found that the offence in question was committed with the intention of:

(a) seriously disrupting a function of vital importance to society (inter alia the legislative, executive or judicial authority, power supply, safe supply of food or water, the bank or monetary system or emergency medical services or disease control);

(b) seriously intimidating a population; or

(c) unduly compelling public authorities or an intergovernmental organisation to perform, tolerate or abstain from performing any act of crucial importance for the country or the organisation, or for another country or another intergovernmental organisation (PC ss.147a and 147b).

98. The second type of activity criminalised under s.147b is to make funds or other assets, bank services or other financial services available to:

(a) Any person or enterprise that commits or attempts to commit terrorist acts as mentioned in s.147a;

(b) Any enterprise that is owned or controlled by persons/enterprises that commit or attempt to commit terrorist acts (cf.PC s.147b); or

(c) Any person or enterprise that acts on behalf of or at the direction of: (i) persons/enterprises that commit or attempt to commit terrorist acts; and/or (ii) an enterprise that is owned or controlled by persons/enterprises that commit or attempt to commit terrorist acts (PC s.147b para.2).[33]

[32] See Annex 11 for a complete list of the activities which constitute terrorist acts under sections 147a and 147b of the Penal Code.

[33] In this context, *enterprise* means a company, society or other association, one-man enterprise, foundation, estate (meaning an estate in bankruptcy or the estate of a deceased person) or public authority (PC s.48a).

99. Section 147b could also reasonably be interpreted to criminalise the provision of funds, assets and services both to terrorist organisations, as well as in respect of activities that would amount to terrorist acts as described in section 147a.

100. Norway has criminalised terrorist financing in a manner that is consistent with the Terrorist Financing Convention. However, the obligations under Special Recommendation II—as elaborated in the Interpretative Note to Special Recommendation II (INSR II)—go beyond what is required by the Terrorist Financing Convention. In addition to criminalising the activities enumerated in the Terrorist Financing Convention, countries are also obligated to criminalise a third type of activity—collecting funds in the knowledge that they are to be used (for any purpose) by a terrorist organisation or an individual terrorist. Norway has not yet criminalised this third type of activity; however, it should also be noted that the FATF issued INSR II in June 2004—only seven months prior to the on-site visit.

101. The terrorist financing offences apply to *funds or other assets.* These terms are not defined; however, the Preparatory Works to the Terrorist Financing Offence explicitly state that the term *funds or other assets* covers anything having an economic value. This is broad enough to meet the definition of *funds* in the Terrorist Financing Convention. The terrorist financing offences do not require that the funds were actually used to carry out or attempt a terrorist act(s). Nor do they require that the funds be linked to a known or identified terrorist act.

102. Norway also has a comprehensive range of ancillary offences to the terrorist financing offence. In particular, it is also an offence to: (i) attempt to commit terrorist financing (PC s.49); (ii) participate as an accomplice in a terrorist financing offence (PC s.147b); or (iii) enter into an agreement to commit terrorist financing as part of the activity of an organised group or network (PC s.162c).

103. Norway's terrorist financing offence has broad application and can be used to punish the financing of a terrorist act even where the terrorist act was committed outside of Norway although this is not immediately expressly clear from the wording of section 147b itself. Section 147b criminalises the financing of the criminal offences that are described in section 147a. Section 147a includes those acts which constitute offences within the scope of the relevant United Nations treaties against terrorism.[34] Qualifying language in section 147a—such as references to "society" and "that country" may indicate that s.147a could be interpreted as being limited to terrorist acts committed domestically. However, Norway advised that the Preparatory Works and their legal traditions mean that the offence does cover terrorist offences committed outside Norway. In addition there are contra-indications within s.147a itself. Importantly, s.147b must be read in conjunction with section 12 of the Penal Code. Section 12 is a general provision that provides for extra-territorial jurisdiction in respect of certain offences (including sections 147a and 147b) for Norwegian nationals and residents and in certain cases even for foreigners (PC s.12). Consequently, the financing of terrorist acts committed both domestically and abroad are covered.

104. The terrorist financing offence is subject to the same principles as the money laundering offence concerning: (i) inferring the intentional element of the offence from objective circumstances; (ii) criminal liability for legal persons; and (iii) the possibility of parallel criminal, civil or administrative proceedings (see paragraphs 88 to 89 of this report). As with the money laundering offence, these requirements are met for the purpose of the terrorist financing offence.

[34] Convention for the Suppression of Unlawful Seizure of Aircraft (1970), Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation (1971), Convention on the Prevention and Punishment of Crimes against Internationally Protected Persons, including Diplomatic Agents (1973), International Convention against the Taking of Hostages (1979), Convention on the Physical Protection of Nuclear Material (1980), Protocol for the Suppression of Unlawful Acts of Violence at Airports Serving International Civil Aviation, supplementary to the Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation (1988), Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation (1988), Protocol for the Suppression of Unlawful Acts against the Safety of Fixed Platforms located on the Continental Shelf (1988), and the International Convention for the Suppression of Terrorist Bombings (1997).

105. The penalties for terrorist financing seem to be sufficiently proportionate and dissuasive. Terrorist financing is punishable by a term of imprisonment not exceeding 10 years. Accomplices are liable to the same penalty (PC s.147b). In terrorist financing cases in particular, corporate liability may be considered as an alternative by the Prosecution Authority if an organisation or financial institution is involved and it proves difficult to establish personal liability.

106. To date, there have been no prosecutions for terrorist financing in Norway. Nor has the MLU received any suspicious transaction reports in which it was indicated that the underlying suspicion relates to terrorist financing. However, this is not very surprising given the Norwegian context in which threat assessments indicate that terrorist-related activities are probably being carried out only on a very limited scale involving a small number of persons. Even though terrorist financing does not appear to be a major problem in Norway, the authorities are aware of the issue and have pursued cases where signs of possible terrorist financing exist. One terrorist financing investigation has been carried out; however, the case was dropped in 2004 due to lack of evidence, despite some indications of terrorist financing having been detected. Additionally, the police initially had a weak suspicion of terrorist financing in two cases on Hawala banking (both of which were conducted before the courts), but terrorist financing did not become a specific subject in the investigations. Norway reports that the challenge in investigating terrorist financing cases has been proving the final destination of the funds and whether the individuals involved (i.e. in collecting, transmitting, transporting or receiving funds) are connected to terrorist acts or terrorist organisations.

2.2.2 Recommendations and Comments

107. Norway's criminalisation of terrorist financing is generally in line with the international standard—in particular, with the Terrorist Financing Convention. The terrorist financing offence of section 147b clearly covers the obtaining or collecting of funds and assets in respect of the commission of terrorist acts (those included in the scope of section 147a) and making funds available to terrorists or terrorist organisations. However, Norway should clarify its legislation to ensure that the offence covers collecting funds in the knowledge that they are to be used (for any purpose) by a terrorist organisation/individual terrorist. The effectiveness of Norway's terrorist financing offence cannot be measured because no cases have been before the Norwegian courts.

2.2.3 Compliance with Special Recommendation II

	Rating	Summary of factors underlying rating
SR.II	LC[35]	• In addition to criminalising the activities enumerated in the Terrorist Financing Convention, countries are also obligated to criminalise a third type of activity—collecting funds in the knowledge that they are to be used (for any purpose) by a terrorist organisation or an individual terrorist. Norway has not yet criminalised this type of activity.

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

2.3.1 Description and Analysis

Confiscation

108. Norway has implemented a comprehensive confiscation system that is achieving good results. Confiscation of the proceeds from any criminal offence (or property of corresponding value) is mandatory, including any asset, profit or other benefit derived directly or indirectly from the proceeds (PC s.34). To trigger confiscation, the Prosecution Authority must prove to the criminal standard of proof that a specific criminal offence generated the proceeds; however, the burden of proof may be

[35] The effectiveness of Norway's terrorist financing offence cannot be measured because no cases have been before the Norwegian courts.

eased as regards the amount of the proceeds. If the amount or value of the proceeds cannot be established, it only needs to be proven to the civil standard. If, on the basis of objective circumstances, the Prosecution Authority can prove that the property is the proceeds of crime, confiscation may take place regardless of whether the money launderer knew that the property was proceeds. Confiscation may apply even when the money launderer cannot be punished because he/she committed the crime while psychotic, very mentally retarded, intoxicated or under 15 years of age (PC ss.44 to 46). However, exemptions can be made if the court finds that confiscation would clearly be unreasonable. Such exemptions are only intended to be used as a safety valve (i.e. when the proceeds have been spent and the perpetrator has a poor financial situation) and should not apply in serious cases (Preparatory Works to the Penal Code). This interpretation has been followed by the Supreme Court in serious drug trafficking cases. When determining whether or not to confiscate proceeds, the court must consider whether such confiscation is necessary for the purpose of penalising the crime. This involves balancing the public interest in the case with the interests of the offender. As a general rule, the public interest in confiscation is strong in a money laundering case.

109. Confiscation of instrumentalities used or intended for use in the commission of any criminal offence (or property of corresponding value), or which are the product of such an offence, may be confiscated if this is considered an appropriate penalty for the act (PC s.35 para.2). Instrumentalities that belong to a third party (or an amount of corresponding value) may also be confiscated if the third party understood or should have understood that the object was meant for use in a criminal act (PC s.36). Confiscation of goods (including rights and claims) that have been produced by or been the subject of the money laundering (corpus delicti) (or property of corresponding value) is also discretionary (PC s.35).

110. The general rule is that proceeds will be confiscated from the persons to whom the gains have directly accrued through the act (PC s.34 para.4). The presumption is that proceeds will be confiscated from the offender, unless the offender rebuts this presumption by showing on the balance of probabilities that the benefits accrued to a third party**.** For instance, if proceeds were transferred directly to the bank account of the offender's wife, those proceeds shall be confiscated from her (PC s.34). Action can be taken against proceeds held by third parties who knew that the property was derived from a criminal offence or it was a gift in whole or in part.

111. Norwegian law provides for three principal types of provisional measure—charging, freezing and seizure**.** Freezing and seizure differ in the following way. Freezing only applies to property suspected of relating to terrorism or terrorist financing and has the effect that the suspect (or a third party) keeps possession of the property, but is legally prevented from disposing of it (CPA chapter 15b). Seizure deprives the suspect (or a third party) of the possession of the property, and prevents any dealing, transfer or disposal of it. The power to seize can also be used with an associated freezing mechanism, which is often used in practice when seizing certain types of property. For example, if the Prosecution Authority decides to seize shares that are registered in the Shareholders Register, the Prosecution Authority's seizure decision is sent to the Register accompanied by an order to freeze the shares. In this case, the seized shares remain on the same account, but the owner cannot dispose of them as long as they are frozen. A similar mechanism applies to freezing money on a bank account. In practice, the police will leave the money in the account (although they could take possession of it), but with an instruction to the bank that the account holder cannot dispose of it. Charging involves placing a charge on the property for a specific amount in order to secure payment of a fine, a confiscation order, the costs of a case, damages or redress for which it is assumed that the person charged will be found liable and when there is reason to fear that the execution will otherwise be precluded or essentially impeded (CPA s.217). Seizure and charging measures can be taken against any type of property, including money in a bank account.

112. In the case of capital assets, when there is a reason to fear that execution will otherwise be precluded or essentially impeded, the court may decide that a charge for a specific amount should be made on capital assets belonging to a person charged with an offence in order to secure the payment of

confiscation orders (for which it is assumed that the suspect will be adjudged liable) (PC s.217). Charging orders may also be made on assets belonging to third parties. Charging can also be used to secure a value-based confiscation claim, although the charging order itself must be related to specific assets. An order cannot be made to charge all of the defendant's assets as a whole. This may create problems in extended confiscation cases where the prosecution does not know all of the property that is owned or controlled by a defendant at the time of charge. It is unclear whether a court has the power to order a defendant to disclose all of his/her assets. However, law enforcement and prosecution authorities may gather information about the assets which a person has declared to the tax authorities in the context of filing tax returns. The charging may continue until a final and enforceable decision has been made in the case (CPA s.217).

113. The procedure for obtaining a charging order is flexible enough to allow the Norwegian authorities to act swiftly in appropriate circumstances, while still containing safeguards of individual rights. The principal rule is that the court takes the decision on charging property following a petition from the Prosecution Authority. However, in urgent cases, the Prosecution Authority may take the decision itself. In both cases, the decision to charge is taken without prior notice to the party concerned. The Prosecution Authority has the possibility to appeal if the court rejects the petition. The Prosecution Authority must notify the court after the execution of the charging order. The court will then summon a court hearing to determine whether the charge on the property shall be sustained (CPA s.218). Charging on real estate needs to be registered in the Real Estate Register. The order of the court regarding sustaining of a charging order is subject to interlocutory appeal under the Criminal Procedure Act.

114. Objects that are deemed to be liable to confiscation may be seized. Seizure can only take place in order to secure property-based confiscation. A seizure order applies only to specified assets and cannot be made to seize all of the defendant's assets. The Commission on Confiscation previously recommended such a power, but ultimately the government did not propose this when the legislation was amended. As in the case of charging orders, the procedure for obtaining seizing orders allows for even swifter action by prosecution authorities, followed by appropriate checks and balances. The principal rule is that the Prosecution Authority takes the decision on seizure; however, the police may effect a seizure when it carries out a decision for search or arrest, and otherwise when delay entails a risk. However, if the police take the decision, the Prosecution Authority must be notified as soon as possible and must decide whether the seizure should be sustained. Seizure may continue until a final and enforceable decision has been made in the case (CPA s.208).

115. The decision to seize and the execution of that seizure are taken without prior notice to the suspect or third party. The principal rule is that notification should be given after the execution of the seizure. The suspect or any third party that has an interest in the property may then ask the court to decide whether the seizure decision should be sustained. However, notification may be waived if there are reasonable grounds to suspect that a criminal act that can be punished by imprisonment of more than six months is committed, and that notification may severely impede the investigation (CPA s.208). Property that has been frozen/seized is not released to meet the defendant's legal expenses, which are met by the State. However an amount may be released to meet the basic living expenses of defendant's dependents.

116. Norway has also implemented measures to ensure that confiscation orders cannot be thwarted by transferring property to third persons. The proceeds of crime or instrumentalities of crime can be confiscated from a third party if they were transferred to the third party: (i) after the offence was committed; (ii) by an offender who is subject to confiscation; and (iii) the third party did not give anything in return (i.e. the third party received the proceeds as a gift); or (iv) the receiver understood or should have understood the connection between the criminal act and the object transferred to him (PC s.37a). In such cases, property-based or value-based confiscation can take place, regardless of the third party's state of mind. On the other hand, if a bona fide third party gave something in return for the proceeds, confiscation is not allowed, thus protecting the rights of bona fide third parties.

However, if the value of the goods/services given by the third party in exchange for the proceeds is not consistent with the value of the proceeds, confiscation of the surplus may be confiscated regardless of the third party's state of mind or good faith. If the court is considering confiscation from a third party, the third party is entitled to be a party in the case. However, the court may confiscate seized property in proceedings against the offender or the possessor at the time of the seizure, if the owner is unknown or does not reside in Norway—provided that this is reasonable having regard to the nature of the case and other circumstances (PC s.37c). Legal arrangements (whether contractual or otherwise) containing provisions that are contrary to the law are considered null and void. Where persons involved knew or should have known as a result of their actions that authorities would be prejudiced in their ability to recover property subject to confiscation, those actions are considered never to have taken place.

117. The police and the Prosecution Authority, including ØKOKRIM, have investigative powers to identify and trace assets. These powers are the same as those which are available to investigate crimes of money laundering and terrorist financing, and include the power to order production of documents, conduct surveillance, search persons and premises, and seize funds and assets. For additional details on the investigative powers available to law enforcement, prosecution and other competent authorities, see section 2.6 (paragraphs 177 to 181) of this report.

118. Norway's confiscation system has achieved very positive results. The number of confiscation orders and total amount of assets confiscated has increased, especially in the period from 2002 to 2003. The following chart sets out the total number of confiscation orders granted and the amount of money confiscated by the Norwegian authorities between 1997 and 2003.

NUMBER OF CONFISCATION ORDERS AND AMOUNT OF MONEY CONFISCATED		
Year	Number of confiscation orders issued	Amount of money confiscated *(Source of statistics: Statens Innkrevingssentral (SI))*
1997	734	NOK 63.2 million (EUR 7.6 million/USD 10 million)
1998	676	NOK 43.2 million (EUR 5.2 million/USD 6.8 million)
1999	724	NOK 34.2 million (EUR 4.1 million/USD 5.4 million)
2000	859	NOK 45.1 million (EUR 5.5 million/USD 7.1 million)
2001	845	NOK 42.7 million (EUR 5.2 million/USD 6.8 million)
2002	628	NOK 58.4 million (EUR 7.1 million/USD 9.2 million)
2003	929	NOK 143.4 million (EUR 17.4 million/USD 22.7 million)

119. In 2003, the number of confiscation orders issued and the total amount of funds seized in relation to drug trafficking, money laundering and alcohol smuggling were as follows: 387 confiscation orders (representing a total of NOK 16.1 million (EUR 2 million/USD 2.5 million) in confiscated funds) relating to drug trafficking offences; 54 confiscation orders (representing a total of NOK 11 million (EUR 1.3 million/USD 1.7 million in confiscated funds) relating to money laundering offences pursuant to section 317 of the Penal Code; and 12 confiscation orders (representing a total of NOK 64 million (EUR 7.8 million/USD 10.1 million) in confiscated funds) relating to alcohol smuggling offences. The highest amount confiscated in a single case was NOK 50 million (EUR 6.1 million/USD 7 .9 million) which was confiscated in a smuggling case.

120. The following charts sets out the value of funds confiscated by ØKOKRIM in relation to its own cases in the last ten years.

VALUE OF FUNDS CONFISCATED BY ØKOKRIM IN RELATION TO THE NUMBER OF SENTENCES ISSUED		
YEAR	NUMBER OF CASES	AMOUNT CONFISCATED

1995	8	NOK 8.9 million (EUR 1.2 million/USD 1.4 million)
1996	6	NOK 700 000 (EUR 85 000/USD 111 000)
1997	3	NOK 27.2 million (EUR 3.3 million/USD 4.3 million)
1998	5	NOK 2.2 million (EUR 267 000/USD 348 000)
1999	11	NOK 4.7 million (EUR 570 000/USD 743 000)
2000	15	NOK 5.1 million (EUR 618 000/USD 806 000)
2001	11	NOK 19.5 million (EUR 2.4 million/USD 3.1 million)
2002	10	NOK 23.2 million (EUR 2.8 million/USD 3.7 million)
2003	20	NOK 9.8 million (EUR 1.2 million/USD 1.5 million)
2004	22	NOK 17.9 million (EUR 2.2 million/USD 2.8 million)
January 2005	1	NOK 1.1 million (EUR 133 000/USD 174 000)

121. The following chart sets out the value of funds confiscated by the Oslo Police District in relation to its own cases in the last three years.

VALUE OF FUNDS CONFISCATED BY OSLO POLICE DISTRICT IN RELATION TO THE NUMBER OF SENTENCES ISSUED		
YEAR	NUMBER OF SENTENCES	AMOUNT CONFISCATED
2002	114	NOK 5.5 million (EUR 667 000/USD 870 000)
2003	239	NOK 12.0 million (EUR 1.5 million/USD 1.9 million)
2004	N/A	NOK 17.1 million (EUR 2.1 million/USD 2.7 million)

122. Although charging and seizing can take place until a legally enforceable confiscation order is made, it cannot take place after a confiscation order has been issued (CPA s.217). Consequently, if the police later find proceeds of crime related to the offence for which the offender was convicted (or find other assets which can be used to enforce the confiscation claim), no charging or seizing action can take place. Instead, the enforcement authorities must be summoned and the assets attached or other interim measures taken. The Norwegian authorities admit that this procedure is "cumbersome and inappropriate" (Action Plan 2004 s.9.6.1). However, taken by itself, this factor does not affect the rating.

123. Norway also keeps statistics concerning the value of property that is subject to confiscation orders, but cannot ultimately be satisfied. As of 31 December 2003, the amount outstanding at the State Agency for the Recovery of Fines, Damages and Costs was NOK 268 million (EUR 32.5 million/USD 42.4 million)—an amount that was aggregated over many years and which represents one third of the value of all property that is subject to confiscation orders. When considering this amount, it is important to note that there are many possible reasons why the full value of property cannot always be recovered. Some of these reasons are not within the authorities' control (e.g. the assets needed to enforce the claim have depreciated or are no longer available because they have been spent/dissipated by the offender, successfully hidden or transferred to bona fide third parties). Another reason (over which the authorities do have some control) is that the police may not secure confiscation claims by seizure (pursuant to CPA s.203 ff) or by charging (pursuant to CPA s.217 ff) early on in the case. Consequently, by the time a confiscation order is issued (usually at the end of the case), the assets are no longer available. Norway is aware of this problem and continues to focus on raising the awareness of police concerning the need to secure confiscation claims (either by charging or seizure) early on in the case (Action Plan 2004 s.9.6.1). This awareness-raising is generating results; the trend in recent years has been that more property is being charged or seized by the Norwegian authorities than was previously the case. It should also be noted that, because Norway has implemented a

mandatory confiscation system, confiscation orders will be issued in cases where the recovery of the proceeds of crime was never possible because the court must order the confiscation of the proceeds, regardless of whether assets are available to satisfy the order.

124. The following chart sets out the value of funds frozen and seized by ØKOKRIM in relation to its own cases in the last five years (not including the value of frozen and seized non-fund assets).

VALUE OF FUNDS FROZEN/SEIZED BY ØKOKRIM	
YEAR	AMOUNT FROZEN AND SEIZED
2000	NOK 6.2 million (EUR 752 000/USD 980 000)
2001	NOK 23.2 million (EUR 2.8 million/USD 3.7 million)
2002	NOK 19.7 million (EUR 2.4 million/USD 3.1 million)
2003	NOK 90.5 million (EUR 11 million/USD 14.3 million)
2004	NOK 78.8 million (EUR 9.6 million/USD 12.5 million)

125. *Additional elements:* Norway has also implemented additional elements that go further and greatly enhance the effectiveness of its confiscation regime. In serious cases (i.e. those which attract a significant penalty of imprisonment and which may result in a considerable gain), the option of extended confiscation is available (PC s.34a). *Considerable gain* has been interpreted to mean gain of at least NOK 75 000 (EUR 9 000/USD 11 900) (Case citation Rt. 1999/1299). If the offender's property is subject to extended confiscation, property of a corresponding value belonging to the offender's current or former spouse/common law spouse/same-sex partner may also be confiscated (if the property was acquired in the course of the marriage and no more than five years before the commitment of the criminal act that provides the basis for extended confiscation). Additionally, property of the offender's *next of kin,* or legal persons that the offender owns or controls may also be confiscated on the same grounds (PC s.37a). The term *next of kin* includes the offender's spouse, ascendants and descendants, siblings, etcetera (PC s.5). In such cases, the Prosecution Authority must prove on a balance of probabilities that the property stems from criminal acts committed by the offender. If all of the conditions to impose extended confiscation are met, the burden of proof is reversed and the offender must prove on the balance of probabilities that the assets were legally obtained (PC s.34a). The reverse burden of proof makes this a very effective tool that is readily available to prosecutors since the threshold for extended confiscation is very low. Confiscated funds go to the Norwegian government (PC s.37d) or may be used to satisfy the claims of victims of crime. There are no civil forfeiture provisions or provisions on automatic confiscation of the proceeds of organised crime groups.

2.3.2 Recommendations and Comments

126. Norway has concentrated great effort on depriving criminals of the proceeds of crime, and has implemented a comprehensive system that is achieving this result. Moreover, Norway continues to focus on this as an important objective. For instance, competence building is an ongoing task and, consequently, Norway continues to work on improving the awareness of police concerning the need to secure confiscation claims (either by charging or seizure) early on in the case. As this work seems to be having a positive effect, it should be continued. Norway should also consider implementing the following elements that, while not required by the FATF Recommendations, would further enhance an already effective confiscation regime: giving the authorities the power to seize/charge all of the defendant's property in appropriate cases (not just specified property); ensuring that the court can order a defendant to disclose all of his/her assets; and allowing property to be seized/charged after a confiscation order has been issued. Although there is some concern about the fact that one third of the value of confiscation orders is not enforced, which goes to the effectiveness of the system, this is balanced overall by the effective implementation of other aspects of the confiscation system, and by

the fact that Norway has already proposed measures in the Action Plan to improve the situation. It may also be that some of the reasons for failure to recover the proceeds are not indicative of ineffectiveness (i.e. if the proceeds have been dissipated before the crime is discovered). Norway should examine whether better data could be collected to identify the causes of this situation and whether it is changing over time.

2.3.3 Compliance with Recommendations 3

	Rating	Summary of factors underlying rating
R.3	C	• Recommendation is fully observed.

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

2.4.1 Description and Analysis

127. Norway has implemented measures to freeze terrorist funds and other assets both in the context of the relevant United Nations Security Council Resolutions—S/RES/1267(1999) and its successor resolutions, and S/RES/1373(2001)—and ordinary criminal investigations. Freezing property in the terrorist financing context means preventing anyone from having the property at his/her direct or indirect disposal. Typically, this involves blocking a bank account. The main purpose of freezing property is to temporarily freeze a person's property as a means of preventing him/her from using the funds to carry out terrorist acts.

128. ***Freezing action pursuant to S/RES/1267(1999):*** United Nations Security Council Resolutions (UNSCRs) S/RES/1267(1999), S/RES/1333(2000) and S/RES/1390(2002), adopted by the United Nations Security Council (UNSC), are implemented by an enabling statute (Act of 7 June 1968 No.4), and further implemented by regulations laid down in the Royal Decree of 22 December 1999 (later amended on 19 January 2001 and 18 January 2002) (Royal Decree). The Act and Royal Decree provide for the authority to freeze and include an effective mechanism for automatically incorporating any changes to the lists attached to these UNSCRs into the Norwegian legal system. Because the regulations cross-reference the United Nations (UN) website, any updates to the UN lists under S/RES/1267(1999) are automatically effected in Norwegian law without further action by the Norwegian authorities. As an added measure, the Ministry of Foreign Affairs also distributes the updates manually to relevant authorities and institutions for their attention. The Act prohibits anyone from making any funds available to entities listed. Breaches are penalised in the Act (a maximum of 3 years imprisonment; a fine may also be imposed). However, Norway has not implemented measures to monitor compliance with the 1968 Act and Regulations. The Ministry of Foreign Affairs is responsible for the Act of 7 June 1968 and the Royal Decree. The scope of such freezing actions meets the requirements of Special Recommendation III in that such freezing actions extend to any funds or other financial assets or economic recourses belonging to designated individuals, groups or undertakings, or any entity associated with them. This includes any fund derived from property owned or controlled, directly or indirectly, by designated entities or by persons acting on their behalf or at their direction. It is furthermore prohibited to directly or indirectly make any funds, financial assets or economic resources available for such persons' benefit.

129. There is no difference between de-listing and unfreezing requests, as far as Norway's implementation of S/RES/1267(1999) is concerned. The freezing action can be legally challenged by the entity frozen; however, the Norwegian authorities could not point at clear gateways for such action. Rather it is assumed that the entity frozen will use the same legal mechanisms that any citizen has at its disposal to challenge governmental decisions. The Norwegian authorities also stated that a Norwegian court would have the discretion to overrule the UNSC decisions, by attaching higher weight to other provisions contained in the United Nations Charter. However, Norwegian authorities also noted that their courts do not have the authority to judge over UN-based designations made pursuant to S/RES/1267(1999).

130. Norway has issued some guidance to financial institutions and other persons/entities that may be holding targeted funds/assets; however, this guidance (Circular no.22/2003) focuses more on how the FSA processes such lists, rather than giving guidance to financial institutions as to how they should be meeting their obligations concerning freezing orders issued pursuant to S/RES/1267(1999). Moreover, it is focused on providing guidance to financial institutions on how to freeze assets of persons designated pursuant to the Regulations relating to special measures against the Republic of Zimbabwe adopted on 15 August 2003—not S/RES/1267(1999) or S/RES/1373(2001).

131. Norway has implemented mechanisms for authorising access to funds or other assets that were frozen pursuant to S/RES/1267(1999). The Royal Decree refers to the relevant UNSC Section Committee that may grant humanitarian exemptions that have been determined to be necessary for basic expenses, the payment of certain types of fees, expenses and service charges or for extraordinary expenses. Applications for humanitarian exemptions can be submitted to the Ministry of Foreign Affairs. Norway had not yet been confronted with such a request. It is unclear how humanitarian exemptions would apply to property frozen pursuant to S/RES/1373 (2001).

132. Norway has frozen one bank account in accordance with S/RES/1267(1999) and its successor resolutions. This bank account has been frozen since February 2003. It was under the control of one individual. The amount frozen is approximately USD 1 000.

133. ***Freezing action pursuant to S/RES/1373(2001):*** The regime in Norway with respect to United Nations Security Resolution S/RES/1373(2001) is different. Rather then using the enabling Act of 7 June 1968, Norway has chosen to implement S/RES/1373(2001) by enacting a freezing mechanism specifically for terrorist funds/assets within the criminal procedure law (CPA ss.202d to 202g). This legislation facilitates the Norwegian authorities taking swift action in such cases by enabling the chief/deputy chief of the PST, or a public prosecutor to take a freezing decision, without the necessity of going to court, when a person is "with just cause suspected" of committing (or attempting to commit) a terrorist act or terrorist financing offence (as defined in PC ss.147a and 147b). This means that the evidence must establish that the person "more likely than not" committed (or attempted to commit) an offence under sections 147a or 147b. Norway reports that in legal teachings, this standard is often described as being a question of whether something is more than 50% likely. This means that, given the scope of the terrorist financing offence (s.147b), Norwegian authorities can freeze the funds/assets of a person who is considered (more than 50% likely) to have committed (or attempted to commit) one of the following acts: (i) obtaining or collecting funds and assets in respect of the commission of terrorist acts (as defined in s.147a); or (ii) making funds available to terrorists or terrorist organisations. However, because the scope of the terrorist financing offence (s.147b) is not quite broad enough, Norway would be unable to freeze the assets in Norway of person who is considered (more than 50% likely) to have collected funds in the knowledge that they are to be used generally (for any purpose) by a terrorist organisation/individual terrorist. The decision to freeze property must be aimed at specific property which must be identified before the decision can be taken and must be described in the decision to freeze. Under section 202d, the property which may be frozen is any property belonging to: (i) the suspect; (ii) any entity owned by the suspect or over which he has control; or (iii) any person/entity acting on behalf of or at the direction of the suspect/entity owned by the suspect (CPA ss.202d, 147a and 147b).

134. As soon as possible (and not later than seven days after the decision to freeze has been made), the Prosecution Authority must bring the case before a court which will (by order) decide whether the decision shall be affirmed (cf.CPA s.202e). In such cases, the suspect and other persons concerned shall be notified and given an opportunity to express their views. If the circumstances of the investigation necessitate, the court may omit the notice and defer giving information about the order, but shall set a time limit for when information shall be given. Initially, the time limit shall not exceed four weeks, but the court may extend its order by up to four weeks at a time. Once the time limit has expired, the suspect and other persons concerned in the case shall be informed of the order and their right to ask court to decide whether the freezing action shall be affirmed. In this way, freezing actions

taken pursuant to S/RES/1373(2001) are based on a case-by-case assessment made to a "more than 50% likely" standard of proof according to the procedures set out in the CPA.

135. A freezing order based on the CPA shall be terminated without undue delay if the conditions for freezing the assets are no longer fulfilled. At the latest, the freezing shall terminate when the case is decided by a final and binding judgment (CPA s.202f). Persons who have had their assets frozen and other persons concerned have a right to ask a court to decide whether the freezing shall continue (CPA s.202e). Obviously, as such freezing orders are not based on a list, entities cannot request to be de-listed. The court's affirmation of the decision to freeze property must be based on evidence that there is just cause to suspect a person of contravening or attempting to contravene PC ss.147a or 147b. These facts must be proven to the court on the same standard as when the initial decision to freeze is made—a more than 50% likely standard of proof.

136. Lists of designated persons emanating from other jurisdictions (for example, lists made pursuant to EU Regulation 2580 or US-designations) are received by the Ministry of Foreign Affairs which distributes them to the relevant Norwegian agencies. The PST uses the lists for intelligence and law enforcement purposes. There are no mechanisms to ensure that relevant information is guided through government authorities to the financial community, nor are there any communication channels for providing feedback between the government and the financial sector.

137. Norway has never found any funds/assets in the name of anyone designated pursuant to S/RES/1373(2001) inside of Norway. Consequently, Norway has never tried to use the freezing mechanisms under s.202d of the Penal Code.[36] Norway has not issued any guidance to financial institutions and other persons or entities that may be holding targeted funds or other assets concerning their obligations in taking action under freezing mechanisms issued pursuant to S/RES/1373(2001). Nevertheless, Norway reports that ØKOKRIM, New KRIPOS and the PST have improved measures to better apply national procedures for freezing terrorist-related assets, improve co-operation between experts in different fields, and utilise the specialised knowledge of lawyers, accountants, experts in communication technology and investigators working in various sectors of the civil service. For instance, the PST uses the information on such lists as part of the basis for identifying possible terrorist threats to Norway. In such cases, the PST may share the results of its investigations with other appropriate government authorities such as ØKOKRIM. Norway has not created, nor attempted to create, a mechanism that would enable government authorities to build a national list. Unlike the lists issued by the UN Security Council pursuant to S/RES/1267(1999), the lists issued by individual countries pursuant to S/RES/1373(2001) are not automatically given effect to. However, Norway's implementation of S/RES/1373(2001) does allow it to examine and give effect to the actions initiated under the freezing mechanisms of other countries through a procedure of examining each case individually on its merits. Assets that are necessary for the maintenance of the person may not be frozen (CPA s.202d).

138. Norway has not implemented any mechanisms to monitor compliance with freezing mechanisms issued pursuant to s.202d of the Penal Code. However, any person who fails to comply with a legally enforceable freezing order (e.g. an order issued pursuant to s.202d) would be subject to section 343 of the Penal Code. This is a general criminal provision which provides that any person "who acts against a legally imposed prohibition" shall be liable to (unlimited) fines or imprisonment for a term not exceeding four months or both (cf. PC s. 26a). If it is someone other than the suspect himself acting contrary to a freezing action imposed under chapter 15b of the CPA, the maximum penalty is imprisonment for a term not exceeding 2 years (cf. PC s. 132). This provision may, however, only be used when someone intentionally obstruct a public investigation (e.g. by destroying or hiding an object, which may be relevant for the investigation).

[36] It should also be noted that Norway does not participate in the EU Clearing House.

139. ***Freezing actions in contexts other than S/RES/1267(1999) and S/RES/1373(2001):*** Seizing, charging and confiscation laws normally used in other criminal cases can be used to charge, seize and confiscate terrorist funds in contexts other than S/RES/1267(1999) and S/RES/1373(2001). In such situations, the same rules apply as those set out in paragraph 117 of this report, including those relating to the protection of the rights of bona fide third parties.

2.4.2 Recommendations and Comments

140. Norway has implemented measures to freeze terrorist funds and other assets, but the freezing regime in Norway does not fulfil all the elements of Special Recommendation III**.** Concerning implementation of S/RES/1267(1999) and its successor resolutions, an effective freezing regime is absent without a comprehensive set of policies and measures supporting the legal implementation of the bare freezing provisions. Norway relies on existing general provisions to process de-listing and unfreezing requests. However, given the exceptional nature of freezing actions in relation to terrorism with respect to the agencies concerned, the required speed, the rareness and complexity of cases and the unpredictability of problems that raise during the designation, listing, freezing, de-listing and un-freezing process, a clear description of all procedures and possibilities is required. Therefore, Norway is recommended to:

- Establish an effective system for communication among governmental institutions and with the private sector (and the like) to facilitate every aspect of the freezing/unfreezing regime within Norway;
- Provide clear guidance (more than the bare reporting obligation in the MLA) to financial institutions that may hold terrorist funds concerning their responsibilities under the freezing regime;
- Create a procedure for considering de-listing requests and for unfreezing the funds or other assets of de-listed persons.
- Create a procedure for unfreezing, in a timely manner, the funds/assets of persons inadvertently affected by the freezing mechanism upon verification that the person is not a designated person.
- Clarify the procedure for authorising access to funds/assets that are frozen and that are determined to be necessary on humanitarian grounds in a manner consistent with S/RES/1452(2002);
- Create an appropriate procedure for a judicial review of freezing actions.

141. The effectiveness of Norway's freezing regime with respect to S/RES/1267(1999) is reduced by the absence of any policy and procedures to handle freezing cases.

142. The implementation of S/RES/1373(2001) through CPA s.202d and 202e enables authorities to freeze terrorist funds, in cases where a link with an act of terrorism financing can be proven to be more than 50% likely.

143. In relation to freezing actions taken pursuant to S/RES/1373(2001), it is recommended that Norway: (i) ensure that it can freeze the assets in Norway of a person who is considered (more than 50% likely) to have collected funds in the knowledge that they are to be used generally (for any purpose) by a terrorist organisation/individual terrorist; (ii) ensure that there are appropriate mechanisms in place to ensure that relevant information is guided through government authorities to the financial community; and (iii) create clear communication channels for providing feedback between the government and financial sector.

144. Norway should also give clear practical guidance to financial institutions concerning how to implement freezing actions under S/RES/1267(1999) or S/RES/1373(2001). It is also recommended that Norway enact measures that would allow for the possibility of freezing funds or other assets where the suspect belongs to a terrorist organisation or is known to finance such organizations or terrorists in general

(even if the financing cannot be connected to an act of terrorism). It should also have measures in place to monitor compliance with both S/RES/1267(1999) and S/RES/1373(2001).

145. Freezing orders in the context of terrorist financing may raise sensitive issues, particularly concerning human rights. However, proper implementation of both S/RES/1373(2001) and Special Recommendation III can be achieved (as has been achieved by countries with legal systems similar to Norway's) while still meeting international obligations concerning the respect for human rights and the fight against terrorism. The underlying rationale for S/RES/1373(2001) and SR III is to implement measures that are both of a preventive and deterrent nature; however, this approach is lacking in the Norwegian system. Certainly it is not apparent why Norway should not implement S/RES/1373(2001) in the same manner as for S/RES/1267(1999) and S/RES/1333(2000), but of course with additional safeguards built in. For the reasons above, Norway has not implemented S/RES/1373(2001) fully in accordance with the FATF standards. Therefore, it is recommended that Norway amends its laws to fully implement S/RES/1373(2001) consistent with its aims and objectives, preferably in a similar way as S/RES/1267(1999) has been implemented. This would create one single system for designating, listing, freezing, de-listing and de-freezing of terrorist assets.

2.4.3 Compliance with Special Recommendation III

	Rating	Summary of factors underlying rating
SR.III	PC	• Norway has not implemented measures to monitor compliance with the 1968 Act and Regulations (S/RES/1267(1999) or freezing mechanisms issued pursuant to s.202d of the Penal Code (S/RES/1373(2001). • The freezing action pursuant to S/RES/1267(1999) can be legally challenged by the entity frozen; however, the Norwegian authorities could not point at clear gateways for such action. Rather it is assumed that the entity frozen will use the same legal mechanisms that any citizen has at its disposal to challenge governmental decisions. • Norway has issued some guidance to financial institutions and other persons/entities that may be holding targeted funds/assets; however, this guidance focuses more on how the FSA processes such lists, rather than giving guidance to financial institutions as to how they should meet their obligations concerning freezing orders issued pursuant to S/RES/1267(1999). • It is unclear how humanitarian exemptions would apply to property frozen pursuant to S/RES/1373 (2001). • Because the scope of the terrorist financing offence is not quite broad enough, Norway would be unable to freeze the assets in Norway of a person who is considered (more than 50% likely) to have collected funds in the knowledge that they are to be used generally (for any purpose) by a terrorist organisation/individual terrorist. • There are no other mechanisms to ensure that relevant information is guided through government authorities to the financial community, nor are there any communication channels for providing feedback between the government and the financial sector. • Norway has not issued any guidance to financial institutions and other persons or entities that may be holding targeted funds or other assets concerning their obligations in taking action under freezing mechanisms issued pursuant to S/RES/1373(2001).

Authorities

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

2.5.1 Description and Analysis

146. ***Recommendation 26:*** The Norwegian FIU is the Money Laundering Unit (MLU) which is located at the ØKOKRIM. It is responsible for receiving, analysing and disseminating information transmitted by the institutions and professionals referred to in the Money Laundering Act. It is also responsible for:

(a) Co-operating with the institutions and individuals referred to in the Money Laundering Act;

(b) Co-operating with local and foreign police and foreign FIUs;

(c) Being the responsible body concerning the Council of Europe Convention of 1990;

(d) Participating at an international level in forums such as the FATF, the Egmont Group, Interpol, Europol and the Baltic Sea Task Force; and

(e) Developing competence in the area of AML/CFT, including working to improve the knowledge and expertise of the police in general and other relevant groups.

147. Pursuant to the MLA, if an entity that has a reporting obligation suspects that a transaction is associated with the proceeds of crime or a violation of sections 147a or 147b of the Penal Code (the terrorism and terrorist financing provisions), it is bound to make further inquiry into the matter and (if this does not dispel the suspicion) make an STR to the MLU. Until the MLU is informed, the entity is not to carry out the transaction unless not doing so is impossible or would impede the case. However, in most cases, reporting FIs proceed with transactions before contacting the MLU. They only contact the MLU for clearance before proceeding with the transaction if they want ØKOKRIM to use its freezing powers. Although the MLU is empowered to require the entity not to carry out the transaction (MLA s.9), Norway has informed the assessors that this power is rarely exercised. The MLU could not give a general indication as to the period that normally elapses between the date of a suspicious transaction and the date the related STR is entered into the database of the MLU. However, the MLU indicated that the STRs received often concern transactions that took place quite a long period previously (in spite of the fact that section 9 of the MLA, as a general rule, prohibits reporting institutions from carrying out suspicious transactions before reporting them to the MLU).

148. The MLU does provide reporting entities with some guidance and practical assistance concerning the manner of reporting, the specification of reporting forms and the procedures that should be followed when reporting. The MLU is manned throughout working hours and can be contacted by telephone for guidance on the money laundering legislation or if the caller is aware of a suspicious transaction which may need to be reported (Circular 9/2004 s.2.11).

149. STRs must be submitted to the MLU in a standardised form (Money Laundering Regulations (MLR) s.11). This form (which does not make any distinction between ML/FT) is publicly available on ØKOKRIM's website. The MLR contain guidelines about the kind of information that (so far as possible) should be contained in an STR. The FSA has also issued guidelines on section 11 which contain even more detailed information regarding the manner of reporting, including specification of the reporting forms, and the procedures that should be followed when reporting (FSA Circular 9/2004 dated 15 April 2004 (Circular 9/2004)). STRs must be sent to the MLU by post, fax or in a machine-readable form. STRs from banks and other reporting institutions (except MVTS providers) are received by fax. There is only one institution in Norway that is legally authorised to provide MVTS—an EU branch of a bank. The current MVTS provider started operations in February 2004. Before that, a different institution (which stopped these operations in December 2004) was providing the same services. STRs from the new MVTS provider are provided to the MLU in a spreadsheet format stored on discs. These STRs are then extracted from the spreadsheet and entered into the database of STRs. This was done on the basis of the same arrangements that existed between the MLU and the old MVTS provider.

150. Upon receiving an STR in the standardised form, the information contained therein is manually input in a computer database that has been specifically designed for such information. The MLU's administrative staff perform this task. The information contained in an STR form is usually entered into the database on the same day it is received or the day after. The MLU then conducts further analysis of the STR to rebut or confirm the suspicion of ML/FT activities. When a new STR has been entered into the database, the MLU conducts an initial examination of the STR database and a selection of other databases to rebut or confirm the reported suspicion of ML/ FT activities. Based on

this initial examination, a decision is made whether to delete the STR in accordance with section 10 of the MLA (which requires deletion of an STR if the suspicion is rebutted or after five years unless new information relating to the person involved is received) or to keep it in the MLU's STR database. This initial examination also helps the MLU's investigators to select STRs for further examination and possible referral for investigation.

151. The MLU has direct access to a wide range of databases and registers, including all police registers, official public registers (such as the Register of Business Enterprises (Business Register)), official registers for Government use (such as the Population Register) and commercial databases (such as credit bureaus) in order to add to the information compiled in respect of STRs. Credit bureau information in Norway contains certain tax related information such as declared income, declared wealth and declared debt in addition to the normal credit related information. According to the new Currency Register Act, the MLU also has direct access to Currency Transaction Register—albeit only once an investigation has begun. Access to the Currency Transaction Register will give the MLU access to information about cross border cash transports, and transfers of money to and from bank accounts abroad. Additionally, the MLU can obtain additional information from the local police or a foreign FIU (within limits set by the professional secrecy).[37]

152. The processing of STRs in the MLU's database is managed by means of an electronic case management system that allows the MLU staff to keep track of actions taken within the MLU in relation to each STR (such as the information pertaining to a particular STR which is added to the database, the number of databases searched in relation to each STR and whether previous STRs relating to the same persons or entities had been filed with the MLU). However, technical limitations prevent the MLU staff from applying analytical tools directly to all of the information in the database, forcing them to extract a selection of STRs to another system where the analytical tools can be applied. As a result any analysis of STR information which the MLU staff might do, is restricted to the selected extract only and is done without the benefit of allowing the analytical tools to search through the entire STR database. If necessary, the MLU can demand additional information/documentation from reporting entities (MLA s.7). However, at the examination stage (before an investigation is instituted), the MLU has no power to ask other reporting entities whether they have had transactions with a person who is the subject of an STR, or to demand additional information/documentation from them. It can only do so from the entity that sent the STR. This impacts negatively on the effectiveness of the system.

153. If the MLU determines that concrete details support the suspicion of ML/FT, a criminal investigation may be initiated. The MLU's decision to refer information (on the basis of which a new investigation may be initiated) amounts to the opening of a criminal investigation and must therefore be based on reasonable grounds to believe that an offence has been committed (CPA s.224). In such cases, the MLU may submit the case to the investigators of a police district or to an investigation team at ØKOKRIM. After that, the MLU does not know what happens to the cases that are reported. The MLU has made several attempts to introduce routines in the Police to report back to it and has tried to follow up on each individual case. However, as the number of cases has increased, this has become very time consuming, and in many cases impossible. In the case of ØKOKRIM, when a criminal case is opened and ØKOKRIM's management decides to assign it to one of its special teams for further investigation, the teams will be committed to following up the case until there is a final indictment and eventual sentence. However, if the MLU sends the criminal case to a police district, the case will be handled as any other complaint given to the police. The police district is not obliged to follow up the case and it is up to them to decide whether the case should be dropped or not. Alternatively, the MLU may refer the case to the PST if the suspicion involves possible terrorist financing. Both the investigation and criminal proceedings are carried out in accordance with the Criminal Procedure Act. Alternatively, the MLU may decide to submit the case to a foreign FIU. Information may also be

[37] See Annex 16 for an overview of the registers in Norway, including a description and details of who has access to them.

disseminated to other authorities when there are reasonable grounds to suspect ML/TF, and for the purpose of rebutting or confirming the MLU's suspicions, on the condition that it only be used to respond to the MLU's inquiries. The MLU's investigators perform all necessary inquiries on an independent basis. However, the decision on whether or not to open criminal proceedings is taken in consultation with the department's responsible prosecutor who is also the head of the MLU. No information is distributed to other law enforcement bodies without analysis. However, overall, the impression is that much of the information from the STRs is distributed to other law enforcement bodies without sufficient analysis. This is because the MLU has insufficient resources to handle the STRs that it receives. However, the Norwegian authorities expect that the situation will be improved when new technological equipment is in place.

154. If a suspicion of ML/FT is rebutted, all information about the transaction and the STR itself must be deleted immediately (MLA s.10). If the suspicion can be neither rebutted nor confirmed, the STR is filed for intelligence. After five years, all information about the transaction must be deleted if no further information of importance is registered, and no investigation or legal measures initiated against the legal or natural person. On the other hand, if new information of importance is registered, a new five-year deadline shall apply from the date of registration (MLA s.10). The MLU places a strong emphasis on the protection of privacy. The information contained in its database can only be accessed by the MLU staff, the Proceeds of Crime team at ØKOKRIM and authorised persons (such as the head of ØKOKRIM). The MLU's work is largely governed by internal guidelines that are intended to ensure prudent and secure handling of STRs. For instance, the MLU must destroy/delete all the information that has been registered (including the STR itself) if the suspicion is rebutted at the stage of the initial examination of an STR (MLA s.10). The following chart sets out how the MLU processed the STRs that it received.

PROCESSING OF STRs				
	2001	2002	2003	2004
Number of reports received	992	1 291	3 459	6 082
Number of decisions	911	1 282	3 482	6 202
Cases (examination) initiated by ØKOKRIM	64	84	97	49
New cases (investigation) referred to ØKOKRIM	15	7	4	11
New cases (investigation) referred to police districts	63	39	23	77
New cases referred abroad	1	1	1	0
Used in criminal case handled by ØKOKRIM	4	2	7	30
Used in criminal case in other police district	41	57	50	94
Cases deleted – suspicion proven to be unfounded	7	17	2	21
Filed for intelligence	716	1 075	3 298	5 910
Decisions by the prosecutor	155	117	92	45
Court decisions	29	56	28	10
Deleted according to law (after 5 years)	140	618	764	713

155. The MLU is subject to the oversight of the Control Committee; however, this oversight only extends to the protection of privacy and personal data. The Control Committee is an independent body that was established in 1995 following express instructions from the legislature. The Control Committee's composition and responsibilities are set out in section 14 of the MLA. The Control Committee reports to the Ministry of Finance. It is currently chaired by a judge and is comprised of representatives from the Norwegian Financial Services Association (FNH), the Employers Association of the Norwegian Finance Sector and the Norwegian Bar Association. The Control Committee is entitled to access any of the MLU's information, documents or other material that it deems necessary,

upon request and without regard to the duty of secrecy. However, the Control Committee is not allowed to access information relating to the investigation of particular STRs once a criminal case has been opened in relation to it. The Control Committee oversees the processing of STRs[38] and, in doing so, emphasises the importance of legal protection and the protection of privacy.[39] In theory, the Control Committee could interfere with the MLU's independence, particularly with regards to the exercise of its discretion on the decision to delete records pursuant to section 10 of the MLA; however, in practice, this does not seem to have occurred.

156. The Control Committee reports having good relations with the MLU and considers that, in general, the MLU performs its functions very well and without systematic mistakes. To date, the Control Committee has not seriously disagreed with the MLU's decisions on the handling of reports. However, even if such a situation were to arise, the Control Committee does not have the authority to take direct corrective action. It can take indirect action at the ministerial level or through the FSA. For instance, the Control Committee could express its concerns in a letter or in its annual report to the Minister of Finance who would then consider further steps. The Control Committee can also send information to the FSA or the Ministry of Finance if, through its supervision, it finds that a reporting entity has not fulfilled its reporting obligations (Regulation No.557 of 14 June 1995 s.6), presumably, address those concerns to the Minister of Justice & Police (who is ultimately responsible for the MLU). Nevertheless, although the Control Committee has no legal powers to interfere with the MLU, it is evident that the MLU takes the Control Committee's recommendations very seriously.

157. When the scope of the MLA was extended in 2003 (coming into force on 1 January 2004) to include additional reporting entities, the government expected that the MLU's resources would need to be increased. The issue was addressed in the white paper on the Money Laundering Act (Ot.prp. nr. 72 (2002-2003) paragraph 14.2). Organisationally, the MLU's budget is part of ØKOKRIM's total budget. Pursuant to the ordinary national procedure regarding budgeting, each local chief of police and head of central institutions is responsible for handling the internal budget. Resources made available to these bodies must be used in accordance with the principal priorities and guidelines set out in budgetary documents issued by the government and Parliament.

158. Police and prosecutors have a duty of professional secrecy (Police Act s.24; PAA s.13) which applies until a criminal case is opened (i.e. after an investigation has formally been initiated) (CPA s.61). However, this duty does not prevent the MLU's employees from providing information to, or gathering information from, other public officials in the police and Prosecution Authority, or from co-operating with foreign police or competent authorities, provided that the purpose of the exchange of information is to prevent or uncover violations (CPA s.61c).

159. The MLU has been a member of the Egmont Group since 1995. Each year, several staff members participate in meetings and seminars of the Egmont Group. The MLU also engages in frequent information exchange via the Egmont Group's own Secure Web System. As an Egmont member, the MLU is aware of the Egmont Group Statement of Purpose and its Principles for Information Exchange Between Financial Intelligence Units for Money Laundering Cases (Egmont Principles for Information Exchange). However, in practice, the MLU does not follow all of these guidelines. For instance, the Egmont Principles for Information Exchange suggest that, if a request has not been processed within one month, the requested FIU should give an indication (either orally or in writing) of when it will be in a position to respond or if it is experiencing any particular difficulties in responding. However, when the MLU's computer systems related to the Egmont Secure Web crashed, and were out of function for three months, in 2004 and it lost several requests for assistance

[38] The assessment team was advised that Norway is considering implementing a National Intelligence Register that could incorporate the MLU's database of STR information. It is possible that this could raise some issues concerning the secure protection and dissemination of the information held by the MLU.

[39] Regulation of 14 June 1995, No. 557 on the Control Committee for Measures to Combat Money Laundering (the Control Committee Regulations) s.2.

from foreign FIUs that were received in the first half of 2004—the MLU did not attempt to contact its foreign counterparts to advise them that any requests could not be processed because requests themselves had been lost. Obviously, since the requests were missing, the MLU did not even know which foreign FIUs had made requests; however, it could have sent out a general notification through the Egmont Group's Secure Web System advising everyone of the problem. That way any foreign counterpart that was affected could resend their requests. Nevertheless, the MLU's ability to co-operate both domestically and internationally was improved by repealing the strict confidentiality provision that existed in the previous legislation (Financial Services Act (FS Act), s.2-17). Now, the MLU can exchange information with foreign FIUs, spontaneously and upon request, regardless of whether the FIU is organised within the police or prosecution authority or within the administration.

160. ***Recommendation 30 (Structure and resources of the FIU):*** The MLU is located at ØKOKRIM, which is a unit within both the police and the prosecution authority. Norway reports that this location for the MLU provides a good basis for initiating investigation of cases involving an STR or that are based on STRs. Cases may be referred to the local police or other teams at ØKOKRIM. The MLU can also gather further information from both police sources and administrative sources in order to decide whether to open criminal proceedings.

161. Since the MLU was created in 1993, it has had 6 leaders and different organisational models have been tried. The MLU has been at ØKOKRIM since its inception. Chief State Prosecutors have headed most of the teams at ØKOKRIM. However, since 2003, the MLU has been under the leadership of a police prosecutor. Until 1999, it was a separate unit responsible for receiving and disseminating STRs. In 2000-2001, the MLU was part of a larger unit called the Money Laundering and Intelligence Unit which had 19 staff in 2000 and 18⅓ in 2001. During this period, the Confiscation team was integrated in the MLU. This model was dropped in 2002 and the larger unit was divided into two parts—the Assets Confiscation Team and the Money Laundering Team. In 2004, a new model was under development. A new team with responsibility for analysing trends etcetera was created and MLU staff were transferred to the new unit. In 2002-2003, a working group appointed by the Police Directorate considered the organisation of the special agencies of the police (including ØKOKRIM) and proposed that the MLU should be moved from ØKOKRIM to KRIPOS. However, the government did not agree, and the conclusion (rendered in spring 2004) was that it should continue as a unit within ØKOKRIM.

162. In December 2003, the MLU had 9⅓ employees and a liaison officer from the Customs Directorate. In 2004, the MLU had the opportunity to add 4 new employees—bringing it to a total of 13½ staff in the course of the year. The unit is multidisciplinary and was to consist of police prosecutors, legal advisers, police investigators, investigators with economic background (i.e. auditors), administrative staff, and other advisors. As at January 2005, the team has 11½ employees, consisting of police investigators, investigators with economic background and administrative staff — only seven of which are directly involved in analysing STRs. This number of staff is inadequate to deal with the volume of STRs that the MLU currently receives. In addition, much of the MLU's activities are based on inefficient manual processes. For instance, the MLU does not accept STRs electronically; most are submitted either by fax, post or in person (though some are provided on a computer disc), after which the MLU staff must manually input the STRs into their system—even though most representatives from the private sector that met with the assessors indicated a strong desire and the current technical capability to submit reports electronically. However, this situation is expected to change in the near future. The Norwegian authorities have committed to implementing a system whereby reporting entities will be able to submit their reports to the MLU electronically. Budgetary resources have already been earmarked and dedicated to this purpose, and the MLU is currently in the process of examining the best system to meet its needs. These steps will certainly increase the effectiveness of how the MLU receives reports. However, until other technological issues are addressed, this may create even greater problems in the short term. With introduction of an electronic reporting system, Norwegian authorities anticipate that the number of STRs filed will increase dramatically. However, because much of the MLU's analytical processes are handled manually (only two of the MLU's staff are trained in the use of Analysts Notebook) and, with its

current systems, there is no possibility for the system to automatically draw connections between STRs) The MLU can only work on a few of the STRs that it receives; the rest are simply filed away for future reference. Manual analysis is done, but is often dependent upon the MLU staff remembering a person's name or a previous STR. Under these conditions, the MLU staff should be commended for the results that they have achieved; however, this process is clearly very inefficient. The MLU is already understaffed to handle the STRs that it currently receives. Unless it receives proper tools and resources to conduct effective electronic analysis, it will be swamped with STRs that it is unable to effectively process.

163. The MLU is connected to, and a frequent user of, the Egmont Group's secure web; however, it is not linked to FIU.net. Although a connection to FIU.net would certainly lead to a better exchange of information, no funds are allocated for this purpose. Because establishing the connection would require a considerable economic investment, the issue must be determined on a political level. However, because the MLU is currently in the process of establishing a system for receiving STRs electronically (the ELMO project), it is of the view that the question of whether to connect with FIU.net should be assessed after the ELMO project has been completely developed and is in use.

164. The MLU currently does not have its own budget. As a unit within ØKOKRIM, it is dependent on the ØKOKRIM budget. Because the MLU budget is not separate, there is some concern that ØKOKRIM takes resources from the MLU. For instance, the assessors are aware of one instance in which a staff member originally destined for the MLU was deployed to another division within ØKOKRIM. ØKOKRIM's budgets since the last evaluation of Norway are set out in the chart below.[40] The budget increases in 2004 were the result of the Parliament's decision that the MLU needed four more staff to deal with the expectation of receiving more STRs when the new MLA entered into force.

BUDGET OF ØKOKRIM	
YEAR	TOTAL ANNUAL BUDGET
1999	NOK 64.7 million (EUR 7.8 million/USD 10.2 million)
2000	NOK 70.5 million (EUR 8.5 million/USD 11.1 million)
2001	NOK 79.4 million (EUR 9.6 million/USD 12.6 million)
2002	NOK 103.8 million (EUR 12.6 million/USD 16.4 million)
2003	NOK 118.1 million (EUR 14.3 million/USD 18.7 million)
2004	NOK 102.1 million (EUR 12.4 million/USD 16.1 million)

165. The MLU has designated a special investigator whose responsibility is terrorist financing. STRs that are received by the MLU are assessed, and then assigned to the special investigator if the STR is believed to have something to do with terrorist financing. Such STRs are examined so far as the available resources allow for. The MLU also focuses on possible trading with merchandise that could be related to weapons of mass destruction.

166. High staff turnover at the MLU has caused some difficulties in maintaining effective relationships with reporting entities, and providing reliable statistics. For example, when a new MVTS provider started operations in Norway in February 2004, the MLU assigned a person to be responsible for advising it of its reporting obligations. Because it was anticipated that the MVTS provider would file a large number of STRs, the MLU's representative was to arrange for it to file its STRs on a disc rather than by fax. This was intended to avoid the MLU having to use a great deal of resources entering the data manually into its systems. Unfortunately, the MLU staff member who was assigned these responsibilities quit. Since then, the MLU has had difficulty in constructing what happened

[40] The high budgetary level in 2003 and partly in 2002 was due to investments in the PCCC.

with the relationship between the MLU and the MVTS provider. At the time of the on-site visit, the MLU did not know why the MVTS provider has only sent one disc containing about 75-80 transactions to the MLU since commencing business operations in Norway. The MLU has informally expressed its concern to the FSA about the MVTS provider's lack of reporting and, since the on-site visit, the FSA has taken action to correct this problem.

167. ***Recommendation 32 (Regular review of AML/CFT systems):*** Norway conducted comprehensive reviews of its AML system in the Action Plan 2000 and the Action Plan 2004 (which also contained some reference to CFT measures). These regular reviews are quite thorough and frank concerning the weaknesses and shortcomings of the Norwegian system. Some of the measures described in the Action Plan 2004 have already been implemented. The main purpose of the Action Plan 2004 is that of a policy paper, seeing as it does not provide for budgets and recourses and has no described implementation procedure. Some of the plan's intentions are rather vague, necessitating extensive negotiations between authorities in order to effectively work out and implement its aims. However, the EMØK is mandated to oversee the implementation of the Action Plan 2004. This includes determining what budgetary resources will be necessary to implement the plan's measures, and making annual budget proposals to the government in that regard.

168. ***Recommendation 32 (Statistics collected by the FIU):*** The MLU maintains the following statistics relating to suspicious transaction reports:

(a) The number of STRs received by the FIU;

(b) A breakdown of the type of financial institution or business/professional making the STR;

(c) A breakdown of the STRs that were analysed/disseminated, including those that resulted in indictments, judicial decisions or deletions (according to the MLA's 5-year deletion rule);

(c) A breakdown of the number of natural and legal persons represented in the STRs;

(d) A breakdown of the amount of domestic and foreign currency involved in the STRs;

(e) The type of transactions involved in the STRs, including the number of transactions related to travellers cheque or foreign currency cheques, and international money transfers;

(f) Reports filed on the cross-border transportation of currency and bearer negotiable instruments;

(g) Formal requests for assistance made or received by the FIU; and

(h) Spontaneous referrals made by the FIU to foreign authorities.

169. Additionally, the MLU collects statistics concerning the ethnicity and citizenship of persons represented in STRs and the size of transactions involved in the STRs. Unfortunately, not all of the statistics collected by the MLU are reliable. In 2004, due to some technical failures with respect to connectivity with the Egmont Secure Web System, the MLU had to replace some computer hardware. This led to a loss of data relating to requests from foreign FIUs, including its statistics relating to formal requests for assistance made or received by the MLU, and spontaneous referrals made by the MLU to foreign authorities. As a result, the system for connecting to the Egmont Secure Web System was itself was down for some 3 months. The inadequacy of the MLU's statistics collection mechanisms (i.e. its computer systems) has thus impeded its statistics collection capabilities.[41]

[41] The Central Bank *(Norges Bank)* kept statistics concerning the number of reports filed on cross-border transactions of currency and bearer negotiable instruments when it was responsible for maintaining the BRAVO Register. The new Currency Transaction Register which replaces the BRAVO Register will have the ability to collect similar statistics, and will be handled by the Customs Directorate. As of 1 January 2005, all police districts have access to the new Currency Transaction Register.

2.5.2 Recommendations and Comments

170. Although, on paper, the MLU generally meets the requirements of Recommendation 26, its lack of effectiveness causes concerns and impedes the overall effectiveness of Norway's AML/CFT system. The MLU is understaffed under-resourced and technologically ill-equipped. Given the paucity of the MLU's resources, it is a credit to its staff that it is generating as many results as it is. However, those results are not adequate given the size of Norway's financial sector and the number of STRs being received. It is recommended that Norway allocate more staff, budget and technological resources to the MLU as soon as possible. In particular, the MLU needs better technology. Although the staff are very professional and highly trained, all staff need to be trained in the use of analytical tools such as Analysts Notebook. In addition to a system for electronic reporting, the MLU urgently needs tools to conduct electronic analysis as soon as possible.

171. It is recommended that Norway remove the twin rules of deleting STR information not acted on within 5 years and STR information where the suspicion has been rebutted. While the desire to protect the privacy of information is understandable, to insist that such STR information be deleted may deprive the MLU of a potential source of information that may be exceedingly useful for its work, and inhibit the effectiveness of the MLU's work. For instance, a transaction that can be satisfactorily explained away (so that suspicion is rebutted) may nonetheless give rise to other inferences if considered together with previous similar transactions as part of a pattern. Yet if the law requires such the STR to be deleted forthwith, it would be impossible to detect the pattern. Requiring automatic deletion after a lapse of 5 years may also be counter-productive to the AML effort since an astute criminal might simply choose to launder money through transactions spaced 5 years apart. Since the data transmitted to the MLU is subjected to extensive protective measures designed to prevent their misuse, the assessors are of the view that to require information to be deleted from the MLU database does not go any further to safeguard the interest of privacy. Furthermore, it is understood that the decision to delete is made by individual officers in the MLU, and there is no practice for the decision to have to be seconded or approved by another officer. Given that deletion would remove all trace of the transaction (including the grounds for deciding to delete), the risk of an erroneous deletion cannot be overstated. The Control Committee's intervention has also impacted on the overall effectiveness of the MLU in that a disproportionate amount of the MLU's very limited resources are now expended towards considering whether to delete or justify retaining old STR files.

172. Moreover, the joint involvement of the Ministry of Finance (through the Control Committee) and the Ministry of Justice & Police (as the ministry directly responsible for the MLU's operation and budget) may result in an unfocused and fragmented approach to the MLU's development. For instance, the Control Committee is aware that reporting by MVTS providers will dramatically increase the MLU's workload (and, in fact, has already done so) to an extent that will be difficult for the MLU to manage given its current level of resources. However, to date, the Control Committee has not formally recommended that the MLU's budget and technical resources be increased because the mandate of the Control Committee does not cover such matters. Nor does the government's Action Plan 2004 emphasise this as a priority. Consequently, although there seems to be widespread recognition that the MLU's resources are inadequate, no additional budgetary resources have been dedicated to it.

173. The management and resources of the MLU currently are not ring-fenced. It is recommended that Norway ring-fence the responsibility and resources of the MLU. Norway should also improve the MLU's statistics collection capabilities by providing it with better technological tools.

174. The Police Directorate is planning for a new national intelligence system which makes it possible to search for information in all the police databases from one platform to gather all information in one database in order to co-ordinate and facilitate searches for information. There is now a discussion at the Police Directorate to link and match this register with the information from

STRs. Norway should ensure that this initiative does not negatively impact the MLU's ability to securely protect and disseminate STR information only in accordance with the law.

2.5.3 Compliance with Recommendations 26, 30 & 32

	Rating	Summary of factors relevant to s.2.5 underlying overall rating
R.26	PC	• Although, on paper, the MLU generally meets the requirements of Recommendation 26, its lack of effectiveness causes concerns and impedes the overall effectiveness of Norway's AML/CFT system. • Technical limitations prevent the MLU staff to apply analytical tools directly to all of the information in the database, forcing them to extract a selection of STRs to another system where the analytical tools can be applied. As a result any analysis of STR information which the MLU staff might do, is restricted to the selected extract only and is done without the benefit of allowing the analytical tools to search through the entire STR database. • Overall, the impression is that much of the information from the STRs is distributed to other law enforcement bodies without sufficient analysis. This is because the MLU has insufficient resources to handle the STRs that it receives. • In theory, the Control Committee could interfere with the MLU's independence, particularly with regards to the exercise of its discretion on the decision to delete records pursuant to section 10 of the MLA; however, in practice, this does not seem to have occurred. At a minimum, the Control Committee's intervention has impacted on the overall effectiveness of the MLU in that a disproportionate amount of the MLU's very limited resources are now expended towards considering whether to delete or justify retaining old STR files. • As an Egmont member, the MLU is aware of the Egmont Group Statement of Purpose and its Principles for Information Exchange Between Financial Intelligence Units for Money Laundering Cases (Egmont Principles for Information Exchange). However, in practice, the MLU does not follow all of these guidelines. • While the desire to protect the privacy of information is understandable, to insist that such STR information be deleted may deprive the MLU of a potential source of information that may be exceedingly useful for its work, and inhibit the effectiveness of the MLU's work.
R.30	PC[42]	• The number of staff is inadequate to deal with the volume of STRs that the MLU currently receives because much of the MLU's activities are based on inefficient manual processes. For instance, the MLU does not accept STRs electronically; most are submitted either by fax, post or in person (though some are provided on a computer disc), after which the MLU staff must manually input the STRs into their system—even though most representatives from the private sector that met with the assessors indicated a strong desire and the current technical capability to submit reports electronically. • Much of the MLU's analytical processes are handled manually and, with its current systems, there is no possibility for the system to automatically draw connections between STRs. • The MLU can only work on a few of the STRs that it receives; the rest are simply filed away for future reference. Manual analysis is done, but is often dependent upon the MLU staff remembering a person's name or a previous STR. This process is clearly very inefficient. • The management and resources of the MLU currently are not ring-fenced. • High staff turnover at the MLU has caused some difficulties in maintaining effective relationships with reporting entities. • Only two of the MLU's staff are trained in the use of Analysts Notebook. • The joint involvement of the Ministry of Finance (through the Control Committee) and the Ministry of Justice & Police (as the ministry directly responsible for the MLU's operation and budget) may result in an unfocused and fragmented approach to the MLU's development. Consequently, although there seems to be widespread recognition that the MLU's resources are inadequate. Although additional budgetary resources have been dedicated to ØKOKRIM to address these issues, the assessment team remains of the view that these resources are still inadequate.

[42] This is an overall rating for compliance with Recommendation 30, based on the assessments in sections 2.5, 2.6 and 3.10 of this report.

R.32	PC[43]	• Not all of the statistics collected by the MLU are reliable. In 2004, due to some technical failures with respect to connectivity with the Egmont Secure Web System, the MLU had to replace some computer hardware. This led to a loos of data relating to requests from foreign FIUs, including its statistics relating to formal requests for assistance made or received by the MLU, and spontaneous referrals made by the MLU to foreign authorities. The inadequacy of the MLU's statistics collection mechanisms (i.e. its computer systems) has thus impeded its statistics collection capabilities.

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

175. Norway has created a comprehensive network of law enforcement and prosecutions authorities who have been designated responsibility for investigating money laundering and terrorist financing matters. The Director General of Public Prosecutions (DGPP) is responsible for ensuring that ML/FT offences are properly investigated and prosecuted, and decides who should have main responsibility for an investigation.

176. ØKOKRIM is a permanent unit that is specialised in investigating complicated economic crime, including crime related to money laundering. ØKOKRIM chooses its own economic crime cases, undertaking only about 40 investigations per year (relative to the 6 000 STRs received annually on a whole range of crimes). A multidisciplinary, specialised Assets Confiscation team is also located there, as is the MLU.

177. Money laundering offences and confiscation cases are investigated by the police under the instruction of the Prosecution Authority in the police district where the offence was committed. The local police may request that ØKOKRIM take over the investigation of complicated/large cases, or may seek its assistance in the investigation. Any team at ØKOKRIM (including the Assets Confiscation Team or the Assistance Team) may provide such assistance. Additionally, each police district in Norway shall establish separate teams to combat economic crime by 1 July 2005 (Action Plan 2004). The local police do not investigate terrorist financing cases. Such cases are under the responsibility of the PST. However, to the extent that financial investigation is required, ØKOKRIM may also be involved in the investigation. Additionally, the Prosecution Authority may decide to waive the arrest of suspected persons and/or seize money for the purpose of identifying persons who are involved in such activities or for evidence gathering.

178. *Additional elements:* Norway has also implemented many other elements that go farther and which greatly enhance its ability to investigate money laundering and terrorist financing. For instance, Norway participates in co-operative investigations with foreign competent authorities (particularly the Nordic countries) in drug and human trafficking cases. Additionally, Norway has legislative measures in place that provide law enforcement with an extensive range of specialised investigative techniques when conducting ML/FT or other criminal investigations, including: (i) secret search (CPA s.200a); (ii) video surveillance and technological tracking (CPA chapter 15a); (iii) concealed video surveillance of a public place (CPA s.202a); (iv) technological tracking when a person with just cause suspected of an act or attempt of an act punishable by imprisonment for five years or more (CPA s.202b); and (v) break-in for the purpose of placing a technical direction finder, or placing such finders in clothes or bags that the suspect wears or carries, when a person with just cause is suspected of an act or attempt at an act punishable for 10 years or more (CPA s.202c). However, these techniques can only be used

[43] This is an overall rating for compliance with Recommendation 32, based on the assessments in sections 2.5, 2.6, 3.13, 6.3, 6.4 and 6.5 of this report.

for serious offences (where the maximum penalty is 5 or 10 years imprisonment). The exception is video surveillance which can be used when there is just cause to suspect that criminal act(s) punishable by a term exceeding six months have been committed (CPA s.202a). In the context of money laundering, this would limit their availability to cases of aggravated or drug-related money laundering. Other coercive measures, such as infiltration (undercover) operations and provocation (i.e. instigating an offence by, for instance, asking someone if they will sell you drugs) are also available; however, these measures are not statutorily regulated. Provocation, for instance, can only be used for intelligence purposes. The Norwegian government is currently studying proposals made by a government-appointed commission to statutorily regulate undercover operations and provocation.

Recommendation 28

179. ***Production orders:*** The competent authorities responsible for investigating ML, FT and other underlying predicate offences have the power to compel production of *objects* that are deemed to be significant as evidence if the possessor is obliged to testify in the case. The word *objects* means movable property, including documents, electronically stored information and financial information that is held or maintained by financial institutions and other businesses or persons (i.e. transaction records, identification data obtained through the customer due diligence (CDD) process, account files and business correspondence, and other records, documents or information) (CPA s.210). To obtain a production order, the Prosecution Authority must submit a petition for a production order to a court. The court may grant the petition without prior notice to the charged person or the financial institution. Under pressing circumstances, the Prosecution Authority may compel the information directly, and then submit the case to court as soon as possible for a subsequent approval (CPA s.210). The charged person shall be notified when information has been compelled; however, notification may be postponed if there is suspicion of a criminal act that is punishable by more than six months imprisonment (provided that the postponement is strictly necessary for the investigation of the case) (CPA s.210a). Production orders can be used to obtain historical data (CPA ss.210 and 210a) or future information that has not yet been obtained by the financial institution (i.e. future transaction records that the financial institution will obtain through account monitoring) (CPA s.210b). If there is suspicion of a criminal act that is punishable by imprisonment of five years or more the court may oblige a financial institution to submit future information for a period not exceeding four weeks. In such cases, notification to the suspect may be postponed if strictly necessary for the investigation (CPA s.210c).

180. ***Search:*** The competent authorities have the power to search premises for financial records, etcetera (CPA s.192) if there are reasonable grounds to suspect that a criminal act punishable by imprisonment is committed. The objective must be to search for evidence or things that may be seized or charged. A search of the suspect's person may also be conducted on the same conditions as a search of his premises, provided that there is reason to believe that search may lead to detection of evidence or things that may be seized or charged (CPA s.195). A search may also take place at premises belonging to a third party provided that there is just cause for suspecting that a criminal act punishable by imprisonment is committed and: (i) the criminal act was committed or the suspect was arrested on the premises; (ii) the suspect was there under pursuit when caught in the act or on finding fresh clues; (iii) or there are particular reasons to believe that the suspect may be arrested there or evidence/things found that might be seized or charged (CPA s.192). Third parties can be searched when a criminal act that is punishable by imprisonment of more than six months is suspected, and there is a particular reason to conduct the search (CPA s.195).

181. As a general rule, the court has powers to issue a search order without prior notification to the suspect; however, in urgent matters, the Prosecution Authority may issue the search order (CPA s.197). A police officer can search premises without decision from the court or the Prosecution Authority if the suspect is caught in the act of committing a crime or there is a danger that a search (which relates to a strong suspicion of a criminal act that is punishable by more than six months imprisonment) might otherwise be spoiled (CPA s.198). The principal rule is that the search should be carried out in the presence of a witness and the suspect (or, if the suspect is absent, a family member

or a neighbour, etcetera). However, notification to the suspect may be postponed (for up to eight weeks at a time) if: (i) there are reasonable grounds to suspect that one of the following types of offences has been committed: a money laundering offence; a drug trafficking offence; a felony against the independence and safety of the state, constitution or head of state; or a criminal act punishable by imprisonment of more than 10 years; (ii) the search is of considerable importance for the investigation; and (iii) the investigation otherwise will be considerably impeded. At the latest, notification must be given in a money laundering case at the time of indictment (CPA s.200a).

182. ***Seizure:*** The competent authorities have the power to seize financial records, etcetera provided that those records may have significance as evidence (CPA s.203). The principal rule is that the Prosecution Authority takes the decision on seizure; however, the police may take the decision when the suspect is caught in the act, pursued when caught in the act, or on finding fresh clues. In such cases, the Prosecution Authority must be notified as soon as possible and must decide whether the seizure should be sustained (CPA s.206). The decision on, and execution of seizure is taken without prior notice to the suspect or third party. The court may also impose a duty for a possessor to remain silent about the seizure (CPA s.208a). The principal rule is that notification should be given after the execution of the seizure. However, notification may be postponed if there are reasonable grounds to suspect that a criminal act punishable by imprisonment of more than six months has been committed, and that notification may severely impede the investigation (CPA s.208a). Such decisions can be taken for a period of up to eight weeks. Once notice has been given, the suspect or any third party with an interest in the property may ask the court to decide whether the decision should be sustained (CPA s.208).

183. ***Witness statements:*** The police and Prosecution Authority do not have the power to compel witness statements, unless the witness is a public official or a person that acts on behalf of the state or a municipality (CPA s.230). However, the witness is obliged to meet at the police station (if served with a summons) in order to advise whether he/she is willing to give a statement. Alternatively, the witness may consent to give a statement to the police or Prosecution Authority (CPA s.230). The general principle is that witnesses are required to give a statement to the court (CPA s.108). In May 2003, the Police Directorate adopted a Witness Protection Program. In January 2004, amendments to the Norwegian Police Act were adopted (chapter 2a), making it possible to give a person a totally new identity. Procedures to prevent witnesses from becoming endangered were also adopted. For instance, anonymous witness statements may now be used as evidence in court in certain cases of serious crime (CPA s.130(a)). As well, witnesses may now remain anonymous during an investigation (CPA s.234a). Moreover, it is now possible to interrogate a witness by use of telecommunication (CPA s.109a).

Recommendation 30 (Resources of law enforcement, prosecution and other competent authorities):

184. ***Police Directorate:*** The Police Directorate manages and co-ordinates the Norwegian police which employs approximately 12 000 people (7 844 police officers, 765 lawyers and 3 440 administrative personnel) and is headed by the National Police Commissioner who is responsible for setting priorities and administering the budget. The police is comprised of the Police Directorate, the PST and 27 police districts (each with its own headquarters and several police stations).[44] The PST is organised directly under the Ministry of Justice & Police. Each district is under the command of a Chief of Police who has full responsibility for all kinds of policing in the district, and is divided into sub-districts (each under command of a lensmann). All police officers are trained to be generalists in order to fulfil every aspect of ordinary police work (such as patrolling and public order policing) and criminal investigation (including investigation in ML cases). Police officers are required to maintain high standards of professionalism and integrity, and must be appropriately skilled. The Oslo police district is the largest in Norway and operates somewhat differently from the others. For many years, it has had a separate section for investigating economic crime. This section is

[44] In 2002, the number of local police districts was reduced from 54 to 27.

now organised as part of the Department of Organised Crime, employing 10 police lawyers, 30 police investigators, four accountants and five administrative personnel. Police budgets for the past three years have been as follows: (2003) NOK 6.8 billion (EUR 824 million/USD 1.1 billion); (2004) NOK 6.9 billion (EUR 833 million/USD 1.09 billion); and (2005) 7.8 billion (EUR 945 million/USD 1.2 billion). This is an increase of 13.9% from 2004 to 2005.

185. Norway recognises that economic crimes and other serious profit-motivated crimes require proper financial investigation to identify and trace proceeds, including effective financial reporting and sufficient access by investigators to police and other registers. All of the police districts in Norway shall establish separate teams to combat economic crime by 1 July 2005 (Action Plan 2004). The large district and most of the others have already done so. Each team is headed by a prosecutor who is assisted by police investigators and accountants. The structure of the teams varies between the police districts, reflecting the size of the districts and their needs, based on the crime threat, etcetera; however, they must integrate police, judicial and economical competence. (For instance, in Oslo, the team is part of the organised crime unit.) Each team is organised as part of the ordinary investigation units, and has access to all police registers (including intelligence information). The objective of this initiative is to ensure that the teams have the competence and resources to investigate complex economic crime, and that more resources than before are allocated to these types of crimes. As of November 2004, 250 persons were working in such teams.[45] Additionally, ØKOKRIM has created a team consisting of ten investigators to enhance competence in investigating economic crime and money laundering. This team is supporting the police districts through education and arranging conferences. Additionally, key persons in the police have received the textbook on confiscation that was produced by the AC/AML Project. As well, the Police College will start with courses in economic crime and ML.

186. ***Prosecution Authority:*** The Prosecution Authority is responsible for the professional leadership of the handling of criminal cases by the police, managing investigations and conducting cases (including ML/FT cases) in court (Judiciary Committee of the Parliament, Budsjett innst.S. nr. 4, page 26). The DGPP (who heads the Prosecution Authority) also has responsibility for managing the police districts and 10 District Public Prosecution Offices and 27 district offices which are integrated in the police and comprised of senior public prosecutors (each under the leadership of a chief state prosecutor). The power of the Prosecution Authority to instigate criminal proceedings was recently extended to allow the police to decide more economic crime cases.[46] The Prosecution Authority operates independently of political influence and administrative control in individual investigations and prosecutions. Only the King in Counsel (which is the whole cabinet of ministers) may prescribe general directives as to how the DGPP shall discharge his duties, but cannot interfere in individual cases. Neither the Ministry of Justice & Police nor any individual minister can give instructions in matters of prosecution (CPA chapters 6 and 7). The Prosecution Authority also governs investigations done by the security police, so that the investigation of criminal cases is not influenced by party or political considerations (The Judiciary Committee of the Parliament, Innst. O. Nr: 89, page 2).

187. Prosecutors are required to maintain high standards of professionalism and integrity, and must be appropriately skilled. They need to have a basic knowledge of: the normal functioning of industry, commerce, public administration and organisations; accounting and economic matters and relations; and specific legislation (i.e. the Tax Assessment Act, the MLA and confiscation provisions in the Penal Code).[47] Additionally, the DGPP is publishing circular letters to inform law enforcement authorities of objectives and priorities. For instance, Circular 2/2004 establishes that the new MLA

[45] The Ministry of Justice & Police intends to submit a Report to the *Storting* (during the first session of 2005) on the role of the police. This report will address issues such as the importance of ensuring that senior police officers are aware of the requirements regarding economic crime investigations (Action Plan 2004 s.5.1).

[46] Statutory amendment of 19 December 2003, which entered into force on 1 April 2004.

[47] Norway reports that it intends to implement measures to raise the level of competence of both the Prosecution Authority in the police and the superior Prosecution Authority

(which entered into force on 1 January 2004) gives both the police and the prosecutor the possibility to use information from STRs during an investigation. It also states that ØKOKRIM shall enhance the competence in the police districts so that STRs can be used in an effective way. According to DGPP's statistics, during 1998-2003, the average rate of crime detection was 36 %. From 1960-2002, the number of felonies increased from 38 700 to 339 506. The distribution of felonies investigated in 2003 is as follows: Crimes of gain-64%; Violence-8%; Drugs-13%; Sexual offences-1%; and Criminal Damage-6%. From 1984-2003, drug seizures increased from 2 200 to 25 210.

188. ***Oslo Police District:*** The Oslo Police District is organised into three major departments (each led by an assistant chief of police) and 16 sections. Money laundering is investigated by 10 of these sections. The prosecutors (who are placed in groups under one section—the prosecution section) work closely with investigators under these 10 sections. The ratio of population to police in Oslo is 500 000 inhabitants to 2 153 staff in the Oslo Police District (1 500 police officers, 100 prosecutors and 553 civilian staff). The Oslo Police District has had a section dedicated to combating organised crime since 1 January 2004 (after the police districts were reorganised). This section is responsible for combating trafficking of illegal drugs and liquor, robbery and other organised crime. It handles around 1 000 cases per year. As well, there is a section dedicated to combating financial crime and investigating more serious fraud, bankruptcy and environmental crimes. It handles around 1 500 cases per year. The number of reports made to the police every year is about 100 000 (and has been so for the last few years). The police also receive a lot of information from ØKOKRIM; however, there are no statistics concerning how much of this information is related to money laundering cases. The Oslo Police District has good co-operation with the MLU. Money laundering investigations usually start after the MLU receives an STR or the police detect money during searches conducted in the course of ordinary investigations.

189. ***ØKOKRIM:*** ØKOKRIM has 116 employees.[48] The Assets Confiscation Team (which is located at ØKOKRIM) has nine staff. ØKOKRIM recruits highly educated and experienced staff with high professional standards. It stresses the need of keeping its staff updated, and has its own programs for that purpose. ØKOKRIM is also involved in building the competence of the police, Prosecution Authority, and Police College concerning financial crime.

190. ***Police College:*** The Police College provides a basic three-year training programme in police subjects. Some of the subjects taught include financial investigation, money laundering and confiscation, but do not currently include instruction in financial investigation.[49] Although the Police College intended to hire a staff member specifically for the purpose of setting up a financial investigation course, the hire was cancelled just prior to the on-site visit. It is not clear if or when the initiative to hire a staff member for this purpose will be renewed.

191. The Police College currently provides an annual advanced training course to police officers and lawyers on economic crime; however, Norway acknowledges that this is not sufficient to meet the need for competence in this area. Consequently, Norway is experiencing difficulty in recruiting lawyers and police officers with adequate professional competence in the area of economic crime. Moreover, there is concern that members of economic crime teams must wait too long to obtain advanced training in economic crime cases. Consequently, members of economic crime teams have been given a pre-emptive right to admission to the Police College's advanced economic crime course (which will be offered annually from the 2004-2005 academic year). Additionally, the Police College will provide short courses (approximately one to two weeks in duration) for the purpose of raising the competence regarding economic crime and financial investigation of the members of economic crime teams pending completion of advanced course by all team members. All such personnel shall been offered such courses by the end of 2005 (Action Plan 2004 s.5.1).

[48] As of May 2005 the number is 125.

[49] The Police College intends to include financial investigation as a separate subject in the basic training course from the academic year of 2005/2006 (Action Plan 2004 s.5.1).

192. Using the resources available to them, Norwegian law enforcement, prosecution and other competent authorities have initiated 2 342 investigations relating to intentional and negligent money laundering offences (not including receiving offences). The following chart sets out the number of investigations that were initiated for the following types of money laundering violations: ordinary, gross and negligent assistance in securing the proceeds of crime for another person, and assistance in securing the proceeds of drug trafficking for another person. (It should be noted that these statistics do not include money laundering offences related to receiving proceeds of crime.)

NUMBER OF MONEY LAUNDERING INVESTIGATIONS INITIATED *(These statistics do not include money laundering offences related to receiving proceeds of crime)*					
TYPE OF OFFENCE *(Statistics provided by STRASAK)*	2000	2001	2002	2003	2004 (up to 30.06.2004)
Ordinary money laundering: Assisting in securing proceeds of crime less than NOK 75 000 (EUR 9 100 / USD 11 900) for another person	66	59	139	212	116
Aggravated money laundering: Assisting in securing proceeds of crime greater than NOK 75 000 (EUR 9 100 / USD 11 900) for another person	38	36	38	37	18
Drug-related money laundering: Assisting in securing the proceeds of drug trafficking for another person	1	1	1	5	0
Negligent money laundering: Negligently assisting in securing the proceeds of crime for another person	240	350	417	410	158
ANNUAL TOTAL OF ML INVESTIGATIONS INITIATED	345	446	595	664	292

193. The following chart sets out the percentage of money laundering cases that were solved, based on the number of money laundering investigations that were initiated (as set out in the chart above).

NUMBER OF MONEY LAUNDERING INVESTIGATIONS SOLVED *(These statistics do not include money laundering offences related to receiving proceeds of crime)*					
TYPE OF OFFENCE *(Statistics provided by STRASAK)*	2000	2001	2002	2003	2004 (up to 30.06.2004)
Ordinary money laundering: Assisting in securing proceeds of crime less than NOK 75 000 (EUR 9 100 / USD 11 900) for another person	71%	86%	61%	64%	45%
Aggravated money laundering: Assisting in securing proceeds of crime greater than NOK 75 000 (EUR 9 100 / USD 11 900) for another person	69%	80%	80%	74%	70%
Drug-related money laundering: Assisting in securing the proceeds of drug trafficking for another person	58%	100%	100%	100%	100%
Negligent money laundering: Negligently assisting in securing the proceeds of crime for another person	77%	94%	97%	89%	92%
ANNUAL TOTAL PERCENTAGE OF ML CASES SOLVED	69%	90%	85%	82%	77%

194. ***ROK:*** The purpose of ROK is to co-ordinate and allocate resources against organised crime and to support the CATCH project.[50] ROK is a council (established in 2000) consisting of representatives from ØKOKRIM, the DGPP, the Police Directorate, New Kripos, the Oslo Police District and one chief of police representing the other 26 police districts. Its budget is NOK 12 million (EUR 1.5 million/USD 1.9 million).

[50] Since 1 April 2005, ROK no longer supports the CATCH project because that project has ceased to exist and its functions are now implemented in New KRIPOS.

195. ***CATCH:*** The CATCH project is focused on combating organised crime, serious drug-related crime and other serious organised crime (such as smuggling and related money laundering). It has a project leader and is staffed as follows: 2 staff from ØKOKRIM, 2 staff from KRIPOS, 16 staff from the Oslo police district, and 2 team leaders with 11 investigators and 2 consultants. CATCH was created three years ago and is concentrating on extensive cases (e.g. heroin smuggling from Kosovo, alcohol smuggling from Spain, monitoring criminal activity originating from prisons, hashish smuggling from the Netherlands, robberies, trafficking in women and amphetamine smuggling from Poland).[51]

196. ***Customs authorities:*** There are approximately 1 700 people employed in the Customs Directorate and the Customs Regions, of which 17% are involved in border control and 8% in the declaration and audit control. The Customs Directorate also has a few dogs that are trained to detect drugs and cigarettes, but none that are trained to detect currency.

197. ***Judicial authorities:*** There is recognition in the Action Plan 2004 that judges need additional special training to handle money laundering cases.

198. *Additional elements:* Norway reports that a number of trends are increasing the demands on judicial competence. For instance, a growing number of criminal cases (such as those dealing with insider trading and currency manipulation) have a high level of difficulty. To address the difficulty of developing and maintaining the necessary judicial competence, expert lay judges may be appointed. However, it is still necessary to ensure that the professional judge understands the expert lay judge. The Norwegian government has recommended that the court administration implement training programmes for judges concerning economic crime. The government is also considering whether certain types of cases involving economic crime should be dealt with by specific courts in the districts (i.e. a central district court in each judicial district) (Action Plan 2004 s.5.3). In the meantime, to address the need for higher competence in cases involving confiscation and financial investigation, one of the members of the AC/AML Project published a textbook in January 2004. Two thousand copies have been distributed to key persons in the police and Prosecution Authority.

199. ***Recommendation 32 (Statistics relating to law enforcement and prosecution):*** Norway maintains the following statistics relating to ML/FT investigations, prosecutions and convictions, and on property frozen, seized and confiscated:

(a) The number of money laundering investigations initiated;

(b) The number and types of decisions on indictment or fine made by prosecution authorities;

(c) The percentage of total investigations solved;

(d) The percentage of convictions based on the total number of cases put before the courts;

(e) The number of confiscation orders issued;

(f) The amount of money confiscated, including a breakdown of the total amount and number of confiscation orders issued in relation to money laundering, drug trafficking and alcohol smuggling offences; and

(g) The number of persons and amounts of property frozen pursuant to the UN Resolutions related to terrorist financing.

200. Statistics collection in this area has improved in that a distinction is now made between the different kinds of money laundering offences, and between extended and normal confiscation. However, no statistical information is available concerning the criminal sanctions that were imposed

[51] As of 1 April 2005, the functions of CATCH are implemented in the regular structure of the National Criminal Investigation Service (New KRIPOS).

on persons convicted of money laundering. Norwegian authorities report that it is difficult to know exactly how many money laundering cases really exist because it depends on how the judge characterises the case. For instance, many offences that are characterised as tax crimes are, in reality, organised crime cases relating to smuggling, drugs or fraud. Because there have not been any prosecutions for terrorist financing in Norway, no statistics exist in this area.

2.6.2 Recommendations and Comments

201. There is concern that ØKOKRIM attracts too many of the highly trained economic crime investigators—to the detriment of the police districts. Moreover, although each police district now has its own economic crime unit, no additional resources were dedicated for this purpose. Existing resources were reallocated to create the economic crime units. Norway should ensure that additional resources are allocated to the economic crime units at the police district level. There is also some concern that, in the last few years, the Police Directorate has not given sufficient priority to AML efforts with regards to the Police College's involvement, ØKOKRIM and others. However, it should be taken into consideration that the Police Directorate was established during 2001. This also coincided with the total restructuring of the police service which was completed at the end of 2004. Consequently, the evolution of these steering and management systems is not yet in a fully mature stage of development. Overall, law enforcement/prosecutorial budgets have increased in recent years. It is a matter for the police chiefs of the individual police districts to prioritise and reallocate resources to implement the AML/CFT measures set out in the Action Plan 2004. For example, each police district had to allocate their budgetary resources to create economic crime teams when the Police Directorate ordered that such teams should be created. Consequently, each police district had to reallocate resources for this purpose. Likewise, even though the Action Plan 2004 recognises that more resources need to be allocated towards training, and the Police College had intended to hire a staff member specifically for that purpose, the hire was cancelled just prior to the on-site visit. Norway should ensure that this hiring is carried out as soon as possible. Norway should ensure that additional resources are allocated to AML/CFT training for police and prosecutors. As well, Norway should collect statistics concerning the types of criminal sanctions imposed for ML. Additionally, Norwegian authorities report that detection of money laundering activity sometimes results in detection of the predicate offences.

2.6.3 Compliance with Recommendation 27, 28, 30 & 32

	Rating	Summary of factors relevant to s.2.6 underlying overall rating
R.27	C	• Recommendation 27 is fully observed.
R.28	C	• Recommendation 28 is fully observed.
R.30	PC[52]	• The Police College currently provides an annual advanced training course to police officers and lawyers on economic crime; however, Norway acknowledges that this is not sufficient to meet the need for competence in this area. Consequently, Norway is experiencing difficulty in recruiting lawyers and police officers with adequate professional competence in the area of economic crime. Moreover, there is concern that members of economic crime teams must wait too long to obtain advanced training in economic crime cases. • There is concern that ØKOKRIM attracts too many of the highly trained economic crime investigators—to the detriment of the police districts. • There is also some concern that, in the last few years, the Police Directorate has not given sufficient priority to AML efforts with regards to the Police College's involvement, ØKOKRIM and others.
R.32	PC[53]	• No statistical information is available concerning the criminal sanctions that were imposed on persons convicted of money laundering. Norwegian authorities report that it is difficult to know exactly how many money laundering cases really exist because it depends on how the judge characterises the case.

[52] This is an overall rating for compliance with Recommendation 30, based on the assessments in sections 2.5, 2.6 and 3.10 of this report.

3 PREVENTIVE MEASURES - FINANCIAL INSTITUTIONS

Customer Due Diligence & Record Keeping

3.1 Risk of money laundering or terrorist financing

3.1.1 Description

202. The current Norwegian AML legislation was adopted in June 2003 before the last revision of the FATF 40 Recommendations. Thus, the legislation is not based on risk assessments in the manner contemplated in the revised FATF 40 Recommendations. However, in line with the 2nd EU Money Laundering Directive, Norway has extended AML/CFT obligations to certain DNFBP sectors that FATF Recommendations do not require countries to cover, including dealers in all objects (not just dealers in precious metals and stones), auctioneering firms, commission agents and the like.

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

3.2.1 Description and Analysis

Recommendation 5

203. Norway has not yet implemented the FATF Recommendations 2003. Consequently, although it has implemented provisions relating to customer identification, it does not have appropriate measures concerning customer due diligence. Currently, Norway's customer identification measures (which are set out in the MLA and MLR) are based on implementation of the 1st and 2nd EU Money Laundering Directive, and the FATF Recommendations (1996). Norway reports (and confirms in its Action Plan 2004) that it was waiting for the 3rd EU Money Laundering Directive to be finalised before fully implementing the FATF Recommendations 2003. It should be noted that the 3rd EU Money Laundering Directive was just adopted. Customer identification requirements are fully applied to all of the financial institutions that must be covered according to the FATF Recommendations. This means that customer identification obligations apply to a broad range of financial institutions and other entities with a reporting obligation in Norway (including branches of foreign undertakings):

(a) Financial institutions (as the term is understood in Norwegian law);

(b) Norges Bank (the Central Bank of Norway);

(c) E-money institutions;

(d) Persons and undertakings operating activities consisting of transfer of money or financial claims;

(e) Investment firms;

(f) Management companies for securities funds;

(g) Insurance companies;

(h) Pension funds;

(i) Postal operators in connection with provision of postal services;

(j) Securities registers; and

(k) Other undertakings whose main activity relates to the business of credit institutions, including the provision of loans, stockbroking, payment transmission, financial leasing, advisory services, and other services associated with financial transactions and letting of safe deposit boxes

[53] This is an overall rating for compliance with Recommendation 32, based on the assessments in sections 2.5, 2.6, 3.13, 6.3, 6.4 and 6.5 of this report.

(collectively referred to as Reporting Financial Institutions or Reporting FIs) (MLA ss.3-4).[54]

204. The MLA does not define the term *financial institution;* however, Norway says that the term has the same meaning as in the Financial Institutions Act (FIA), which defines financial institutions as companies, undertakings and other institutions which carry on financial activity (except for certain specified classes). *Financial activity* is in turn defined as the granting, negotiating, or furnishing of guarantees for credit or otherwise participating in the financing of activity other than one's own but excluding, inter alia, the placement of investments with other financial institutions. The term *financial institution*, as used in the MLA would therefore refer to savings banks, commercial banks, finance companies, mortgage companies and insurance companies. The chart at paragraph 19 of this report lists the financial institutions authorised in Norway to perform the various activity encapsulated in the FATF definition of a financial institution.

Anonymous accounts and accounts in fictitious names

205. Norway's legislative regime effectively precludes the use of anonymous accounts or accounts in fictitious names. Reporting FIs are not allowed to register anonymous accounts or accounts in fictitious names. This follows from the requirement of the MLA that Reporting FIs are required to identify their customers and record the name, identification number, address and other identification information produced by the customer (MLA s.6) (see further details below). Numbered accounts are not known in Norway.

When CDD is required

206. Although Norway has implemented customer identification obligations, it has not implemented full customer due diligence (CDD) requirements. Reporting FIs are required to identify the customer in three situations (see MLA s. 5, Circular 9/2004 s. 2.7.1). First, customer identification is required at the time the customer relationship is established (MLA s.5 para.1). Second, customer identification is required when the Reporting FI enters into a transaction (including a wire transfer) involving NOK 100 000 (EUR 12 100/USD 15 800) or more with a customer with whom the reporting FI has no previously established customer relationship.[55] This obligation applies to situations where the threshold is exceeded in a single operation or in several operations that appear to be linked (MLA s.5 para.2). The term *transaction* refers to any transfer, intermediation, exchange or placement of assets (MLA s.2), but it does not include an account holder's deposits or withdrawals from his/her own account (Circular 9/2004 s.2.7.1). In the context of occasional customers, a Reporting FI comprising more than one branch is regarded as a single institution. Consequently, a branch that accepts an assignment is obliged to view this assignment in the context of any other executed transactions of which it is aware (Circular 9/2004 s.2.7.1). Third, customer identification is required in all cases if the Reporting FI suspects that a transaction is associated with the proceeds of crime, terrorist offences or terrorist financing (MLA s.5 para.3). Moreover, if the Reporting FI has reason to believe that data contained in the customer's identity documents is not correct, it is required to verify that data (MLR s.8).

Required CDD measures

207. ***Identification of natural persons:*** The general rule is that customers who are natural persons must have their identity verified by attending at the office of the Reporting FI (MLA s.5). The customer must produce valid written proof of identity on the basis of either original documents or certified copies (MLA s.5; MLR s.4). The Reporting FI must then satisfy itself of the customers' identity by verifying that the photograph and signature appearing in the identity document match the

[54] See Annex 5 for a description of how many financial institutions exist. See Annex 12 for a complete description of Reporting FIs.

[55] This threshold is lower than the threshold of EUR 12 000 currently required by the 2nd EU Money Laundering Directive.

appearance and signature of the individual who is appearing in person (MLR s.8). The identity documents must not have expired. Although original identity documents must generally be produced, certified copies are admissible in exceptional cases (i.e. when a person applying for a visa must send the original identity documents to an embassy or consulate), provided that the copies are verified by an authorised person(s). The only persons authorised to confirm the veracity of a certified copy are postal employees (including rural postmen), the police, lawyers, state authorised/registered auditors, Reporting FIs and all other businesses and professions that are obligated to report under the MLA (with the exception of high value goods, including auctioneering firms, commission agents and the like) (Circular 9/2004 s.2.3).[56] Electronic proof of identity is not regarded as valid proof of identity.[57]

208. The customer's identity document(s) must contain the customer's full name, signature, photograph and personal identity number or D-number (MLR s.4). If no personal identity or D-number has been allocated, satisfactory identity documents must be produced containing the customer's full name and date of birth, place of birth, sex and nationality. Other (mostly) foreigners that do not have a Norwegian identity number can use their own country's identity documents. If the Reporting FI is aware that the customer has dual nationality, this shall also be recorded as additional information (MLR s.4). Not all of this information has to be contained in the same document; presentation of several documents is acceptable to meet this requirement (Circular 9/2004 s.2.3).

209. Norway has implemented detailed requirements to ensure that a natural person's identity is verified using only reliable, independent source documents. The identity documents must have been issued by a public authority or other body that has a satisfactory and generally accepted level of security concerning the issuance of documents (MLR s.4). The FSA interprets this to mean that identity documents must be recognised either as national or correspondingly international (i.e. within the EEA). Identity documents that meet the requirements as to verification routines and security level include (positive list):

(a) Valid passport or other approved travel document;

(b) Bank card (Norwegian);[58]

(c) Driving licence–original and duplicate (not, however, a Norwegian "green driving licence", which is now obsolete);

(d) The new Armed Forces ID card;

(e) Norway Post's ID card issued after 1 October 1994;[59]

(f) EU card;[60] and

(g) Asylum seeker certificate. However, due to factors related to their issue and use, such certificates may, based on a concrete assessment, be deemed unsuitable for identity verification purposes (Circular 9/2004 s.2.3).

---

[56] See Annex 12 for a complete description of the Reporting BPs.

[57] On 9 March 2004, the Norwegian government introduced a bill which puts electronic proof of identity on an equal footing with written/visual proof of identity (Electronic Signatures Act No. 81). Once the necessary amendments are made to the Money Laundering Act, these provisions will apply to the AML/CFT legislation (Circular 9/2004 s.2.3).

[58] Norwegian bank cards have the customer's photograph, 11-digit identification number, date of birth and signature. If the card can be used to make payments or withdraw cash, it also is provided with a pin code.

[59] Norway Post identification cards that were issued after 1 October 1994 have the customer's photograph, 11-digit identification number, date of birth and signature.

[60] An EU card is an identification card that has been issued by the government of an EU country and contains (at a minimum) the customer's photograph, date of birth and signature.

210. A number of documents (such as bank cards that were issued in a particular period) do not contain a complete personal identity number (11 digits). If a document which lacks a complete personal identity number is presented, the Reporting FI must require proof of a personal identity number. This could be furnished in the form of a certificate of tax paid on declared earnings or a card issued by the National Population Register confirming the prospective customer's personal identity number (Circular 9/2004 s.2.3). Locally-issued or limited use cards issued within an undertaking (such as a school, university or association) cannot be accepted as valid proof of identity. The following documents can certainly not be regarded as meeting the requirements of the money laundering legislation (negative list):

(a) Credit cards, invoicing cards and the like;

(b) Norway Post's identity cards issued prior to 1 October 1994;

(c) Travel pass for bus, tram, train, etcetera;

(d) Association membership cards; or

(e) Identity cards issued by schools or universities (Circular 9/2004 s.2.3).

211. In between the "positive" and the "negative" list there is a grey area where Reporting FIs themselves have to make an assessment whether or not to accept an identity document. However, Norway has implemented some controls to ensure that Reporting FIs give careful consideration when exercising this discretion. For instance, the Reporting FI has to be able to justify to the FSA why it did accept an identity document in any particular case. Moreover, the acceptance of a document on the positive list must, in some circumstances, also be justified having regard to the circumstances (i.e. driving licences from non-EEA countries).

212. ***Identification of legal persons:*** Reporting FIs must identify the natural person(s) who will be authorised to operate the account/safe custody facility or to have transactions carried out (MLR s.4; Circular 9/2004 s.2.5). This obligation also applies to a procurist, the holder of "power of position" *(stillingsfullmakt)* or "dependent authority" *(oppdragsfullmakt),* or a person(s) entitled to execute an isolated transaction (Circular 9/2004 s.2.5). As is the case with natural persons, Norway has implemented detailed requirements to ensure that a legal person's identity is verified using only reliable, independent source documents. The Reporting FI is obligated to verify the legal status of customers that are legal persons in the following way[61]:

(a) Legal persons that are registered in the Business Register must produce an original or certified copy of its certificate of registration dated within the past three months (MLR s.6; Circular 9/2004 s.2.5). Alternatively, a full transcript of the legal person's identification information dated within the past three months and obtained from the Brønnøysund Register Centre or by licensed credit information businesses may be provided (Circular 9/2004 s.2.5).

(b) Legal persons that are registered in the Central Co-ordinating Register, but not in the Business Register, must produce a transcript (dated within the past three months) of all its registered data from the Central Co-ordinating Register (MLR s.6; Circular 9/2004 s.2.5).

(c) Legal persons that are not registered in the Central Co-ordinating Register, but are registered in another public register shall produce similar documentary evidence that sets out the legal person's name, the address of its place of business or head office and, if applicable, its foreign organisation number. The documentation shall also state which public register, within or outside Norway, can verify the information given (MLR s.6).

(d) Legal persons that are limited companies in the process of incorporation and have not been registered in the Business Register or the Central Co-ordinating Register at the time of

[61] Norway has several registers for legal entities. Many of those registers interconnect; some serve as source registers for others, while others are used to compare changes.

establishment or at the time of the transaction must present the original incorporation document. A copy of this document must be kept by the Reporting FI (MLR s.15; Circular 9/2004 s.2.5).

(e) Where the legal persons is clearly/probably not registered in a public register (e.g. associations, co-ownerships, investment clubs, charitable organisations and collection accounts), the proof of identity of a natural person shall be recorded (MLA s.5-6; MLR s.6; Circular 9/2004 s.2.5). In other words, to establish the customer relationship, the Reporting FI must register the customer relationship in the name of a natural person. The natural person in whose name the legal person will be registered depends on the nature of the undertaking, including any delegation of authority to sign on its behalf and/or the designation of any disposition holder. The natural person may be the chief executive officer, general manager, board chairman or association chairman. However, if the legal person has no such officers, the natural person may be an associate, partner, co-owner, promoter, sub-manager or agent. This is not an exhaustive list. Where the natural person is not a sub-manager and/or agent for the customer, he or she must also provide proof of identity and register the information in accordance with sections 5 and 6 of the MLA. However, as the FSA admits, this requirement is not stipulated in law or regulation.

213. There are extensive rules on the identification of a customer who is a legal person and also of an individual acting for that legal person. However, there is presently no legal requirement under the MLA or MLR for a Reporting FI to verify that the individual is duly authorised to act for the legal person. The FSA has informed the assessors that they are working with the Ministry of Finance to have the law amended.

214. ***Identification of beneficial owners:*** As in most civil law jurisdictions, in Norway, ownership is absolute. If a Reporting FI knows or has reason to believe that a customer is acting as a (legal) representative of another, on behalf of another, or that another person owns the asset that is the subject of a transaction, the FI is required to identify that other person (MLA s.6). Other than this, there is no other requirement to identify a beneficial owner within the meaning of the FATF Recommendations (i.e. the natural person(s) who ultimately owns or controls a customer and/or the person on whose behalf a transaction is being conducted, and incorporating those persons who exercise ultimate effective control over a legal person or arrangement). As used in the FATF Recommendations, the term *beneficial owner* captures both the notion of equitable owner, as well as the notion of a person exercising ultimate ownership and control over a legal person or arrangement.[62] In Norway, Reporting FIs are not legally required to actively inquire if the customer is "fronting" for any other person in respect of an account or a transaction (for instance, by asking as a routine part of the account opening procedure whether the account holder is acting on behalf of another person). The FSA has informed the FATF assessors that they do expect Reporting FIs to make such inquiries as part of the process of knowing their customers, although this does not appear to be included within Circular 9/2004. Reporting FIs are also not required to obtain information relating to the shareholding or any corporate group behind a customer who is a legal person. There is a requirement for all Norwegian and foreign legal persons conducting business in Norway to register in the Business Register (Business Register Act), including filing their articles of association with the Business Register. When Reporting FIs enter into a business relationship with a legal person, the legal person is obligated to provide its certificate of registration. This certificate of registration contains information about the nature of the legal person's business and purpose, for instance, whether it is an import/export company. However, this does not go as far as the FATF Recommendations require in that there is no obligation on the Reporting FI to inquire about the purpose and nature of the business relationship vis-à-vis the Reporting FI itself. For instance, if a company is opening an account with a bank, there is no obligation on the bank to obtain information from the company about why it is opening the account, the purpose of the account, the anticipated volumes going through the account, etc. Nor is there an obligation on the bank to conduct ongoing due diligence on the business relationship in this regard.

[62] See the definition of *beneficial owner* in the Glossary to the FATF Recommendations.

Risk

215. Norway has implemented the same customer identification rules for all types of customers, with certain exceptions (see below). There is no enhanced CDD legislation for higher risk categories of customers. Except as noted below, Norwegian legislation does not provide for any simplified or reduced CDD measures. The general rule is that customers must be subject to the full range of identification measures set out above. However, the obligation to request proof of identity and to record the identification data does not apply at all if the customer is:

(a) A savings bank, commercial bank, finance company or mortgage company (grouped together and referred to as a financial institution within the meaning of the FIA);

(b) Branches of a credit institution which are established and authorised to carry on business in Norway but are subject to the supervision of authorities of other EEA states;

(c) Branches of a credit institution with its head office in a non-EEA state, with authorisation to carry on financing activity in Norway;

(d) An investment firm;

(e) A management company for securities funds; or

(f) A foreign undertaking which is subject to equivalent legislation that satisfies the identification obligations set out in Council Directive of 4 December 2001 on prevention of the use of the financial system for the purpose of money laundering (2001/97/EC) and is subject to a supervisory regime of EEA standard (MLR s.7). Countries with supervisory arrangements of EEA standard are assumed to include–alongside EU/EEA states–Australia, Canada, Hong Kong, Japan, New Zealand, Singapore, Switzerland, Turkey and the USA (all of which are members of FATF). This is based on the assumption that all of these countries have implemented the FATF Recommendations to a satisfactory standard. The new countries joining the EU in the first half of 2004 will meet the requirements as to supervisory arrangements of EEA standard once they have the required rules in place. It has yet to be decided to what extent the supervisory arrangements of the newer FATF countries–Brazil, Mexico, Argentina, Russia and South Africa–are up to EEA standard (Circular 9/2004 s.2.6).

216. Additionally, the obligation to request proof of identity and to record the identification data does not apply to the following types of insurance activity:

(a) Writing insurance policies where the premium is to be paid by debiting an account opened in the customer's name with a credit institution that: (i) is subject to the MLR or equivalent legislation in conformity with the 2nd EU Anti-Money Laundering Directive; or (ii) has by other means satisfied itself, and recorded evidence, of the identity of the customer;

(b) An authorised institution writing life insurance policies where the annual premium does not exceed NOK 8 000 (EUR 970/USD 1 300), or where a single premium is to be paid not exceeding NOK 20 000 (EUR 2 400/USD 3 200). However, if the periodic premium amount to be paid in any given year is increased so as to exceed the NOK 8 000 threshold, full customer identification must be performed;

(c) An authorised institution writing pension insurance policies where the policy is taken out by virtue of a contract of employment or the insured's occupation, provided that such policies do not contain a surrender clause and may not be used as collateral for a loan (MLR s.7); or

(d) An authorised institution writing non-life insurance policies, including travel insurance policies, as well as credit insurance policies (MLR s.7).[63]

Additionally, the Ministry may exempt e-money institutions from the customer identification obligations on a case-by-case basis (MLR s.7), and has done so in one case. However, this is a very limited exemption from the obligation to have the person attend in person for the purpose of identity verification with several conditions attached to it. The exemption is time limited (one year, 6 months). Further conditions are that the e-money account must be managed through a bank that must comply with the obligation for the customer to attend in person, the e-money institution shall perform customer identification when the transactions in one e-money account in total exceeds 40 000 NOK. Moreover, the exemption did not extend to the obligation to request proof of identity if there is a suspicion that the transaction related to ML/FT. The preceding exemptions from the identification obligations are not overridden if the Reporting FI has a suspicion that a transaction is connected with proceeds of crime or terrorist financing.

217. Where the customer is unable to produce the identity documents required by section 4 of the MLR, the Reporting FI may still establish a customer relationship or carry out the requested transaction if: (i) the Reporting FI is certain of the customer's identity; (ii) the Reporting FI has reason to believe that the customer does not possess identity documents; and (iii) it is unreasonable in view of the customer's age or state of health to require him/her to obtain identity documents. Nevertheless, even in these cases, the Reporting FI must still obtain and register the identification data required by section 6 of the MLA by other means (MLR s.5). The FSA states that this exemption only applies in exceptional cases (e.g. when opening an account for an under-age person, such as a child about to be christened), but it does not apply to customers who undertake large transactions on a regular basis (MLR s.5; Circular 9/2004 s.2.4).

Timing of verification

218. Norway has implemented measures that require prompt identification of customers. When establishing a customer relationship, the Reporting FI must verify the customer's (but not the beneficial owner's) identity at the time the customer is able to use the Reporting FI's services (i.e. in connection with opening an account or being issued a payment card) (MLR s.2). The FSA interprets this to mean that customer identification must take place at the earliest point in time at which the customer is able to make use of the Reporting FI's services (regardless of whether the customer actually avails himself/herself of that opportunity). Consequently, customer identification cannot be postponed until the customer makes the first payment into the account or uses the payment card for the first time (Circular 9/2004 s.2.2). The following chart sets out specific examples of when a customer relationship is considered by the FSA to be established (thereby triggering the obligation to identify the customer).

CUSTOMER IDENTIFICATION: WHEN THE OBLIGATION IS TRIGGERED AND WHO IS RESPONSIBILE FOR FULFILLING IT		
TYPE OF FINANCIAL ACTIVITY	WHEN THE CUSTOMER RELATIONSHIP HAS BEEN ESTABLISHED / CDD TRIGGERED	WHO MAY IDENTIFY THE CUSTOMER
Deposit accounts	• When the account agreement is entered into	• Reporting FI
Sales finance (i.e. motor vehicle sales)	• When the customer takes possession of the capital item (at the latest)	• Reporting FI • Dealer/supplier of the capital good[64]
Customer applying for current account credit accessed by a	• When the account credit agreement is entered into if the customer appears in person at the premises	• Reporting FI • Dealer/supplier (if the customer

[63] The exceptions set out in paragraphs (b), (c) and (d) correspond with the exceptions set out in Article 3, No.3-4 of the EU's 2nd Money Laundering Directive (2001/97/EC).

[64] See also MLR s.8

card	of the dealer/supplier; or • When the customer receives the card by registered mail	appears in person at the premises of the dealer/supplier) • Norway Post (if the customer receives the card by registered mail)
Customer applying for a payment/credit card which is unrelated to a concrete purchase of a product/service	• When the customer receives the card by registered mail	• Reporting FI • Norway Post
Company card issued to the customer on the basis of his/her employment contract	• When the card is issued to the customer	• Reporting FI • Company/organisation employing the customer
Subscription of financial instruments	• When the customer's Central Securities Depository Account is established and before the customer makes any payments or any securities are transferred the account (i.e. no later than when the decision is made to allot securities to the customer)	• Reporting FI
Subscription of financial instruments over the internet	• Before the securities are transferred to the customer's Central Securities Depository account	• Reporting FI
Corporate finances services	• When a verbal/written agreement is entered into accepting an assignment (including counselling or preparing offer documents and prospectuses), arrangement, guarantee provision or other services is entered into (i.e. before/upon signing the mandate agreement	• Reporting FI (the Investment firm concerned)

219. In the case of occasional customers making a transaction involving NOK 100 000 (EUR 12 100/USD 15 800) or more, the customer must also be identified. If the transaction amount is not known at the time it is carried out, the customer must be identified as soon as the Reporting FI becomes aware that the threshold has been exceeded (MLA s.5).

Failure to satisfactorily complete CDD

220. Except where there is an exemption from having to perform customer identification (paras 213 to 215 above), if customer identification cannot be carried out or if identification documents believed to be incorrect cannot be verified, then the Reporting FI must refuse to establish a customer relationship or carry out a transaction (MLR s.9). However, there is no obligation not to open an account, not establish a business relationship, consider making an STR or (in the case of existing customers) terminate the business relationship in instances where the beneficial owner cannot be identified or information concerning the purpose and intended nature of the business relationship cannot be obtained. This is because there is no obligation to collect this information in the first place.

Existing customers

221. There are no legal or regulatory measures in place as to how Reporting FIs should apply CDD measures to their existing pool of customers. There is no legal requirement for a customer's identity to be re-verified upon a subsequent enlargement of the customer relationship in the same institution (i.e. the opening of a new account, writing a new insurance policy, etc). However, the FSA requires the Reporting FI to be certain of the customer's identity in connection with any customer care implementation or any enlargement of the customer relationship (Circular 9/2004 s.2.7.1).

222. Norway cannot confirm that all Norwegian account holders have been identified. Since 21 November 1975, there has been an obligation to register the name, address, date, month and year of birth for each customer (according to bank legislation) and the customer's 11-digit personal identity number (according to tax legislation). Since 1 January 1992, the obligation to register the customer's

11-digit person identity number has also been an obligation in the banking legislation. For the last eight years, Norway has been working on a risk-based approach to re-verify the identification on existing account holders and bring existing accounts that were opened prior to 1975 and 1992 in line with current customer identification obligations; however, the work is still ongoing.

223. In addition to the deficiencies in the law itself, the effectiveness of the current customer identification measures is unclear. In February 2004, the FSA conducted thematic inspections of 12 banks and finance companies to determine their level of compliance with AML legislation, including random checks of customer identification files. The inspections revealed substantial defects in the procedures for identifying legal persons that mainly related to identity verification of sub-managers and obtaining original registration certificates or certified copies. The bulk of the institutions had a defect percentage exceeding 50%. The quality of identity verification of physical persons also varied widely. Flaws mainly related to illegibility of copies and/or the absence of a "certified copy" stamp. In three of the institutions, it was not even possible to verify that identity controls had been carried out correctly. The inspections also showed that the institutions had a low level of awareness concerning who is entitled to sign on behalf of a legal person and in what circumstances. None of the institutions were able to document written guidelines stating when a signature should be required or when it is acceptable for a procurist or chief executive to sign on behalf of a company. Most of the institutions employed internal guidelines stating that permanent made-up customer numbers (i.e. customer numbers that are not taken from the official Norwegian registers) should only be assigned to foreign companies, to some degree to foreign nationals, and to businesses not subject to registration. However, flawed follow-up and control routines relating to these guidelines were brought to light at some institutions. The results of these thematic inspections do raise some preliminary concerns about how compliant Norwegian financial institutions are with these requirements; however, as only 12 such inspections have been conducted on the Norwegian financial sector, it is premature to draw conclusions on this basis about the overall effectiveness of the system.

Recommendation 6

224. Norway has not implemented any AML/CFT measures concerning the establishment of customer relationships with politically exposed persons (PEPs).

Recommendation 7

225. Norway has not implemented any AML/CFT measures concerning the establishment of cross-border correspondent banking relationships.

Recommendation 8

226. Norway does not allow non-face-to-face business to be established. Reporting FIs are obligated to verify the customer's identity at the time the customer relationship is established, regardless of the amount involved and regardless of whether the services are provided with or without face to face contact (Circular 9/2004 s.2.7.1). The general rule is that the customer's identity must be verified by the customer personally attending at the Reporting FI itself, or at an agent or outsourcee. The Reporting FI must verify that the photograph and signature appearing in the customer's identity document match the appearance and signature of the customer (MLA s.5; MLR s.8). However, there are two exceptions to this requirement.

227. The first exception is if a personal appearance constitutes a major inconvenience for the customer when it would be extremely burdensome for the customer to do so (MLA s.5). Examples include: (i) when the customer is unable to travel due to illness, handicap or similar situation; (ii) the customer is in prison; or (iii) the geographical distance may bring the excepting provision into play. If such a "major inconvenience" exists, the FSA recommends that the reporting entity should consider the feasibility of visiting the customer to conduct identity verification; however, this is not a requirement. In any event, the Reporting FI is still obligated to conduct satisfactory verification of the

customer's identity, although it may do so through other means than those prescribed by the legislation (Circular 9/2004 s.2.7.2.1).

228. The second exception is if a personal appearance may not be practicable because, for instance, the Reporting FI does not have a branch network, offers its services electronically or if the customer (natural or legal) resides abroad (Circular 9/2004 s.2.7.2.2 and 2.7.2.5). Where such non-face to face business relationships or transactions are conducted, the Reporting FI may outsource its customer identification and verification obligations. In this context, while there is no face-to-face contact with the Reporting FI, there remains face-to-face contact between the customer and the outsourcee. In an outsourcing agreement, the Reporting FI relies on another Reporting FI, other entity that has reporting obligations under the MLA (see MLA s.5) or a foreign entity with AML/CFT reporting obligations (the Outsourcee) to identify and verify customer's identity. To qualify as outsourcees, foreign entities must meet requirements corresponding to FATF's revised recommendations and be subject to a supervisory arrangement of EEA standard (Circular 9/2004 s.2.7.2.5).

229. Outsourcing agreements must be in writing, and may be of a general or case-by-case nature (MLR s.8; Circular 9/2004 s.2.7.2.2). Although the Outsourcee is subject to the obligations set out in the ML Act, the Reporting FI remains responsible for ensuring that the Outsourcee: (i) conducts the customer identification and verification properly (including to obligation to verify the customer's identity through a personal appearance at the Outsourcee's premises); (ii) maintains proper records of the customer identification information (next to the copy / information to be sent and to be kept by the reporting FI); and (iii) properly trains its employees in recognising transactions that may be related to money laundering or terrorist financing (MLA s.4-5; MLR ss.8, 10 and 16; Circular 9/2004 s.2.7.2.2). The agreement must specify the following:

(a) When verifying the customer's identity, the Outsourcee shall: (i) make a copy of the identity documents; (ii) stamp each copy with "certified true copy"; (iii) endorse them with the name in block capitals of the staff member who has performed the identity verification; (iv) sign for having performed the identity verification; and (v) send this material to the Reporting FI (MLR s.8, Circular 9/2004 s.2.7.2.3). The Reporting FI is obligated to retain this data (MLR s.15). Having noted that the quality of copies of identity documents varies, the FSA now emphasises that the photograph, stamp, name and signature shown in copies must be easily legible (Circular 9/2004 s.2.7.2.3).

(b) The management board of the Reporting FI retains responsibility for the activity that is outsourced and must have established guidelines for the outsourcing.

(c) The outsourcing agreement must provide the necessary basis for allowing supervisory authorities to access information, inspect and supervise the Outsourcee in the same way as when the Reporting FI itself performs the activities in question.

(d) The activity to be outsourced must be stated. The agreement must entitle the Reporting FI to instruct the Outsourcee and to audit the outsourced activity.

(e) The Reporting FI itself must have the competence to assess whether the Outsourcee is performing the assignment satisfactorily.

(f) The Reporting FI shall throughout have the opportunity to identify and control risks associated with the outsourcing of assignments.

(g) The Reporting FI shall have a plan for resolving problems which may arise should the Outsourcee be unable to carry out the assignment.

(h) The Reporting FI must secure a reasonable right to terminate the agreement under satisfactory conditions until an alternative solution has been established (NOU 2001:23 on Financial institutions' activity, chapter 5, p.28-30).

230. Customer verification obligations are often outsourced to Norway Post (MLA s.4; Circular 9/2004 s. 2.7.2.5). Norway Post refers to this method of customer identification as "Personal

Collection with Receipt" (PUM). The PUM method of receipt and identification verification works as follows. The Reporting entity sends a letter to the customer by registered first-class mail. When the letter is collected, the recipient (customer) goes to an office of Norway Post and confirms receipt of the letter with his/her signature. A photocopy must be taken of the customer's proof of identity.[65] Norway Post's customer service personnel confirm the handover of the letter with their signature and name in capitals and a "certified copy" stamp. A copy of the identity document is sent to the Reporting FI in a closed envelope. The Reporting FI must retain these documents (which are proof that identity verification has been performed) as required by section 15 of the MLR. The Reporting FI retains full and complete responsibility for ensuring that identity verification is carried out in a proper manner in compliance with the money laundering legislation.

231. Norway Post itself has outsourced the provision and performance of various financial (and postal) services, including the PUM identity verification, to shops in the retail market (Post Office in Shop). The FSA has no objections to such outsourcing, provided that this activity is operated in accordance with the AML legislation and guidelines. Only shop staff with proper training (corresponding to that required by MLR s.16) may provide such services (Circular 9/2004 s.2.7.2.5). Investment firms and securities funds management companies can also engage in outsourcing. Such agreements are also regulated (Circular 9/2004 s.2.7.2.4).

3.2.2 Recommendations and Comments

232. Norway should implement the following missing elements of Recommendation 5 as a matter of priority:

(a) There should not be an exemption from customer due diligence if the reporting FI has actual suspicion that a transaction is connected with ML/TF (i.e. there should not be an exemption from MLA section 5 para.3).

(b) There is no requirement for a Reporting FI to re-perform customer identification when it has doubts about previously obtained identification data. Presently the obligation is only to verify data if the information contained in the presented documents is on its face incorrect (MLR s. 8).

(c) Although there are extensive requirements for identification of a customer that is a legal person, there is no requirement for a Reporting FI to verify that an individual purporting to act on behalf of that legal person is in fact so authorised.

(d) There is no definitive duty imposed on a Reporting FI to check if the customer is acting on behalf of another person. Currently the duty is a contingent one (i.e. to check only if it has reasons to suspect this to be the case).

(e) There is also no duty imposed to check the corporate or ownership structure behind a customer who is a legal person, by identifying, for example, the controlling shareholder or operating mind behind the customer

(f) There is no duty imposed to inquire about the purpose and nature of the business relationship vis-à-vis the Reporting FI itself.

(g) Reporting FIs are not required by law to conduct ongoing due diligence on their business relationships.

[65] The previous Money Laundering Regulations allowed Norway Post to make a written copy of the relevant data contained in the identity documents. Because these requirements are new, there is a transitional period to allow Norway Post time to bring its procedures into line with the MLR. During the transitional period, the FSA may approve a written copy to be made of the relevant data contained in the customer's identity documents, provided that the customer sends a copy of the identity document in question to the Reporting FI and the Reporting FI verifies that the photocopy matches Norway Post's written copy. The Reporting FI is then required to retain this photocopy under section 15 of the MLR (Circular 9/2004 s.2.7.2.5).

(h) There are also no rules governing the CDD treatment of existing customers.

233. The transition from pure identification to CDD has not been made in Norway. The legal and regulatory system of Norway only sets forth measures to be taken to identify customers—which means that Norway is only in compliance with those elements of Recommendation 5 that implement customer identification. Any other element, going beyond the initial establishment of the customer relationship is not regulated. The assessors did not find any evidence that CDD is implemented on a voluntary best practice level by FIs. Norway should implement the missing elements of Recommendation 5 as a matter of priority.

234. The requirements regarding customer identification are primarily focused on the banking sector. However, this one-size-fits-all approach may, in some cases, not take into account the normal conduct of business in non-bank sectors. Norway is recommended to reassess the existing identification requirements and procedures and consider developing measures that are more tailored to the business practices of the non-bank financial sectors.

235. Recommendation 6 and Recommendation 7 have not been implemented at all. Norway should implement both Recommendations as a matter of priority. Recommendation 8 is fully observed.

3.2.3 Compliance with Recommendations 5 to 8

	Rating	Summary of factors underlying rating
R.5	PC	• Although Norway has implemented customer identification obligations, it has not implemented full customer due diligence (CDD) requirements. • There are extensive rules on the identification of a customer who is a legal person and also of an individual acting for that legal person. However, there is presently no legal requirement under the MLA or MLR for a Reporting FI to verify that the individual is duly authorised to act for the legal person. • If a Reporting FI knows or has reason to believe that a customer is acting as a (legal) representative of another, on behalf of another, or that another person owns the asset that is the subject of a transaction, the FI is required to identify that other person (MLA s.6). Other than this, there is no other requirement to identify a beneficial owner within the meaning of the FATF Recommendations (i.e. the natural person(s) who ultimately owns or controls a customer and/or the person on whose behalf a transaction is being conducted, and incorporating those persons who exercise ultimate effective control over a legal person or arrangement). • Reporting FIs are not legally required to actively inquire if the customer is "fronting" for any other person in respect of an account or a transaction (for instance, by asking as a routine part of the account opening procedure whether the account holder is acting on behalf of another person). • Reporting FIs are also required to obtain information relating to the shareholding or any corporate group behind a customer who is a legal person. • There is no obligation on the Reporting FI to inquire about the purpose and nature of the business relationship vis-à-vis the Reporting FI itself, or to conduct ongoing due diligence on the business relationship in that regard. • There is no enhanced CDD legislation for higher risk categories of customers. Nor does Norwegian legislation provide for any simplified or reduced CDD measures. • There is no obligation not to open an account, not establish a business relationship, consider making an STR or (in the case of existing customers) terminate the business relationship in instances where the beneficial owner cannot be identified or information concerning the purpose and intended nature of the business relationship cannot be obtained. This is because there is no obligation to collect this information in the first place. • There are no legal or regulatory measures in place as to how Reporting FIs should apply CDD measures to their existing pool of customers. There is no legal requirement for a customer's identity to be re-verified upon a subsequent enlargement of the customer relationship in the same institution (i.e. the opening of a new account, writing a new insurance policy, etc).
R.6	NC	• Norway has not implemented any AML/CFT measures concerning the establishment of

		customer relationships with politically exposed persons (PEPs).
R.7	NC	• Norway has not implemented any AML/CFT measures concerning establishment of cross-border correspondent banking relationships.
R.8	C	• Recommendation 8 is fully observed.

3.3 Third parties and introduced business (R.9)

3.3.1 Description and Analysis

236. ***Recommendation 9:*** Under Norwegian law, Reporting FIs cannot rely on the identity verification performed by another Reporting FI—even if it is part of the same financial group. However, a Reporting FI may enter into an outsourcing agreement with other Reporting FIs within the group whereby the latter perform identity verification. Additionally, Reporting FIs that belong to the same financial group may verify a customer's identity jointly, provided that the customer relationships in question are established simultaneously. In such cases, each Reporting FI within the financial group must retain a copy of the identity documents. However, identity verification that was carried out previously by another Reporting FI—whether within or outside of the same group—cannot be taken as a basis when establishing customer relationships (Circular 9/2004 s.2.7.1). Norwegian legislation does not allow for any other types of introductory business to take place. In all cases, the customer must either appear in person at the offices of the Reporting FI so that the mandatory identification check can be conducted (MLA s.5). Alternatively, the Reporting FI can outsource the mandatory identification check to another Reporting FI (MLR s.8).

237. In the domestic context, these rules would typically work as follows. Assume that a natural person living in Norway is a client of a Norwegian bank that has a commercial alliance with a Norwegian securities firm. If the client wants to conclude a securities transaction with the securities firm, the securities firm cannot rely on customer identification performed by the bank (even though they have a commercial alliance). The securities firm (or its outsourcee) must perform the mandatory identification check, which includes having the client appear in person (Circular 9/2004 p.19).

238. In the context of conducting business internationally, these rules work as follows. If a natural person (who lives in Germany) telephones a Norwegian bank (that is located in Norway and has no prior relationship with the Norwegian) and asks to open a bank account in the Norwegian bank in Norway, the Norwegian bank can fulfil its customer identification obligations by entering into an isolated or general outsourcing agreement with a foreign reporting entity. The foreign entity must meet requirements corresponding to the FATF's revised recommendation and must be subject to supervision according to EEA standards (Circular 9/2004 s.2.7.2.5). The same rules apply regardless of whether the natural person is Norwegian or not. If the natural person had been introduced to the Norwegian bank by its branch in Germany, then the German branch could carry out the identification check. Conversely, branches in Norway of foreign Reporting FIs may rely on the confirmation from the Reporting FI's head office that the customer's identity has been verified (MLR s.8). The same rules apply to all types of Reporting FIs (including the insurance and securities sectors) and Reporting BPs (including real estate agents and lawyers).

239. Similarly, in the context of conducting business domestically, customer identification obligations can be outsourced—although the outsourcee must be another Reporting FI or Reporting BP under the provisions of the Money Laundering Act (MLR s.8). Norway reports that, in practice, outsourcing agreements are usually entered into with other entities of the same financial group or with branches of Norway Post (*Posten Norge AS*) that following the PUM method for customer identification (see paragraphs 228 to 229 of the report).

240. Norway prohibits FIs from relying on third parties and introduced business in the absence of an outsourcing agreement. This applies both in situations where the business relationship is initiated either by the customer approaching a Norwegian FI directly (who then seeks a third party's assistance

to perform CDD) or where a foreign FI introduces a customer to the Norwegian FI and the foreign FI performs CDD according to the terms of an outsourcing agreement.

3.3.2 Recommendations and Comments

241. Recommendation 9 does not apply.

3.3.3 Compliance with Recommendation 9

	Rating	Summary of factors underlying rating
R.9	NA	• Recommendation 9 does not apply in the Norwegian context.

3.4 Financial institution secrecy or confidentiality (R.4)

3.4.1 Description and Analysis

242. ***Recommendation 4:*** The duty of confidentiality is imposed by statute on employees of savings banks, commercial banks, management companies for securities funds, the parent company in a financial group, insurance companies, and investment firms.[66] In essence, the duty is to maintain the confidentiality of any information concerning the customer which comes to the knowledge of the employee by virtue of their position. The duty is however not absolute and disclosure is permitted if this is specifically prescribed by law. Thus, the duty of confidentiality does not inhibit disclosure of information by reporting FIs to ØKOKRIM as required under MLA s 7. Section 11 of the MLA specifically provides that such disclosure to ØKOKRIM in good faith does not constitute a breach of the duty of secrecy and does not provide a basis for compensation or penalties.

243. S. 11 of the MLA allows reporting entities referred to in s. 4(1) of the MLA to exchange necessary customer data as a necessary step in investigating suspicious transactions before making a report to ØKOKRIM. S. 4(1) mentions financial institutions while s. 4(7) mentions insurance companies. This wording suggests that s. 11 does not extend to insurance companies. The FSA however has explained to the assessors that this is an oversight, and that the term financial institutions includes insurance companies under the Financial Institutions Act, and has adopted this policy in its Circular 9/2004. Although insurance companies are currently permitted to exchange confidential information with each other for the purposes of preventing insurance fraud (IA s.1-3), it is unclear what is the legal effect of such an interpretation by the FSA. All Reporting FIs are obligated to record the results of investigations (either in written or electronic form) (MLR s.10). These results must be made available to the FSA at all times (Circular 9/2004 s.2.10).

244. Board members and employees of the FSA are obligated to treat as confidential any information about a customer's affairs which may come to their knowledge in the course of their work (FS Act s.7). However, the duty of confidentiality does not prevent administrative agencies (such as the FSA and the Supervisory Council) from sharing information concerning natural/legal persons for the purpose of facilitating performance of the tasks assigned to the administrative agencies pursuant to statute, instructions or terms of reference. This includes providing information concerning the natural/legal person's connection with the administrative agency, decisions made and any other information that may be necessary to facilitate performance of the tasks assigned to the said agency pursuant to statute, instructions or its terms of reference (PAA). Nor does the duty of confidentiality apply when the FSA discloses information to the following entities as is necessary for the discharge of their statutory functions: authorised stock exchanges; authorised securities registers; and authorised clearing houses (FS Act s.7).

[66] SBA s.21; CBA s.18; SFA s.2-9; FIA ss.2a-13 and 13-14; IA s.1-3; and STA s.9-8.

245. When the FSA discloses information to foreign supervisory authorities, the duty of confidentiality does not apply provided that the information is disclosed subject to the following conditions. First, the information may only be used to perform supervision. Second, the information must be treated as confidential by the recipient. Third, the information cannot be passed on without the FSA's consent and then only for the purposes for which consent is given.[67] If the FSA receives information from a foreign supervisory authority, it may only pass it on with the consent of the foreign supervisory authority concerned and only for the purposes for which consent is given (Reg.1102 s.3).

246. ØKOKRIM may provide information that it receives concerning suspicious transactions to public authorities (other than the police) that are engaged in tasks associated with the prevention of terrorism or terrorist financing (MLA s.11). The police and Prosecution Authority (including the MLU) also have a duty of confidentiality (CPA s.61a). However, exemptions similar to the ones that apply to the administrative authorities apply when necessary for the prevention of crime and in relation to investigation.

3.4.2 Recommendations and Comments

247. Allowing a confidentiality override so that banks and finance companies can exchange information in the course of investigating suspicious transactions is sensible, but Norway should consider extending this to other types of Reporting FIs. The FSA's policy of extending the override to insurance companies is to be commended, but it may not go far enough. Given the irregularity as described, Norway should look into rectifying this. This Recommendation has been implemented. Secrecy provisions appear not to hinder the competent authorities exchanging information nationally or internationally. However, for the sake of giving other financial institutions the same tools to protect themselves against criminal abuse as banks have, Norway is recommended to allow them to exchange information. This recommendation does however not affect the rating.

3.4.3 Compliance with Recommendation 4

	Rating	Summary of factors underlying rating
R.4	C	• Recommendation 4 is fully observed.

3.5 Record keeping and wire transfer rules (R.10 & SR.VII)

3.5.1 Description and Analysis

248. ***Recommendation 10:*** Reporting FIs are obligated to retain copies of any documents used to verify the customer's identity. These documents must be endorsed with "certified true copy" and the signature of the person who carried out the customer identity verification (MLR s.15). The date of identity verification should also be indicated (Circular 9/2004 s.2.15). When establishing a business relationship or when performing single transactions, Reporting FIs must record the following identification information on customers (including any person that the customer is acting on behalf of, or who owns the asset that is the subject of the transaction):

(a) Full name or name of company;

(b) Personal identity number, organisation number, D-number[68] or, if the customer has no such number, another unique identity code;

(c) Permanent address;

(d) Reference to proof of identity supporting the identity of verification; and

[67] FSA s.7; Regulation no.1102 of 30 November 1998 concerning exchange of information with supervisory authorities from countries within and outside the EEA area (Reg.1102) ss.1-2.

[68] A five-digit "D-number " is assigned to foreign nationals who do not hold a Norwegian personal identity number who wish to register with the Brønnøysund Register Centre.

(e) Any other data required pursuant to regulations issued by the Ministry (MLA s.6 and 8).

249. The Reporting FI must ensure that the information recorded in relation to a transaction/establishing a business relationship can be connected to the corresponding information about the customer relationship (MLA s.6).

250. Both the documents used to verify the customer's identity and the recorded customer identification information must be retained for five years after termination of the customer relationship or after the transaction is carried out (MLA s.8; MLR s.15). However, information that is relevant for the annual accounts of the Reporting FI (i.e. information related to transactions carried out by banks and other reporting entities) must be kept for ten years.[69] If a Reporting FI has conducted further examinations of a transaction to confirm/disprove a suspicion of money laundering or terrorist financing, any documents relating to those transactions must also be retained for five years after the transaction is carried out. These documents must be destroyed within one year after expiry of the retention period (MLA s.8).

251. Reporting FIs are required to make their accounting records available to the supervisory authorities. This includes providing assistance free of charge, such as making available the equipment and software needed to verify the accounts. The accounting material shall at the request of the supervisory authorities be presentable on paper for up to 3½ years after the end of the accounting year (Loose-leaf Regulation No.1156 of 16 December 1992 (LLR) s.5-4**).** All of this information must be made available to the supervisory authorities as required.

252. Reporting FIs are obligated to store their records in a satisfactory manner. Documents must be secured against unauthorised access (MLR s.15). Reporting FIs must also maintain their records in such a way as to ensure that the documents do not lose their evidentiary value (MLR s.15). Consequently, documents that are physically retained must be stored against fire, theft, frost, flooding and other external influences (Circular 9/2004 s.2.15). Data that is electronically retained must be stored in an easily accessible location to permit checking during the period of storage. It must be organised in a manner that permits efficient follow-up of the accounts and the documentation. It should also be properly secured to prevent damage and alteration. All data should be easily legible directly with the aid of a computer screen/reading machine throughout the period of storage (LLR ss. 5-3 and 5-4).[70] The information must be available on a timely basis. Consequently, storage must be systematic to ensure that the appropriate document can actually be retrieved (Circular 9/2004 s.2.15). For instance, the Reporting FI must ensure that there is a unique connection registered between the customer relationship and the customer identification information (either through an account number or in another manner) (MLA s.6).

253. Although the record-keeping provisions are sufficient on their face, the level of compliance by financial institutions (and thus the effectiveness of the measures) is unclear. In February 2004, the FSA conducted thematic inspections of 12 banks and finance companies to determine their level of compliance with AML/CFT legislation, including the rules related to record keeping (s.15 MLR). The inspections showed that only two institutions had routines that ensured full traceability of identity documents and were able to link the identity documents to an agreement established with the customer enabling full signature verification. Other flaws consisted mainly of incomplete transcripts, illegible copies, and instances where identity documents were only retained by another reporting entity where the verification had been carried out. Although the results of these thematic inspections do raise some preliminary concerns about how effectively record keeping measures have been implemented, only 12 such inspections have been conducted on the Norwegian financial sector. Consequently, it is premature to draw conclusions on this basis about the overall effectiveness of the system. Norway has however

[69] Act No.73 on Bookkeeping (19 November 2004) s.13.

[70] Although the Loose-leaf Regulations themselves apply to "accounting records", the same principles apply to the retention of information collected pursuant to the MLA and MLR (MLR s.15).

given the assurance that the results of the thematic inspections conducted in February 2004 were not representative of the overall state of the financial sector's compliance with current Norwegian AML/CFT rules.

254. ***Special Recommendation VII:*** In most respects, SR VII has not been implemented. For wire transfers being conducted by permanent customers at a Reporting FI, the full originator information (i.e. name, account number/unique reference number and address of the originator) will be obtained and maintained (MLA s.6). This information is verified by checking the veracity of the customer identification documents on their face (i.e. ensuring that the photograph and signature on the document match the person, ensuring that the document is valid, etcetera). (For more information on how Reporting FIs verify customer identification documents, see paragraphs 205 to 211 of this report.)

255. There is no legal obligation to include full originator information in the message or payment form that accompanies a cross-border or domestic wire transfer. Although Section 18 no.3 of the MLA does provide a legal basis to establish rules concerning which originator data shall accompany a transaction in the payment chain, such regulations have not yet been adopted. Norway reports that it has not done so because it is awaiting further clarification from the FATF on SR VII before it enacts regulations. In this regard, it should be noted that the FATF is in the process of working on a revised Interpretative Note to SR VII.

256. The MLA does not contain any obligation to collect or maintain this information for an occasional customer who is ordering a wire transfer that is below the threshold of NOK 100 000 (EUR 12 100/USD 15 800) unless the reporting entity suspects that the transaction is associated with terrorism or ML/FT (in which case, the reporting entity must request proof of identity, regardless of whether the customer is an occasional or permanent one (MLA s.5 para.4)). This threshold is significantly higher than the USD 3 000 threshold currently permitted by SR VII. In practice, Norwegian banks choose not to offer wire transfer services to occasional customers. Consequently, occasional customers must use the services of Norway's one authorised MVT service provider. Although not legally obligated to do so, this MVT service provider does appear to obtain and retain full originator information on its customers (i.e. name, unique reference number and address).

257. However, the new Currency Transaction Register Regulations (CRR) (which came into force on 1 January 2005) require financial institutions (i.e. savings banks, commercial banks, finance companies and mortgage companies) to report all incoming and outgoing cross-border transactions (regardless of the amount) to the Currency Transaction Register. If the transaction exceeds NOK 100 000 (EUR 12 100 / USD 15 800), the report must also specify the purpose of the transaction.[71] The same obligations apply to MVTS providers. As well, financial institutions that are authorised to carry out foreign exchange activity must submit reports to the Currency Transaction Register concerning the following types of foreign exchange transactions that are made in cash or monetary instruments (i.e. banknotes, coins, bills of exchanges, cheques, and other drafts or letters of credit conferring the right to payment in Norwegian or foreign banknotes and coins):

(a) Domestic foreign exchange transactions equal to or exceeding NOK 5 000 (EUR 600/USD 790); and

(b) Transfers equal to or exceeding NOK 25 000 (EUR 3 000/USD 4 000) that are made with an international payment card. For credit card transactions under this limit, the aggregate sums of transactions must be reported to the Currency Transaction Register on a monthly basis per credit card per customer.

The information in the Currency Transaction Register is directly accessible by the MLU, law enforcement, tax authorities, the National Insurance Administration and customs authorities.

[71] CRR as described in the Note by Norway to the OECD Working Party No. 8 on Tax Avoidance and Evasion (CTPA/CFA/WP8(2004)25/CONF).

258. Reports to the Currency Transaction Register shall contain: the identification number of the financial institution making the report; the customer's name, address, postal code, country and identification number; and the amount and type of currency (CRR). The financial institution making the report shall advise both the person sending the transaction and the person receiving the transaction that a report is being made (CRR). The report must be made within five days of the transaction taking place. Between 140 and 160 enterprises are obliged to report to the Currency Transaction Register. The CRA has only recently come into force; however, Norway expects that the Currency Transaction Register will receive daily reports on 50 000 to 60 000 transactions. Norway also estimates that reports on an additional 50 000 transactions based on aggregated sums will also be reported each month.

259. For domestic wire transfers, there is no obligation to maintain full originator information in such a manner that: (i) it can be made available to the beneficiary financial institution and to competent authorities within three business days of receiving a request; and (ii) domestic law enforcement authorities can compel immediate production of it. Originator information relating to all cross-border transfers is filed in the Currency Transaction Register.

260. There is no obligation on Reporting FIs to ensure that non-routine transactions are not batched where this would increase the risk of money laundering or terrorist financing. Nor are there obligations on intermediary Reporting FIs in the payment chain to maintain all of the required originator information with the accompanying wire transfer. As well, there are no obligations on beneficiary Reporting FIs to adopt risk-based procedures for identifying and handling wire transfers that are not accompanied by complete originator information. Finally, there are no sanctions for breaching many of the obligations under SR VII because many of the obligations themselves have not been implemented. There are, however, sanctions for not complying with the Currency Register Act and Regulations.

3.5.2 Recommendations and Comments

261. Norway should continue taking measures to ensure that Reporting FIs are effectively implementing record-keeping provisions. This includes imposing sanctions for failing to comply where appropriate. SR VII has not been implemented in most respects. Norway should implement the provisions of SR VII as soon as possible.

3.5.3 Compliance with Recommendation 10 and Special Recommendation VII

	Rating	Summary of factors underlying rating
R.10	C	• Recommendation 10 is fully observed.
SR.VII	NC	• The MLA does not contain any obligation to collect or maintain this information for an occasional customer who is ordering a wire transfer that is below the threshold of NOK 100 000 (EUR 12 100/USD 15 800) unless the reporting entity suspects that the transaction is associated with terrorism or ML/FT (in which case, the reporting entity must request proof of identity, regardless of whether the customer is an occasional or permanent one (MLA s.5 para.4)). This threshold is significantly higher than the USD 3 000 threshold currently permitted by SR VII. • There is no legal obligation to include full originator information in the message or payment form that accompanies a cross-border or domestic wire transfer. • For domestic wire transfers, there is no obligation to maintain full originator information in such a manner that: (i) it can be made available to the beneficiary financial institution and to competent authorities within three business days of receiving a request; and (ii) domestic law enforcement authorities can compel immediate production of it. • There is no obligation on Reporting FIs to ensure that non-routine transactions are not batched where this would increase the risk of money laundering or terrorist financing.

		• There are no obligations on intermediary Reporting FIs in the payment chain to maintain all of the required originator information with the accompanying wire transfer. • There are no obligations on beneficiary Reporting FIs to adopt risk-based procedures for identifying and handling wire transfers that are not accompanied by complete originator information. • There are no sanctions for breaching many of the obligations under SR VII because many of the obligations themselves have not been implemented.

Unusual and Suspicious Transactions

3.6 Monitoring of transactions and relationships (R.11 & 21)

3.6.1 Description and Analysis

262. ***Recommendation 11:*** Reporting FIs are required to conduct additional examinations of transactions that are suspected of being related to ML/FT (MLA s.7). Examples of circumstances that may trigger the obligation to make such examinations are that the transaction: (i) appears to lack a legitimate purpose; (ii) is unusually large or complex; (iii) is unusual in relation to the customer's habitual business or personal transactions; or (iv) is otherwise of an anomalous nature (MLR s.10). Section 2.10 of Circular 9/2004 provides additional elaboration (which is not exhaustive) on these triggering circumstances:

(a) A transaction that appears to lack a legitimate purpose may, for example, involve an assignment in which a sum of money is to move back and forth between different accounts within a given period, that the same amount is to move back and forth between different institutions in accordance with a given assignment, and that a sizeable sum is split into a number of smaller sums, but is reunited in a new account.

(b) A transaction that is unusually large or complex, or is unusual in relation to the customer's habitual business or personal transactions must be determined by assessing the customer's account and usual transaction patters. A transaction may be large in relation to one customer, but quite normal in relation to another. Consequently, Reporting FIs must apply their knowledge of the individual customer.

Whether a transaction is otherwise of an anomalous nature involves a concrete assessment of the individual case. Some examples might be:

(i) Rapid and extraordinary repayment of loans in cash;

(ii) A significant disparity between documented debt-servicing ability in terms of income, financial assets etc., and the amount owed and agreed repayment conditions (extraordinary repayment), may indicate money laundering;

(iii) Use of bank drafts that are repeatedly renewed;

(iv) Large-scale exchange of old banknotes that have become invalid;

(v) Use of unusual means of payment in relation to the underlying operation;

(vi) Large cash transactions; and

(vii) Use of payment cards to carry out an unusually large number of transactions over a short period.

263. Reporting FIs are also warned that foreign exchange operations (including foreign currency exchange and payment transfers to foreign countries) are particularly vulnerable to abuse for ML/FT purposes. Likewise, Reporting FIs are advised to pay special attention to business areas where there is little or no face-to-face contact with the customer. Reporting FIs are still responsible for fulfilling their investigative obligations even if the customer is conducting business through the internet or other electronic systems. As well, Reporting FIs are referred to the typologies information on the FATF's

internet website (Circular 9/2004 s.2.10). There is no other guidance by the authorities, except for non-cooperative countries and territories (NCCT) warnings (see the discussion of Recommendation 21 in paragraphs 263 to 264 below).

264. Credit institutions are obligated to establish electronic surveillance systems (by 1 January 2005) for the purpose of monitor their accounts on an ongoing basis to identify transactions that are suspected of being related to ML/FT (MLA s.15). This obligation applies to: (i) savings banks and commercial banks; (ii) finance companies licensed under chapter 3 of the FIA; (iii) branches of credit institutions (banks and finance companies) within the EU/EEA;[72] and (iv) Norwegian-registered branches or undertakings of foreign credit institutions (banks and finance companies) whose head office is in a state outside the EEA, and which are authorised by Norwegian authorities to engage in financing activity in Norway. Consequently, this obligation applies to financial service providers headquartered in countries outside the EU/EEA which have established such business in Norway (Circular 9/2004 s.2.12). The FSA may make exceptions from the obligation to establish electronic surveillance systems on a case-by-case basis (MLR s.12). Regardless of whether an electronic monitoring system is implemented, the transactions identified by such systems must be checked and followed up manually (i.e. investigated) before being reported to ØKOKRIM. Reporting FIs are also obligated to record the results of investigations (in written or electronic form) (MLR s.10) and make them available to the FSA at all times (Circular 9/2004 s.2.10).

265. ***Recommendation 21:*** One of the circumstances which may trigger a suspicion of ML/FT (and, therefore, an examination by the Reporting FI) is a transfer to/from a customer in a country or area lacking satisfactory measures against ML/FT (MLR s.10). The results of such examinations must be recorded (either in written or electronic form) and be made available to the FSA at all times (MLR s.10; Circular 9/2004 s.2.10). Additionally, Reporting FIs are warned to be alert to transactions with customers or institutions in countries with strict secrecy laws that offer high returns and tax exemptions (Circular 9/2004). The FSA also publishes and updates the FATF list of NCCTs on its website and advises Reporting FIs to consult the websites of both the FSA and the FATF (Circular 9/2004 s.2.10).

266. Where a country continues not to apply or insufficiently applies the FATF Recommendations, Norway is able to apply countermeasures. In response to an FATF decision, the Ministry of Finance can also impose special prohibitions or restrictions on the rights of Reporting FIs to establish customer relationships with or carry out transactions with natural/legal persons associated with countries or areas which have not implemented satisfactory AML/CFT measures (MLR s.14). Alternatively, the Ministry of Finance may impose a special, systematic obligation to report to the MLU transactions with or on behalf of natural/legal persons associated with countries or areas which have not implemented satisfactory AML/CFT measures (MLR s.13). Such a reporting obligation will be adopted by the Ministry of Finance in the form of a decision that will be published on the FSA's website, www.kredittilsynet.no, and communicated to reporting entities in other ways (Circular 9/2004 s.2.13). Nevertheless, Norway reports that it has applied countermeasures during the NCCT process by informing (through the FSA) all banks, finance companies, securities funds management companies and the central bank to consider (as a general rule) that all transactions to/from Norway and one of the countries on the NCCT list should be considered suspicious. In such cases, the Reporting FI had a duty to make further inquiries. When the country in question was removed from the NCCT list, the FSA advised Reporting FIs accordingly. Additionally, Norway has applied countermeasures to Nauru, the Philippines and Myanmar in accordance with FATF decisions. In the case of Nauru, financial institutions were requested to regard all transactions to/from Nauru as suspicious, and to make further examinations to confirm/disprove the suspicion. Further, financial institutions were requested to carry out special thorough customer identification before establishing business relations with companies in Nauru.

[72] Based on the principle of mutual recognition set out in the Consolidated Banking Directive (2000/12/EC), such credit institutions can establish branches in Norway provided they are authorised, and subject to supervision, by the authorities in their own state.

3.6.2 Recommendations and Comments

267. Recommendations 11 and 21 are fully observed.

3.6.3 Compliance with Recommendations 11 & 21

268. Norway is compliant with Recommendations 11 and 21.

	Rating	Summary of factors underlying rating
R.11	C	• Recommendation 11 is fully observed.
R.21	C	• Recommendation 21 is fully observed.

3.7 Suspicious transaction reports and other reporting (R.13-14, 25 & SR.IV)

3.7.1 Description and Analysis[73]

269. ***Recommendation 13 and Special Recommendation IV:*** Reporting FIs are obligated to report transactions to the MLU if there is any suspicion that the transaction is associated to the proceeds of crime (MLA s.7; MLR s.11). While the law itself does not specify what level of suspicion is required, the preparatory works indicate that the suspicion must relate to some facts or grounds. This is taken to mean that the required suspicion is lower than reasonable grounds; any grounds to suspect is sufficient. The reporting obligation applies to the proceeds of any crime, without restriction. Consequently, it applies to a concept of money laundering that is broader than the definition of money laundering in section 317 of the Penal Code (which does not include self-laundering) (MLA s.7). The reporting obligation also applies to transactions suspected of being related to terrorism or terrorist financing, including making funds available to a person/entity that commits/attempts to commit terrorist acts, an entity owned/controlled by such a person or any person/entity acting on behalf of/at the direction of such a person/entity. Norway confirms that this section is interpreted to include instances where there is any suspicion that there is a link to a terrorist organisation or terrorist financier. Moreover, Circular 9/2004 specifically refers Reporting FIs to FSA Circular 22/2003 on the handling of lists from the UN and FATF (dated 29 August 2003) as being one of the circumstances that may trigger a STR. Reporting FIs are also obligated to report suspicious transactions related to tax matters. However, as no cases have yet come before court, the courts have not yet interpreted this provision.

270. When forwarding an STR to the MLU, the Reporting FI must provide all essential data concerning the transaction and the suspicion (MLA s.7). This includes a description of the basis for the suspicion, information concerning the suspects and third parties involved (if any), account data (if any), data on the movements on the account, data on the nature and size of the transaction, whether the transaction has actually been carried out, to whom the funds are to be transferred and the origin of the funds. Relevant documents supplementing such information should be attached or forwarded as well (MLR s.11). A customer or third party shall not be informed that such information has been forwarded. All STRs must be reported using a standardised form that has been prescribed or approved by the MLU (MLR s.11) and is available on its website (www.okokrim.no) (Circular 9/2004 s.2.11). Reports must be submitted by post, fax or in a machine-readable form. If the data is transferred electronically, it must be coded or secured by other means to ensure confidentiality (MLR s.11). In Oslo, it is permissible to deliver the report to the FIU in person. Ordinary e-mail is not allowed because of the risk of information tapping (Circular 9/2004 s.2.11).

271. The AML/CFT reporting obligations for both apply to both completed and attempted transactions, regardless of amount. Additionally, Reporting FIs are not permitted to carry out any transaction if

[73] The description of the system for reporting suspicious transactions in s.3.7 is integrally linked with the description of the FIU in s.2.5, and the two texts need to be complementary and not duplicative.

identity documents are not produced, or there is reason to believe that the documents are not correct. However, if the institution regards the attempted transaction as being suspicious, it must carry out an examination of the transaction for the purpose of confirming/disproving the suspicion. If the suspicion cannot be disproven, the Reporting FI must submit a suspicious transaction report to the MLU. Likewise, the Reporting FI must submit an STR to the MLU if the customer's identity is in doubt (MLR s.9).

272. In 2001 and 2002, the number of STRs reported to the MLU increased (mainly as a result of increased reporting from the banking and insurance sectors). In 2002, reporting patterns in the banking sector underwent a noticeable change; the number of cash transactions for deposits/payments rose by 52.4% and cash withdrawals jumped by 72.4% (a notable increase from 2001). As well, reported transfers abroad increased by 141%. Norway has reason to believe that this increase could be viewed in connection with enhanced awareness of ML/FT. In 2003, the number of reports sent to the MLU by banks and insurance companies decreased; however, overall the number of reports received increased considerably over the previous year (mainly due to the establishment of new routines for receiving and registering reports from MVTS providers). The marked decline in the number of reports being received from commercial banks from 2002 to 2003 could be the consequence of a shift in ML methods (i.e. money launderers may be using other institutions or professionals that did not have AML/CFT obligations under the 2003 regime). Of all the reporting groups, banks (savings banks and commercial banks) and MVTS providers report the largest number of transactions suspected to be related to ML operations. Non-Norwegians, immigrants, asylum-seekers and refugees are represented in about 70% of the STRs received. Reports from MVTS providers represent an increasing percentage of the cases, and it seems as if immigrants, asylum-seekers and refugees make particular use of this service.[74] Cross border money transfers also increased noticeably in 2002. In many of these cases, cash deposits were made to the accounts just before the money was transferred. Non-Norwegians and immigrants have been represented in most of these reports. The following charts set out the number of STRs received by the MLU, broken down by source.

NUMBER OF STRs RECEIVED: BREAKDOWN BY SOURCE				
TYPE OF REPORTING ENTITY	2001	2002	2003	2004
Type of Reporting FI filing the STR				
Commercial bank	711	935	609	640
Savings bank	274	320	303	239
Insurance company	5	22	16	21
Stock brokers	1	0	3	5
Norges Bank	0	1	1	0
Brokerage firm	1	1	3	1
Credit card company	1	6	-	-
Money transfer services			2 513	4 115
Type of Reporting BP filing the STR				
Lawyers	0	0	0	17
Accountants	0	0	0	8
Authorised accountants	0	0	0	25
Real estate agents	0	0	0	4

[74] Money Transfer reports are reports of transactions through a special service that transfers cash abroad, without using the ordinary banking system.

273. The following chart sets out how much money was involved in the suspicious transaction reports, including how much Norwegian and foreign currency was involved.

TOTAL AMOUNT OF MONEY INVOLVED IN STRs						
Year	NOK	USD	EUR	GBP	SEK	DKK
2004	331 million	22.8 million	1.8 million	51 000	250 000	269 000
2003	628 million	23 million	1.9 million	64 000	443 000	475 000
2002	309 million	7.4 million	32 million	455 500	444 000	558 000
2001	637 million	540 million	473 000	297 000	487 000	105 000

274. The following chart sets out the types of transactions comprising the STRs received.

TYPES OF TRANSACTIONS COMPRISING STRs				
Type of transaction	2001	2002	2003	2004
Not registered	5	7	3	288
Opening accounts with banks. Cash – deposits/payments.	11	13	4	3
Change – large amounts	25	20	22	14
Travellers cheque/foreign currency cheque	7	7	5	4
Cheques	14	25	12	4
Transfer of money out of Norway	146	355	248	178
Domestic transfers	130	168	194	187
Transfer from abroad	31	48	33	22
Payments through the internet	0	2	4	3
Night safe	4	4	1	1
American Express / Money gram	6	4	2 507	4 110
Loans	16	27	26	11
Cash withdrawals	75	131	94	89
Cash deposits, debt payment etc.	320	497	415	366
Remittances	28	63	57	48
Purchase of foreign currency – payments in NOK	344	227	147	1012
Purchase of NOK – payments in foreign currency	33	48	10	55
Insurance	5	26	12	3
Payment card	1	8	4	1
Transaction by other bank services	2	4	2	2
Others	24	39	45	14

275. The MLU has received most of its STRs relating to money transfers from two main sources: one of the major Norwegian banks and the old MVTS provider that was previously authorised to conduct this sort of business in Norway. (The old MVTS provider no longer offers this service, but a new MVTS provider is now authorised to conduct this business in Norway.) In 2004, the MLU received 10 STRs from the major Norwegian bank, containing approximately 1 000 transactions. The average time for these to be reported was 15 days. The old MVTS provider sent the MLU 33 discs of STRs, containing a total of approximately 4 115 transactions. The average time for these to be

reported was 10 days. The remaining STRs received by the MLU in 2004 (approximately 1 000) greatly differed in the amount of time between the moment the transaction was undertaken and the time the transaction was reported (the time span varied from 3 hours to 1 year). The MLU does not have statistics concerning the average time for STRs to be reported after the transaction is performed; however, the high degree of variation is due to the very different nature of each case. Some transactions might be of a suspicious nature immediately, while others first become suspicious over time when it is possible to observe a certain pattern. The following chart sets out the size of transactions (in terms of monetary value) comprising STRs.

SIZE OF TRANSACTIONS COMPRISING STRs				
Size of the transaction	2001	2002	2003	2004
> 5 million NOK	24	36	42	12
< 5 million NOK	31	38	28	37
< 2 million NOK	37	50	52	91
< 1 million NOK	82	127	105	138
< 500 thousand NOK	301	480	344	470
< 100 thousand NOK	508	538	2 880	5 220
Not registered	9	22	8	114
TOTAL STRs RECEIVED	992	1 291	3 459	6 082

276. The following chart breaks down how many STRs are related to transactions to/from NCCTs. The majority of these are outgoing transactions (from Norway to the NCCT). The MLU explains that the extraordinary large increase in MVTS transactions from 2003 to 2004 between Norway and Nigeria is due to increasing numbers of Nigerian prostitutes operating in Norway. Prostitution could also partly explain the increase in the number of transactions between Norway and Ukraine.

NUMBER OF STRs RECEIVED INVOLVING NCCTs			
Country/Territory	2003	2004	2004 (old MVTS provider)
Nigeria	157	6	1 406
Cook Islands	0	0	0
Indonesia	4	1	4
Myanmar	0	0	0
Nauru	0	0	0
Philippines	56	52	51
Bahamas	0	0	0
Egypt	10	1	5
Guatemala	1	0	0
Ukraine	133	5	301

277. In general, there are some concerns about the effectiveness of the reporting system. For instance, (except for MVTS providers), the number of STRs being reported by non-bank financial institutions is very small and the number of STRs being reported by banks themselves is also decreasing. Additionally, there were some indications during the on-site visit that, in the past year, a MVTS provider had not been complying with its reporting obligations. The FSA has since taken action to correct this problem. Another effectiveness concern relates to the fact that, in general, banks seem to focus on transactions performed by foreigners as being suspicious, rather than focusing on the

nature and characteristics of the transactions themselves. There also appears to have been defensive reporting of STRs by the old MVTS provider (i.e. reporting of STRs without giving proper consideration to whether or not they are really suspicious).

278. ***Recommendation 14:*** According to the FSA, Reporting FIs and their employees are exempt from civil and criminal liability for breach of confidentiality when they report STRs to the FIU in good faith (MLA s.11). Consequently, filing an STR in good faith cannot be used as a basis for bringing legal action against either the Reporting FI or its employees (Circular 9/2004 s.2.11). "Tipping off" a customer or any third party in connection with reporting a STR to the MLU is prohibited (MLA s.7). Neither the customer nor any third party should be informed that such investigations are in progress (MLR s.10). Nor shall the customer or any third party be informed that information has been provided to ØKOKRIM (MLA s.7). Although in some cases it may be natural to ask the customer questions to confirm or disprove a suspicion, the obligation is to ensure that the customer is not made aware that investigations are in progress. Consequently, in such situations, the Reporting FI should proceed with caution (Circular 9/2004 s.2.10)**.** Norway reports that the prohibition against tipping off applies to the Reporting FI as well as its directors, officers and employees (whether permanent or temporary).

279. *Additional elements:* Reporting STRs to ØKOKRIM is the responsibility of a senior manager who has been assigned special responsibility for this task (i.e. the compliance officer) (MLA s.13). Norway reports that the identity of other employees (i.e. the person who initially formed the suspicion about the transaction) is kept confidential. No statutory legislation exists to protect the senior manager who bears this responsibility; however, only authorised persons at ØKOKRIM have access to the database containing this information. The name of the compliance officer does not appear in the reports that are sent to the police districts. Nevertheless, it has come to ØKOKRIM's attention that, in a few cases, situations perceived as threatening for bank personnel have occurred. Generally, such threats are directed towards the counter staff—although occasionally, the person responsible for AML measures is threatened. The assessors were told that in 2002, an informal survey was carried out with the largest banks in Norway to learn more about possible security problems**.**

280. ***Recommendation 25 (Guidelines and feedback from supervisors):*** The FSA has issued detailed guidance to Reporting FIs concerning how to comply with the reporting obligations. Circular 9/2004 contains specific details concerning: (i) what types of activity may be suspicious; (ii) how to submit an STR to the MLU; (iii) the rationale for implementing electronic systems to monitor accounts; (iv) transactions related to countries that insufficiently apply AML/CFT measures; (v) prohibitions and restrictions on the right to establish customer relationships with persons from countries that insufficiently apply AML/CFT measures; and (vi) how to obtain further information and assistance concerning these issues (Circular 9/2004 s.2.10 to 2.14). Despite the guidance given 70% of all STRs are based on transactions made by non-Norwegians. It seems that the only real indicator or typology that has made any impact within the reporting community is the fact that a non-Norwegian is performing a transaction. It does not seem that those STRs should not have been made, which leads however to the conclusion that there is a potential for other types of STRs to be reported if only the employees of the reporting institutions had been guided to focus not only on the customer, but also on the nature of the transactions.[75] Norway's initial experience with its new electronic monitoring system for banks and finance companies is a pattern of reporting that focuses more on the nature of the transaction. This system will ensure that institutions focus on a wide range of red-flag indicators and not just the nationality of the customer.

281. ***Recommendation 25 (Guidelines and feedback on the reporting obligation from the FIU):*** In addition to answering daily telephone inquiries, the MLU performs lectures for reporting entities (i.e. banks, auditors and lawyers). Course and seminar activities have increased in 2003 and 2004 due to

[75] Norway reports that, in recent months, this focus has changed as a result of the new electronic surveillance system which was introduced in Norway on 1 January 2005.

the implementation of the new Act. On average, about two external courses/seminars per month are being provided. The MLU also sends some specific feedback to Reporting FIs. Upon receipt of the STR, the MLU sends a computer printout with information about the reference number to the financial institution. After making its inquiries, the MLU normally informs the Reporting FI of the decision that was taken, and (if applicable) of the police district or foreign unit investigating the case. However, this has not been a consistent practice in the last years. The Reporting FI should also receive transcripts of legal decisions; however, this has not been followed up lately. Previously, Reporting FIs received a report every six months about the current status of all the STRs that the Reporting FI had reported; however, this is no longer the practice. Until 2004, the MLU sent quarterly reports to reporting entities; however, this practice was stopped due to a lack of resources. Norway reports, however, that the practice of sending quarterly reports recommenced as of 1 January 2005. The MLU also had a tradition of giving feedback to Reporting FIs/BPs through a Contact Forum (biannual meetings with representatives from these entities). The Contact Forum discussed issues such as feedback, suspicious transactions, money laundering methods and other similar topics; however, this Forum has been abolished. Instead, the MLU has been giving information and feedback through its quarterly newspaper "Money Laundering News".

3.7.2 Recommendations and Comments

282. Section 7 of the MLA specifically obligates reporting entities to report transactions that are suspected of being "associated with…offences covered by section 147a or section 147b of the Penal Code". However, because the scope of the terrorist financing offence as articulated in s.147b is not quite broad enough, it is not clear that the reporting obligations under Recommendation 13 and Special Recommendation IV apply to transactions that may be related to the mere collection of funds for a terrorist/terrorist organisation. Because the reporting obligation in relation to money laundering is more general (referring to transactions suspected of being related to "the proceeds of crime", rather than specifically referencing s.317 of the Penal Code itself), the fact that the scope of the money laundering offence is not quite broad enough would not appear to have a similar negative impact on the scope of the reporting obligation.

283. The FSA should ensure that non-bank financial institutions, including MVTS providers, comply with their reporting obligations. Steps should also be taken to refocus reporting in general to concentrate more on the nature of the transaction. Norway fully observes Recommendation 14.

284. In relation to Recommendation 25, almost every reporting entity that the assessors met with (particularly the DNFBP sectors) asked for more specific and tailored guidance concerning AML/CFT obligations. In that regard, the guidance given by the FSA should be deepened, broadened and based on the different typologies, trends and techniques that focus more attention on the nature of transactions themselves. Additional guidelines that are more tailored to particular types of financial institutions should be issued. As well, more outreach to the DNFBP sectors should be undertaken to ensure that sector participants understand the rationale for the reporting obligation and how to comply with it. As well, the MLU should deliver more specific feedback to reporting entities, particularly concerning the status of STRs and the outcome of specific cases. Norway reports that the MLU's ability to deliver such feedback is expected to improve when its new data system is in place.

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	LC	• In general, there are some concerns about the effectiveness of the reporting system. For instance, (except for MVTS providers), the number of STRs being reported by non-bank financial institutions is very small and the number of STRs being reported by banks themselves is also decreasing. Additionally, there were some indications during the on-site visit that, in the past year, a MVTS provider had not been complying with its reporting obligations. The FSA has since taken action to correct this problem. Another effectiveness concern relates to the fact that, in

		general, banks seem to focus on transactions performed by foreigners as being suspicious, rather than focusing on the nature and characteristics of the transactions themselves. There also appears to have been defensive reporting of STRs by the old MVTS provider (i.e. reporting of STRs without giving proper consideration to whether or not they are really suspicious). • It is not clear that the reporting obligations under Recommendation 13 and Special Recommendation IV apply to transactions that may be related to the mere collection of funds for a terrorist/terrorist organisation.
R.14	C	• Recommendation 14 is fully observed.
R.25	PC[76]	• Almost every reporting entity that the assessors met with asked for more specific and tailored guidance concerning AML/CFT obligations. • The FSA has issued detailed guidance to Reporting FIs concerning how to comply with the reporting obligations. Despite the guidance given, 70% of all STRs are based on transactions made by non-Norwegians. It seems that the only real indicator or typology that has made any impact within the reporting community is the fact that a non-Norwegian is performing a transaction. It does not seem that those STRs should not have been made, which leads however to the conclusion that there is a potential for other types of STRs to be reported if only the employees of the reporting institutions had been guided to focus not only on the customer, but also on the nature of the transactions. • Upon receipt of the STR, the MLU sends a computer printout with information about the reference number to the financial institution. After making its inquiries, the MLU normally informs the Reporting FI of the decision that was taken, and (if applicable) of the police district or foreign unit investigating the case. However, this has not been a consistent practice in the last years. The Reporting FI should also receive transcripts of legal decisions; however, this has not been followed up lately. Previously, Reporting FIs received a report every six months about the current status of all the STRs that the Reporting FI had reported; however, this is no longer the practice. Until 2004, the MLU sent quarterly reports to reporting entities; however, this practice was stopped due to a lack of resources. Norway reports, however, that the practice of sending quarterly reports recommenced as of 1 January 2005. • The MLU also had a tradition of giving feedback to Reporting FIs/BPs through a Contact Forum (biannual meetings with representatives from these entities). The Contact Forum discussed issues such as feedback, suspicious transactions, money laundering methods and other similar topics; however, this Forum has been abolished. Instead, the MLU has been giving information and feedback through its quarterly newspaper "Money Laundering News".
SR.IV	LC	• Unclear if the reporting obligation extends to all transactions where there is any suspicion that there is a link to a terrorist organisation or terrorist financier. • Concerns raised above in Recommendation 13 about the effectiveness of the reporting system apply equally to SR IV.

Other types of reporting

3.7A Large transaction and cross-border transaction reporting (R.19 & SR IX)

3.7A.1 Description and Analysis

285. ***Recommendation 19:*** The FATF amended Recommendation 19 and deleted Interpretative Note after Norway received the mutual evaluation questionnaire related to this evaluation. Nevertheless, Norway has agreed to be evaluated on its compliance with amended Recommendation 19. High-level public officials at the Ministry of Finance has confirmed that, on different occasions, Norway has considered the feasibility and utility of implementing a system whereby Reporting FIs would report all domestic cash transactions above a fixed threshold to a national central agency with a computerised

[76] This is an overall rating for compliance with Recommendation 25, based on the assessments in sections 3.7, 3.12 and 4.5 of this report.

database. However, Norway has concluded that, so far, it has not found sufficient feasibility and utility to introducing such a system in Norway.

286. ***Special Recommendation IX:*** The FATF adopted SR IX (Cash couriers) and its Interpretative Note after Norway received the mutual evaluation questionnaire related to this evaluation. Nevertheless, Norway has agreed to be evaluated on its compliance with SR IX. Pursuant to its customs legislation, Norway has a declaration system to monitor incoming and outgoing cross-border transportations of cash. All of the declared cash must also be reported to the Currency Transaction Register by the customs authorities (see paragraphs 287 and 289 of this report). The declaration system is not new, but it is new in that it is being regulated by the customs regulations as of 1 January 2005. The purpose of the CRA is to prevent and combat financial crime (including ML) and to correct payment of taxes and duties by giving the relevant authorities access to information concerning transactions that involve foreign exchange or cross-border elements. The declaration system is administered by the Norwegian Customs Directorate. The role of Customs is to detect illegal movements of goods and currency entering or leaving Norway and, if successful in that regard, to turn the case over to the police. Customs authorities monitor the land and sea borders of Norway, its airports and its territorial waters. There are no free-trade zones in Norway.

287. The declaration obligation applies to both in-coming and out-going cross-border transportations of cash of a value equal to or exceeding NOK 25 000 (EUR 3 000/USD 4 000) (or the equivalent value in a foreign currency). However, the declaration obligation does not apply to bearer negotiable instruments—although when foreign negotiable instruments are cashed in, at a Norwegian bank for instance, the bank involved will be obliged to report the transaction to the Currency Transaction Register. However, in such cases it is the cashing-in that is being detected and, therefore, required to be reported, not the cross-border transportation itself, because the cashing-in is when the transaction takes place. Moreover, this system will not capture cross-border transportations of bearer negotiable instruments, regardless of whether they are cashed in Norway or not. In relation to bearer negotiable instruments, there is no possibility to stop or restrain them to determine whether evidence of ML/FT may be found, there is no penalty for falsely declaring them (because there is no obligation to declare and identification of the bearer is not retained). .

288. Cross-border transportations that are made by couriers, postal firms, delivery firms and private travellers must be truthfully reported to the customs authorities who have five days to register the report in the Currency Register. This obligation also applies to insured letters (*verdibrev)* containing currency or monetary instruments.[77] Insured letters are letters delivered by Norway Post that have their contents insured. Insured letters can be used to send money and other valuables through the mail. However, the maximum amount that can be sent through this method is NOK 40 000 (EUR 4 800/USD 6 300).

289. It is a criminal offence to make a false declaration. The penalty is a fine normally amounting to 2.5-3% of the value of the currency being transported. There is no need to have found evidence of ML/FT or some other crime in order to impose a fine in these circumstances. There is no possibility to confiscate the entire sum of money, simply because it has been falsely declared; however, there is the possibility to confiscate currency that are found to be related to ML/FT. In such instances, the normal criminal provisions apply (see paragraphs 108 to 118 of this report). In the administrative control situation, the customs authorities will ask questions relevant to sort out whether this is a criminal case, which has to be handled further by the police. Upon discovering that a false declaration has been made (or no declaration was made when this should have been done) or when there is a suspicion of ML/FT, the customs authorities will hand the suspected person and the confiscated funds to the police.

[77] Theoretically, postal operators have additional reporting obligations under the MLA (although these provisions have not yet entered into force) (MLA s.4 no.9). Norway reports that the Ministry of Finance still needs to discuss the issue with the Ministry of Transport and Communications before the provision may enter into force.

Breaches of the duty to declare incoming/outgoing cross-border transportations of currency are reported to the MLU. The customs authorities will then also hand over any intelligence information they possess to the police. When a false declaration has been made or when there is a suspicion of ML/FT, the customs authorities can hold the carrier for a short period of time—equal to the length that it takes to conduct administrative checks. This may vary depending on the seriousness of the case. After this, the police must take over the case, ask additional questions or, in cases where there is a suspicion of ML/FT, ascertain whether evidence of a crime may be found. Cases that are turned over to the police (i.e. if a false declaration is made or a suspicion of ML/FT exists) are not registered in the Currency Transaction Register because the currency/monetary instruments has not technically entered or left Norway. The money will be registered if and when this is delivered back and declared.

290. Declaration forms are available on the internet and also at all customs offices and all false declarations are reported to the MLU as soon as possible. The customs authorities report suspicious cross-border transportation of currency to the MLU. They also report large cash payments exceeding NOK 75 000 (EUR 9 100/USD 11 900) in value. The latter is not a legal requirement; it is an internal routine that was developed by the customs authorities. Smaller amounts may be reported if the customs authorities suspect that the money is proceeds of crime. Information on the currency involved and information identifying the persons receiving/sending them are collected and retained through this system.

291. The Customs Directorate is responsible for the new Currency Transaction Register The Currency Transaction Register replaces the BRAVO Register (the former repository for cross-border transaction reports). All of the information that existed in the BRAVO Register concerning transactions which date back to 2000 has been transferred over into the new Currency Transaction Register. The information in the Currency Transaction Register shall be deleted after 5 years (CRA s.7). The Currency Transaction Register contains more information than the BRAVO-register did and is more accessible to the competent authorities responsible for combating ML/FT. The MLU, police, the Prosecution Authority, the FSA, tax authorities, National Insurance Administration, Norges Bank, the Ministry of Foreign Affairs, and Customs Directorate have electronic access to the information in the Currency Transaction Register.[78] The CRA also allows the administrator of an estate in bankruptcy to have access to information in the Currency Transaction Register for the purpose of discharging his/her duties under the Bankruptcy Act. The Ministry of Finance may issue regulations that limit the availability to certain (authorised) persons or groups within these institutions (CRA s.6). The Ministry of Finance is also authorised to give other parties access to the register. Only those members who have enforcement/investigative duties have access to the Register. Additionally, the Norwegian government body responsible for collecting statistics will have direct access to the Register. This Register is not publicly available.

292. The police and Prosecution Authority (including ØKOKRIM and the MLU) can only access the Currency Transaction Register after an investigation is started. In other words, a police officer must have taken the informal decision to start investigating (before a formal charge or indictment is laid). However, it is left to the police and Prosecution Authority to make this determination and it is their responsibility to ensure that they only access the database after an investigation has been started. At this stage, there is no need to have proof of a crime; a suspicion is enough. The Currency Transaction Register can be searched by name, amount of the transaction or by type of currency, among other ways. The ability of the tax and customs authorities to access the Currency Transaction Register is much broader. These authorities may access the Currency Transaction Register for the purpose of conducting internal controls of the system. In other words, they do not need to have any suspicion of wrongdoing or to have started an investigation. In the course of their access, if they find activity which raises suspicion of a crime, they can then inform the police.

[78] The National Bureau of Statistics and the Banking, Insurance and Securities Commission will also have restricted access to the Currency Register.

293. The Customs Act authorises the customs authorities to share information with the police (including the MLU), when the information is related to a breach of customs regulations. If the customs authorities have reasonable grounds to suspect a criminal offence outside their administrative area, they may give this information to the police if the criminal offence can be punished with imprisonment for more than six months. It is not necessary that a suspicion of ML/FT or some other crime exist. Information in the Currency Transaction Register can be exchanged with international counterparts under the authorities of tax treaties or judicial conventions. Information exchange under tax treaties is, of course, limited to the context of tax cases. The Customs Directorate can also decide whether to share information with foreign customs authorities. The Customs Directorate routinely co-operates with the Norwegian police, tax and immigration authorities, security personnel at the airports and foreign customs authorities. However, they do not co-operate with foreign immigration authorities. Nevertheless, the Norwegian Customs Directorate co-operates extensively with their counterparts in Europe, the United States, South Africa, Russia, Ukraine and Poland. The Customs Directorate has memoranda of understanding (MOUs) with some European countries specifically and with the EU generally. It has the ability to co-operate without an MOU, but in such cases information can only be shared on conditions. For instance, information contained in the Currency Transaction Registry can be shared with foreign customs authorities, provided that they have privacy standards comparable to those in the EU.

294. Checks on the cross-border transportation of goods and currency are made both randomly and, more frequently, on the basis of intelligence. At times, Norwegian customs authorities conduct control actions in co-operation with foreign customs authorities. For instance, such a control action was conducted in the Baltic Sea specifically for the purpose of trying to detect money laundering activity.

295. The information recorded on cross-border transportation of cash is: whether or not the cash is being imported/exported; the name and identity of the declarant (i.e. a person, courier or post service), including date of birth, personal identification number/passport number/business number or other legitimation, address and country), what kind of transport is being used (e.g. car, boat (including name of the boat), flight (including flight number), post or other); name and identity of the forwarding agent; country of origin/destination; the value and type of currency being transported; and the date and place of declaration. If NOK 100 000 (EUR 12 100/USD 15 800) or more is being taken out of Norway, then a record is also made concerning what the transaction relates to. Such information must be recorded in the Currency Transaction Registry within five days of the transportation being made.

296. The lists of designated persons and entities made pursuant to UN S/RES/1267(1999) are distributed to the customs authorities and are available to all customs posts electronically. However, lists of persons/entities designated pursuant to S/RES/1373(2001) are not. No specific guidance has been given to customs officers concerning freezing actions pursuant to such lists; however, Norwegian authorities believe that if such money were detected entering or leaving Norway, it would be frozen. If Norwegian authorities discover an unusual shipment of currency, monetary instruments, precious metals, or gems, etcetera, they are, on certain conditions, allowed to notify the customs authorities in the country from which that shipment originated, pursuant to the Customs Act (s.4) or bilateral agreements on mutual legal assistance in customs matters that Norway participates in.

3.7A.2 Recommendations and Comments

297. At the time of the on-site visit, pre-printed declaration forms and signs informing travellers of their reporting obligations were only available on the internet; however, they are now readily available at every airport and customs post. At a minimum, the MLU, and possibly also the police/ØKOKRIM should have electronic access to the Currency Transaction Register even where no investigation has formally commenced. The MLU should be able to conduct a check against this register in the same way as it conducts checks against many other registers when it receives an STR. Although information is not retained in the Currency Transaction Register when a false declaration is made or when there is a suspicion of ML/FT, this information is retained by the MLU. In addition to

distributing the lists of persons designated under S/RES/1267(1999) to the customs authorities, lists of persons designated under S/RES/1373(2001) should also be distributed. Overall, Norway's declaration system is insufficient in scope, and should be extended to include incoming and outgoing cross-border transportations of bearer negotiable instruments.

3.7A.3 Compliance with Recommendation 19 and Special Recommendation IX

	Rating	Summary of factors underlying rating
R.19	C	• Recommendation 19 is fully observed.
SR.IX	PC	• The declaration obligation does not apply to bearer negotiable instruments—although when foreign negotiable instruments are cashed in, at a Norwegian bank for instance, the bank involved will be obliged to report the transaction to the Currency Transaction Register. However, in such cases it is the cashing-in that is being detected and, therefore, required to be reported, not the cross-border transportation itself, because the cashing-in is when the transaction takes place. Moreover, this system will not capture cross-border transportations of bearer negotiable instruments in Norwegian currency, regardless of whether they are cashed in Norway or not. In relation to bearer negotiable instruments, there is no possibility to stop or restrain them to determine whether evidence of ML/FT may be found, there is no penalty for falsely declaring them (because there is no obligation to declare and identification of the bearer is not retained). • The police and Prosecution Authority (including ØKOKRIM and the MLU) can only access the Currency Transaction Register after an investigation is started. • Lists of designated persons and entities made pursuant to UN S/RES/1267(1999) are distributed to the customs authorities and are available to all customs posts electronically. However, lists of persons/entities designated pursuant to S/RES/1373(2001) are not.

Internal controls and other measures

3.8 Internal controls, compliance, audit and foreign branches (R.15 & 22)

3.8.1 Description and Analysis

298. ***Recommendation 15:*** All Reporting FIs are obligated to establish satisfactory internal control and communications procedures to meet their obligations under the MLA and MLR. For instance, Reporting FIs must establish proper internal control and communications routines to ensure that STRs can be properly investigated. For instance, each Reporting FI must designate an AML officer at the senior manager level (i.e. at a level which carries sufficient powers to allow the AML officer to discharge his/her statutory tasks, and to have sufficient authority and effectiveness vis-à-vis the Reporting FI's employees and top management). At the same time the AML officer needs to devote enough of his/her working time to maintaining contact with the segment of the Reporting FI's employees who perform customer-service functions (Circular 9/2004 s.2.11). In financial groups, each Reporting FI that is a member of the group is required to have an AML officer; however, the financial group may also have an AML officer at the group level. Internal reporting procedures must be established through which an employee who becomes suspicious of a transaction can report the suspicion to his/her superiors and the Reporting FI's specially designated AML officer. The AML officer reports directly to a specially nominated senior manager who ensures that the control and communication routines are established and being observed in the event of suspicious transactions and who is responsible for following up on these procedures (MLR s.10). The AML officer/unit has full access to all the mentioned data and information, and the statutory duty of confidentiality does not limit such access (MLA ss.4, 7 and 11; MLR s.11). Internal control procedures must be established at a senior management level and set down in writing.

299. The following types of Reporting FIs are required to have an independent audit department or internal audit function to test compliance with their internal controls: commercial banks; saving

banks; non-life insurance companies; life insurance companies; finance companies and mortgage companies; stock exchanges and authorised market places; investment firms; management companies for securities funds; private, municipal and regional pension funds and pension schemes; clearing houses; securities registers; and e-money institutions. This requirement also applies to other institutions that have aggregate total assets for own account and clients' account in excess of NOK 10 billion (EUR 1.2 billion/USD 1.6 billion) or which form part of a financial group with aggregate total assets in excess of this figure.[79] The internal audit unit must report to the Reporting FI's board of directors. It is entitled to attend board meetings, and must submit a report on the internal control system at least once a year. The board of directors must approve the internal audit unit's resources and plans on an annual basis, and has responsibility for appointing and dismissing the head of the internal audit unit.

300. Financial institutions are required to retain an authorised public auditor (FIA s.3-13), in addition to a control committee that is responsible for supervising its activities and ensuring that it complies with the provisions of the FIA (FIA s.3-11). As well, a person in senior management must be designated to be responsible for ensuring that the FI complies with AML/CFT legislation (MLA s.13). Auditors are authorised by the FSA and must meet fit and proper requirements (Auditors Act (AA) s.3-4). The AA sets out that a person who wants to be authorised as registered or state authorised auditors must: (i) have a record of honourable conduct; (ii) be capable of fulfilling their obligations as they arise; and (iii) be of full age and capacity. Auditors are at all times under the supervision of the FSA. The institution has no separate obligation to report to the FSA if the insurer becomes aware of circumstances that may be relevant to the fitness and propriety of its auditors, but will normally do so anyway.

301. At Reporting FIs without an internal audit function, the board of directors must ensure that an external body confirms compliance annually. In such cases, the external body must submit an annual report that states:

(a) Whether a systematic review of significant risks has been undertaken at the Reporting FI and how the internal control system is structured to manage these risks;

(b) Whether implementation of the internal control system is being monitored and whether failures are reported to the management in a systematic manner; and

(c) Whether the required documentation is to hand.

302. Reporting FIs are obligated to establish special training programmes (including follow up programmes) for employees and other relevant persons in order to comply with AML/CFT obligations (MLA s.13). All persons who perform services on behalf of or for Reporting FIs, including substitutes and other temporary labour must receive adequate instruction, training, maintenance and upgrading of their knowledge of AML/CFT legislation and measures (Circular 9/2004 s.2.16). Employee training is considered to be a key element of the AML/CFT measures of Reporting FIs. Reporting FIs should ensure that new staff are familiarised with relevant AML/CFT legislation and their obligations under it, and that existing staff are regularly updated on new developments in the rules. All personnel in the undertaking who deal with transactions, settlement and control functions must be informed of the identity of the undertaking's money laundering officer (Circular 9/2004 s.2.16). Staff training needs should be evaluated on a continual basis. Reporting FIs should also maintain an awareness of what training is most appropriate to their particular institution (i.e. in terms of their particular customers, types of transactions, etcetera) (Circular 9/2004 s.2.16). Additionally, employees and other persons performing AML/CFT tasks should participate in special training programmes that teach them to recognise transactions which may be related to ML/FT and advise them on how to handle such cases (MLR s.16; Circular 9/2004 s.2.16). Although there is no legal obligation on Reporting FIs to establish screening procedures to ensure high standards when hiring employees, Reporting FIs have implemented internal ethical and professional guidelines.

[79] Regulation no. 1057 of 20 June 1997 relating to the verification of control responsibilities, documentation and confirmation of the internal control system.

303. There are some preliminary concerns about how effectively internal controls have been implemented. The internal controls themselves suffer from the same deficiencies as the legal requirements. For instance, because full CDD is not a legal requirement in Norway, there is no legal obligation to implement internal controls to ensure that full CDD is performed, and it did not appear that institutions had voluntarily implemented the much higher standards that are required. Moreover, as illustrated by the results of the FSA thematic inspections of 12 banks and finance companies in February 2004, there seems to be room for financial institutions to improve their level of compliance. The FSA is aware that the Prosecution Authority has detected cases where loans may have been raised for ML purposes. Consequently, the FSA is of the view that financial institutions should require a borrower to document his debt-servicing ability with a view to confirming that there is no disparity between his income and asset situation and agreed repayment conditions. The borrower's own capital should also be scrutinised and documented. The FSA also found that some institutions had not prepared written guidelines concerning the issuance of declarations of approbation. The FSA is concerned with these issues because it is aware that, during financial crime investigations, questions are sometimes asked whether Norwegian financial institutions can, at the request of a customer, issue various types of approbation that serve to create general legitimacy which may enable customers to open accounts with foreign institutions. None of the institutions inspected have issued declarations of the type mentioned, although some confirmed that declarations concerning customer relationships may be issued at the customer's request. However, the institutions in question had not prepared written guidelines defining possible content of such declarations, which personnel could issue such declarations or filing requirements.

304. ***Recommendation 22:*** There is an assumption that AML/CFT legislation is harmonised in the EU/EEA area and that it is consistent with the FATF Recommendations. Subsidiaries of Norwegian financial institutions have to comply with AML/CFT legislation in the host country. However, there is no obligation to ensure that foreign subsidiaries observe AML/CFT measures consistent with Norwegian requirements and the FATF Recommendations to the extent that host country laws and regulations permits. The FSA is responsible for the supervision of Norwegian financial institutions, including their establishments abroad (unless such an establishment is under supervision of the host state), as well as any other companies which may be part of the group. The FSA will not authorise a Norwegian financial institution to establish a branch in a country that has inadequate regulation and supervision unless the FSA has full authority for supervising that branch, including satisfactory access to reports and information. The FSA has indicated that where permission is sought to establish a branch or subsidiary in a foreign country with lesser AML/CFT measures, they will adopt the policy of requiring that the foreign branch/subsidiary complies with Norwegian AML/CFT standards. However, no cases have so far emerged in relation to subsidiaries established abroad. There is no requirement for a financial institution to inform the FSA if its foreign branch or subsidiary is unable to observe appropriate AML/CFT measures because this is prohibited by the laws or regulations of the host country.

3.8.2 Recommendations and Comments

305. Reporting FIs should be obligation to establish screening procedures to ensure high standards when hiring employees. Once Norway has corrected the legal requirements in the other areas of its AML/CFT regime (particularly with regards to customer identification measures), Reporting FIs should be obligated to implement satisfactory internal controls in that regard. Norway should implement an obligation that foreign subsidiaries observe AML/CFT measures consistent with Norwegian requirements and the FATF Recommendations to the extent that host country laws and regulations permits. Norway should also implement a requirement that a financial institution inform the FSA if its foreign branch or subsidiary is unable to observe appropriate AML/CFT measures because this is prohibited by the laws or regulations of the host country.

3.8.3 Compliance with Recommendations 15 & 22

	Rating	Summary of factors underlying rating
R.15	LC	• There is no legal obligation on Reporting FIs to establish screening procedures to ensure high standards when hiring employees. • There are some preliminary concerns about how effectively internal controls have been implemented. The internal controls themselves suffer from the same deficiencies as the legal requirements. For instance, because full CDD is not a legal requirement in Norway, there is no legal obligation to implement internal controls to ensure that full CDD is performed, and it did not appear that institutions had voluntarily implemented the much higher standards that are required.
R.22	LC	• There is no requirement for a financial institution to inform the FSA if its foreign branch or subsidiary is unable to observe appropriate AML/CFT measures because this is prohibited by the laws or regulations of the host country.

3.9 Shell banks (R.18)

3.9.1 Description and Analysis

306. ***Recommendation 18:*** Shell banks are indirectly prohibited in Norway. All savings banks and commercial banks are required by law to have their registered office and head office in Norway (or any other EU/EEA country): (CBA Act s.8, SBA s. 3). There are no other requirements relating directly or indirectly to shell banks. Consequently, nothing prohibits financial institutions from entering into or continuing correspondent banking relationships with shell banks. Nor is there any obligation on financial institutions to satisfy themselves that a respondent financing institution in a foreign country is not permitting its accounts to be used by shell banks.

3.9.2 Recommendations and Comments

307. Norway should implement provisions that: (i) prohibit financial institutions from entering into or continuing correspondent banking relationships with shell banks; and (ii) obligate financial institutions to satisfy themselves that the respondent financial institution in a foreign country does not permit its accounts to be used by shell banks.

3.9.3 Compliance with Recommendation 18

	Rating	Summary of factors underlying rating
R.18	PC	• There is no prohibition on financial institutions entering into or continuing correspondent banking relationships with shell banks. • There is no obligation on financial institutions to satisfy themselves that a respondent financing institution in a foreign country is not permitting its accounts to be used by shell banks.

Regulation, supervision, monitoring and sanctions

3.10 The supervisory and oversight system - competent authorities and SROs

Role, functions, duties and powers (including sanctions) (R.17, 23, 29 & 30)

3.10.1 Description and Analysis

308. ***Recommendation 23 (Licensing and supervision of financial institutions):*** The licensing function for financial institutions is divided between the Ministry of Finance and the FSA. The FSA has responsibility for ensuring that all Reporting FIs have adequate policies, practices and procedures in order to comply with AML/CFT legislation (FS Act s.3). In line with the general practice of other financial regulators, the FSA allocates its supervisory resources on a risk sensitive basis. No entities supervised by the FSA are overlooked, but the weaker ones would generally get more attention than others considered to be better managed. The FSA has stated that it looks to Core Principles in its supervision of banks, insurers and investment firms and tries to co-ordinate this approach with AML/CFT supervision.

SUPERVISION AND LICENSING OF FINANCIAL INSTITUTIONS	
Financial institutions supervised by the FSA	Licensing decision made by:
Banks	Ministry of Finance
Finance companies	Ministry of Finance/FSA
Mortgage companies	Ministry of Finance/FSA
Insurance companies	Ministry of Finance
Insurance brokers	FSA
Pension Funds	FSA
Investment firms	FSA
Management companies for securities funds	FSA
Stock Exchanges	Ministry of Finance
Real estate agents	FSA
Debt-collection agencies	FSA
Auditors	FSA
External accountants	FSA

309. ***Supervision of MVTS providers and foreign exchange offices:*** Foreign exchange offices and independent MVTS providers are not permitted to operate in Norway. Only banks, finance companies and EU/EEA branches of such undertakings are authorised to perform this type of activity (FIA chapter 4a). It is illegal to perform regulated activities (such as the provision of financial services) without authorisation. Such action will be followed up by the authorities, including the FSA which is responsible for ensuring that this sector complies with AML/CFT legislation. There is some concern about how effectively this sector is being supervised given that the assessors have been made aware of some problems concerning how the reporting obligation is being complied with. Norway has reported that inquiries are in progress on this case and appropriate action will be taken.

310. ***Effective implementation of the FATF Recommendations:*** So far, Norway has only conducted 12 thematic inspections relating to AML/CFT issues. Consequently, it is premature to draw firm conclusions about the effectiveness of Norway's implementation of the FATF Recommendations. Nevertheless, it should be noted that those inspections (of five banks and seven finance companies which the FSA considers to be a high risk business—private banking) revealed substantial variations among them in terms of their awareness of and focus on AML issues. Breaches related to: (i) failure to establish satisfactory internal AML controls or to designate a person in senior management to follow up on these controls; (ii) defects in procedures for verifying the identity of legal persons; and (iii) failure to keep records in a manner that ensured full traceability of identity documents. In all cases, the FSA requested the financial institutions to take steps to correct these deficiencies, but did not impose any sanctions. However, the FSA has followed up on these inspections and all the financial institutions in question have implemented relevant measures to comply with the final remarks from the inspections. The FSA indicates that, although it has discovered some instances of breaches of AML/CFT regulation, none have been particularly serious. Consequently, the FSA has not had to revoke a license or report to the police.

311. ***Recommendation 29 (Supervisor's powers of enforcement and sanction):*** The FSA is authorised to impose a broad range of administrative sanctions against Reporting FIs that do not comply with Norwegian law (including the AML/CFT requirements). It is empowered to order a Reporting FI to stop any activity, produce information, and convene meetings of its board, control

committee or controlling bodies (FS Act ss.4-5). Additionally, the FSA may: (i) restrict the current activities of the Reporting FI; (ii) withhold approval of new activities or acquisitions; (iii) restrict or suspend payments to shareholders or share repurchases; (iv) restrict asset transfers; (v) bar individuals from banking; (vi) replace/restrict the powers of managers, directors or controlling owners (but only in the context of applications to acquire qualifying holdings in financial institutions as described in paragraphs 314 to 315 below); (vii) arrange a take-over by/merger with a healthier institution; or (viii) impose conservatorship. However, the FSA has no authority to sanction breaches of its circulars (such as Circular 9/2004 relating to AML/CFT) because circulars are not legally binding. Circular 9/2004 only expresses the FSA's interpretations of the AML/CFT legislation. Nevertheless, the circular is an important tool for the financial sector in organising and implementing AML/CFT measures. In the case of minor violations, the FSA can use oral or written communication as a corrective measure. In most cases, the Reporting FI would then correct the problem. If the Reporting FI continues to not comply, the FSA may order the Reporting FI to correct the problem within a certain time limit. Such an order has a coercive effect in that failure to comply can result in a single payment or recurrent fine that may be enforced by execution proceedings (s. 17 MLA). In serious cases, the FSA may take steps to revoke the Reporting FI's license (if the FSA is the licensing authority) or try to have the Reporting FI's licence revoked (if the Ministry of Finance is the licensing authority) or report it to the Prosecution Authority (or other relevant public authority within whose jurisdiction the specific matter falls). In cases that may be related to ML/FT, the FSA must report it to ØKOKRIM (FS Act s.6). The FSA also has the power to: (i) impose fines on the officers/employees of a Reporting FI for breaches of the FS Act (FS Act s.10); or (ii) impose fines on the Reporting FI or its officers or employees for violations of the MLA/MLR (MLA s.17). Because the FSA has not imposed any sanctions for breaches of AML/CFT obligations, no statistics exist in this area.

.

312. ***Recommendation 30 (Structure and resources of the supervisory authorities):*** The FSA comes under the general responsibilities of the Ministry of Finance, but is otherwise an operationally independent government agency, tasked with the responsibility of supervising the Norwegian financial sector. (For a list of entities supervised by the FSA, see paragraph 305 above.) The activities of the FSA are managed by an independent board whose members are appointed by the King in Council for renewable 4 year terms. On a day to day basis, management of the FSA is in the hands of the Director General, who is appointed by the King in Council for a renewable term of 6 years. The objective is that the FSA shall be in a position to exercise its supervisory function independently of government or industry interference. Parties who are affected by a decision that is made by the FSA in the exercise of its supervisory functions are entitled to complain to the Ministry of Finance. In such cases, the Ministry of Finance may review the FSA's decision.

313. At the end of 2003, the FSA had 183 employees, including 62 economists, 45 lawyers and 20 actuaries or auditors. Of these, 94 had more than five years of supervisory experience and 47 had more than five years of relevant business experience. The remaining employees were primarily administrative staff. In 2003, this workforce was responsible for supervising 2 518 separate entities, including 158 banks; 64 finance and mortgage companies including branches; 4 e-money institutions; 284 insurance companies (life and non-life, including branches, private pension funds and schemes); 49 insurance brokers; 8 holding companies; 78 investment firms; 21 management companies for securities firms; 2 clearing houses; 2 stock exchanges; 1 authorised market place; the Central Securities Registry; 114 debt collection agencies; 578 real estate agencies; 1 178 lawyers' whose practice includes offering real estate services; 47 co-operative building associations acting as real estate agents; 10 debt purchase businesses; 5 358 auditors; 518 auditing firms; 6 724 external accountants; and 2 542 external accounting firms. Considering the number of entities that the FSA is responsible for supervising, its number of staff seems inadequate. In 2003, the FSA generated 132 supervisory reports and 113 supervisory comments (i.e. observations). The FSA's budget in 2003 was NOK 134.6 million (EUR 16.3 million/USD 21.3 million). The FSA endeavours to recruit high quality staff at all levels and (within its budget) endeavours to hold sufficient staff and resources to perform its supervisory tasks. The FSA also endeavours to offer competitive salaries, but is not always in a position to offer salaries competitive to those offered in financial institutions. The FSA is also continuously upgrading its technical resources to the extent allowed in its budget.

314. In general, the FSA employees are under a consistent requirement to obey administrative law principles and rules for good conduct pertaining to the public administration (including a requirement to observe procedural fairness). New employees must sign a declaration explicitly undertaking to observe professional secrecy. The FSA's employees are under a legal obligation to maintain the confidentiality of non-public information (such as operational or business matters of a company which for competition reasons it is important to keep secret) and to treat as confidential any information about a customer's affairs, which may come to their knowledge in the course of their work (FS Act; PAA). Law or regulation determines the circumstances under which disclosure may be made to another agency. The FSA has also developed a set of ethical rules and guidelines that apply to all of its employees and which are designed to avoid conflicts of interests for the FSA's board members/employees, and the financial institutions that it supervises. New employees must read through the guidelines and sign a written statement agreeing to follow these rules. Employees must as a general rule not receive gifts or invitations from institutions under supervision, and are obliged to report all purchases of financial instruments and use of services provided by financial institutions under the supervision of the FSA (FS Act). Bonds and shares may not be sold earlier than one year after they were purchased.[80]. Employees and board members shall not be given loans in financial institutions under supervision without the consent of the Director General or the Ministry of Finance. Additionally, the FSA invests in training seminars and courses for its, in order to maintain the skill of its staff. Representatives from the FSA also participate in the delegation to FATF.

Recommendation 17: Following an inspection, the approach of the FSA is to write a report of its findings which is sent to the company's board of directors. The board, in turn, is asked to comment on the report and to forward the report to the external auditor and control committee for their comments. The FSA reviews all of the comments and then concludes the inspection by writing final remarks that are submitted to the board of directors. The FSA reports that always, after allowing the reporting entity a reasonable period of time to implement improved routines and measures, it will follow up the finding from an inspection. In most cases, the FSA finds that the reporting entity has complied with the FSA's remarks. For instance, the FSA reports that this procedure was followed with the 12 financial institutions that underwent AML/CFT inspections. The FSA reports that all of them have corrected the deficiencies that had been found and that such results thus made it unnecessary for it to use its more severe powers. On occasions, the FSA has issued formal warnings, specific orders to comply and also required regular follow-up reporting by deficient FIs. .

315. Where a Reporting FI has not complied with its AML/CFT obligations, the wording of the MLA does not make it clear whether sanctions can be applied to the directors and senior management of the FI that was responsible for the violation by the FI.

316. In relation to criminal penalties, the assessors feel that the legal provisions cited by Norway are unclear, but Norway is of the firm view that criminal penalties can be applied to the directors and employees of Reporting FIs in respect of a breach by the Reporting FI. Both the imposition of fines and imprisonment require conviction in a court of law; however, no cases have been prosecuted for breach of the MLA. It should be noted that the MLA came into force on 1 January 2004 (over a year before the on-site visit).

317. In relation to civil penalties, s. 4(7) of the Financial Supervision Act gives the FSA the authority "to order an institution to rectify the matter if an institution's bodies have acted, or shown negligence, in contravention of their duties pursuant to legislation". The FSA could then rely on s. 10 of the FSA to take action against an officer or employee of the Reporting FI for failing to comply with the s. 4(7) order. S. 10 provides that any officer or employee who wilfully or negligently contravenes an order of the FSA is punishable by (unlimited) fines or up to one year imprisonment. These provisions provide

[80] Additionally, a prohibition for the employees to trade stocks is being considered.

a means for the FSA to take a form of civil enforcement action but it would be applicable on a forward looking basis.

3.10.2 Recommendations and Comments

318. It is recommended that Norway clarify the law beyond a doubt concerning its ability to sanction directors and senior management of Reporting FIs for The FSA has just 183 staff to ensure not only the compliance of FIs with prudential and AML/CFT laws and regulations, but also the AML/CFT compliance of 17 741 Reporting FIs/BPs. The FSA should be given additional resources to be allocated for AML/CFT supervision. The FSA should consider creating a well staffed stand alone AML/CFT unit or at least a team of examiners specialising in AML/CFT measures that check FIs compliance with AML/CFT on an ongoing basis for all supervised entities.

3.10.3 Compliance with Recommendations 17, 23 (criteria 23.2, 23.4, 23.6-23.7), 29 & 30

	Rating	Summary of factors relevant to s.3.10 underlying overall rating
R.17	LC	• Where a Reporting FI has not complied with its AML/CFT obligations, the wording of the MLA does not make it clear whether sanctions can be applied to the directors and senior management of the FI that was responsible for the violation by the FI. In relation to criminal penalties, the assessors feel that the legal provisions cited by Norway are unclear, but Norway is of the firm view that criminal penalties can be applied to the directors and senior management of Reporting FIs in respect of a breach by the Reporting FI. In relation to civil penalties, the Financial Supervision Act provide a means for the FSA to take a form of civil enforcement action but it would be applicable on a forward looking basis.
R.23	LC[81]	• There is some concern about how effectively the MVTS sector is being supervised given that the assessors have been made aware of some problems concerning how the reporting obligation is being complied with. Norway has reported that inquiries are in progress on this case and appropriate action will be taken.
R.29	LC[82]	• Another concern is that the FSA's powers seem to be quite limited in certain respects. For instance, the FSA may assess whether managers, directors or controlling owners are fit and proper, but only in the context of granting licences for the first time and applications to acquire qualifying holdings in financial institutions.
R.30	PC[83]	• Considering the number of entities that the FSA is responsible for supervising, its number of staff seems inadequate.

3.11 Financial institutions - market entry and ownership/control (R.23)

3.11.1 Description and Analysis

319. ***Recommendation 23 (Market entry and ownership/control):*** The FIA requires approval to be sought from the Ministry of Finance to acquire/dispose of shareholdings in a bank, insurance company, finance company or mortgage company that cross defined thresholds (10%, 20%, 25%, 33% and 50%) or would allow the shareholder to exercise significant influence on the management of the credit institution and its business (a "qualifying holding") (s.2-2 FIA). In cases where the application involves a proposed holding equal to or exceeding 25%, the Ministry of Finance shall refuse the authorisation unless it is convinced that the applicant is fit and proper, and the acquisition will not have undesirable effects on the functioning of the capital and credit markets. Conditions may be

[81] This is an overall rating for compliance with Recommendation 23, based on the assessments in sections 3.10, 3.11 and 3.13 of this report.

[82] This is an overall rating for compliance with Recommendation 29, based on the assessments in sections 3.10 and 3.13 of this report.

[83] This is an overall rating for compliance with Recommendation 30, based on the assessments in sections 2.5, 2.6 and 3.10 of this report.

attached to the authorisation. When assessing whether or not to give authorisation, the Ministry of Finance shall attach special importance to whether the ownership structure of the credit institution after the acquisition will impede effective supervision of it and whether the applicant: (i) is fit and proper (based on previous conduct in business relationships, available financial resources and consideration for due and proper business activity); (ii) will be able to use his influence in the institution to achieve advantages for his own or affiliated activity, or indirectly exert influence on other commercial activity; and (iii) is commensurate with the aim of a financial market based on competition between mutually independent institutions, or is likely to impair the credit institution's independence in relation to other commercial interests (s.2-3 FIA). Similar conditions apply to the acquisition of shareholdings (10%, 20%, 33% and 50%) in investment firms and management companies for securities funds (STA ss 7-2 and 7-4). In relation to insurance companies, the Ministry of Finance's approval is needed for the acquisition of shares that will turn the company into a wholly owned subsidiary (IA s 3-6). Sections 2-2 and 2-3 of the FIA apply to all financial institutions, including insurance companies.

320. Financial institutions must obtain authorisation to establish a subsidiary/branch abroad or acquire more than 10% of the shares in a foreign financial institution (FIA, s.2a-3). In such cases, a Norwegian financial institution will not be issued an authorisation to establish a branch in a country with inadequate regulation and supervision unless the FSA has full authority for supervising that branch (including satisfactory access to reports and information). Financial institutions are also obligated to advise the FSA of every acquisition/disposal of qualifying holdings of which they become aware.[84] They also have to report once a year on the owners of qualifying holdings in the institution. The Ministry of Finance may also establish rules and regulations that: (i) require financial institutions to notify the FSA of all owners who have qualifying holdings in the institution; and (ii) require all legal persons that hold qualifying holdings in a financial institution to inform the FSA of the names of the members of their board of directors and management team. Authorisation to acquire a qualifying holding shall be denied if the applicant is not considered prudent or fit to exercise such influence on the credit institution (s.2-3 FIA). In the case of banks (commercial and savings), insurance companies, finance companies, mortgage credit institutions and credit institutions, the Ministry of Finance has the power to withdraw an authorisation where there are grounds for assuming that the holder has displayed such conduct that the basis for granting the authorisation no longer exists. The following factors are relevant for a fit and proper evaluation of the owners of a qualifying holding in a financial institution: (i) the applicant's previous behaviour in business and his economic resources; (ii) if the applicant may use the institution's influence to get advantages for his business; (iii) if the acquisition may weaken the institution's independence or reduce free competition; and (iv) if the acquisition may complicate the supervision of the credit institution.

321. ***Recommendation 23 (Fit and proper test for directors and management):*** When a financial institution is granted licence, the Ministry of Finance and the FSA ensure that the board of directors and the general manager (as the key functionaries) meet fit and proper requirements (FSA Circular 29/2001). The FSA shall refuse to grant authorisation if the board members, managing director or other person directly in charge of a commercial or savings bank or finance company cannot be deemed fit and proper.[85] The FSA interprets this requirement to also apply to changes in the management of banks established before the requirement came into force (SBA; CBA). Similar requirements apply to management companies for securities funds, insurance companies and investment firms.[86] Management companies for securities funds are subject to a requirement that they must be considered fit by the FSA to take care of the unit-holders' interests (SFA, s 2-2). A functionary will not pass the fit and proper test if he/she: (i) cannot be deemed to have the experience necessary to fill the post or the office; (ii) has been convicted of a criminal offence, and the offence committed gives reason to assume that the person in question would not discharge the position or the post in a satisfactory

[84] Regulation on Control of Ownership in Financial Institutions s.6.

[85] CBA s.8a.

[86] SBA s.3; SFA s.2-2; FIA s.3-3; IA ss.2-1 and 2-2; and STA s.7-2.

manner; or (iii) in his/her post or in the performance of other office the person has displayed conduct that gives reason to assume that he/she would not discharge the position in a satisfactory manner. This information is verified by reference to the applicant's curriculum vitae, a police attestation and answers to a standard questionnaire made by the FSA. The questionnaire asks: (i) if the person has been subject to a bankruptcy petition, or to bankruptcy proceeding, in the course of the past 10 years; (ii) if the person is under indictment for a criminal offence; and (iii) if the person has, in the past 10 years, been subject to an "estimated earnings" assessment, or been required to pay additional tax by any tax authority. The financial institutions referred to above are obligated to notify the FSA if its ownership changes after the authorisation is granted.

322. Financial institutions must ensure that its board members and manager are fit and proper at all times. If the functionaries change after authorisation is granted, the onus is on the financial institution to ensure that the new key functionaries are fit and proper, to gather the above information on them and to submit this information to the FSA on demand. As soon as the financial institution becomes aware of circumstances that deprive the fitness and propriety of these key functionaries, it must take remedial measures. In such cases, there is no explicit order to notify the FSA. The FSA confirms (by on-site inspection and on an ad hoc basis) that financial institutions are implementing routines to fulfil these requirements (Circular 29/2001). It is understood that in practice, banks, finance companies and mortgage companies would generally abide by the FSA's views and take relevant action should the latter consider the new director or manager not to be fit and proper.

3.11.2 Recommendations and Comments

323. There is no obligation on the financial institution to notify the FSA of changes in management.

3.11.3 Compliance with Recommendation 23 (criteria 23.1, 23.3-23.5)

	Rating	Summary of factors underlying rating
R.23	LC[87]	• There is no obligation on the financial institution to notify the FSA of changes in management.

3.12 AML/CFT Guidelines (R.25)

3.12.1 Description and Analysis

324. ***Recommendation 25 (AML/CFT guidelines issued by supervisors):*** In April 2004, the FSA issued Circular 9/2004 which sets out detailed guidance to Reporting FIs concerning how to implement and comply with their respective AML/CFT requirements. Circular 9/2004 also explains the importance of complying with AML/CFT measures, including rationales for the measures themselves. For instance, it explains that proper customer verification will not only counter ML/FT, but will also help reduce the Reporting FI's counterparty risk (the risk of financial loss and loss of reputation) (Circular 9/2004 s.2.7.2). Circular 9/2004 sets out additional detailed guidance concerning customer identification, including: identification of legal persons and beneficial owners; specific circumstances which constitute establishing a customer relationship; lists of documents that are acceptable customer identification information; and procedures for verifying customer identity. It gives details on the reporting obligation, including: specific examples of the types of financial activity that may be unusual; the importance of and rationale for implementing the reporting obligation; and how to properly file an STR. Circular 9/2004 was developed with the co-operation of industry organisations representing commercial banks and insurance companies, savings banks and finance companies. During a first round of consultation, the FSA asked these organisations to suggest topics and problems to be dealt with in the circular, most of which were ultimately incorporated. During a second round of consultation, a draft of the circular was sent on a non-public hearing to the co-

[87] This is an overall rating for compliance with Recommendation 23, based on the assessments in sections 3.10, 3.11 and 3.13 of this report.

operating industry organisations, in addition to industry organisations representing investment firms and management companies for securities funds. Circular 9/2004 is distributed to all Reporting FIs, including credit institutions, insurance companies, investment firms, management companies for securities funds, pension funds and insurance brokers and Reporting BPs (including real estate agents, auditors and external accountants). The FSA is very involved in training seminars (including the police trainee-program which has an AML/CFT component, and co-operation with the private sector on training issues), education and providing day-to-day advice by telephone. The FSA also issues general guidance concerning internal control systems (include those relating to AML/CFT).[88]

325. The Supervisory Council, NARF nor NIPA have issued AML/CFT guidance to the Reporting BPs that they supervise. However, the Supervisory Council, NBA, MLU and FSA are currently represented in a working group established by the Ministry of Justice & Police (and headed by the AC/AML Project) that shall propose AML/CFT guidance to lawyers. The group had its first meeting in August 2004 and is currently in the final stages of its work. The NARF and the NIPA (which are not supervisors, but industry associations) and ØKOKRIM are also part of a working group that was established by the FSA and is developing guidelines for auditors and external accountants.

3.12.2 Recommendations and Comments

326. The FSA should respond to the requests of Reporting FIs/BPs for additional and more specific AML/CFT guidelines on a more regular basis. Just as was done in the banking, insurance and securities sectors, such guidance should be more tailored to the different types of FIs and DNFBPs. The group that was established by the Ministry of Justice & Police to propose AML/CFT guidance for lawyers is encouraged to complete the final stages of its work as soon as possible. The working group comprised of NIPA, the NARF and ØKOKRIM should finish developing guidance for auditors and external accountants as soon as possible .

3.12.3 Compliance with Recommendation 25 (criteria 25.1, financial institutions)

	Rating	Summary of factors underlying rating
R.25	PC[89]	• The Supervisory Council (which supervises lawyers and independent legal professionals) has not yet issued AML/CFT guidance for lawyers (although it is currently working on this issue).

3.13 Ongoing supervision and monitoring (R.23, 29 & 32)

3.13.1 Description and Analysis

327. ***Recommendation 23 (Regulatory and supervisory measures for prudential purposes):*** The FSA supervises and monitors Reporting FIs for compliance with the Core Principles (in the banking, insurance and securities sectors), as well as compliance with AML/CFT legislation, particularly with a view to implementing the EU's First and Second Anti-Money Laundering Directives.

328. ***Recommendation 29 (Inspection authority of supervisors):*** The FSA is obligated to ensure that the financial institutions it supervises operate in an appropriate and proper manner, in accordance with law, and in accordance with the principles set out in its articles of associations (i.e. concerning its business purpose and reason for being established). In particular, the FSA is responsible for supervising the compliance of financial institutions with applicable AML/CFT measures (FS Act s.3). This involves examining the financial institution's internal control measures, internal ethical and professional policies, practices and guidelines, including those related to AML/CFT.

[88] Annex to FSA Circular no. 16/2003 Guide to the internal control regulations.

[89] This is an overall rating for compliance with Recommendation 25, based on the assessments in sections 3.7, 3.12 and 4.5 of this report.

329. The Financial Supervision Act gives the FSA comprehensive inspection and surveillance powers. The FSA has the power to require information from supervised institutions, and to conduct on-site inspections in addition to off-site review. There are no written regulations or guidelines prescribing the procedure that the FSA must follow during an inspection, particularly with regards to detecting breaches of AML/CFT legislation. However, before conducting an on-site inspection, the FSA sends a standard notice of inspection to the financial institution requesting it to supply the FSA with its internal AML/CFT routines. Although the FSA is not legally required to give prior notice that it is going to be conducting an on-site inspection, it has never conducted an inspection of a bank, finance company, insurance company, insurance broker, investment firm or management company for securities funds without doing so. The FSA shall examine accounts and other records of the FIs, and can carry out any investigations of their position and activity as it deems necessary.

330. FSA supervision is founded on a risk-based approach. FIs are obliged to produce self-assessment reports that are used by the FSA to determine which FIs will be visited on-site. However, these self-assessments are based on the prudential supervision and contain no AML/CFT questions. AML/CFT assessments of Reporting FIs by the FSA are an integral part of regular visits but seem to be too limited. For example, for a larger bank, the FSA indicated that the AML/CFT component of a regular examination took 2 days of off-site studies and 1 hour during the on-site. Moreover, for smaller FIs, the FSA indicated that AML/CFT assessments are not held annually, but only when there are indications that an assessment would be necessary. The assessors found that some institutions, that were deemed to be high risk, had just been assessed for the first time in 7 years. Not surprisingly, the assessment found some major shortcomings (like lack of a good AML/CFT compliance handbook within the institutions) that should normally not be found in countries that have implemented the FATF standard for some time.

331. The FSA's power to compel production of or obtain access to a financial institution's records is not predicated on the need to obtain a court order. At all times, the FI is obliged to furnish all information that the FSA may require. This includes giving the FSA access to and handing over to the FSA for inspection the financial institution's records, registered accounting information, accounting documentation, ledgers, documents, computers or other technical aids and material that is available via such aids and holdings of any kind. If the FI does not comply with this disclosure duty, the duty may be imposed on the individual officers/employees of the FI. (As a rule, the FI will be notified in such cases.) Consequently, the FI's auditor may be ordered to disclose information that appears in the annual accounts, account forms, staff pay summaries and deduction sheets, auditor's records and auditor's report (FS Act s.3). AML compliance is one of several items checked during on site inspections. For instance, the FSA will investigate whether the Reporting FI's record keeping routines comply with the AML legislation. Additionally, at on-site inspections, it is normal procedure to make spot checks of how institutions carry out the mandatory customer identification checks. During 2004, the FSA conducted 12 thematic AML inspections in banks and finance companies. Additionally, over the past six years, the FSA conducted ordinary inspections as set out in the following chart.

NUMBER OF ON-SITE INSPECTIONS CONDUCTED BY THE FSA ON REPORTING FIs						
	1998	1999	2000	2001	2002	2003
Banks/finance[90]	47	43	42	51	55	53[91]
Holding companies	0	0	0	2	2	0
Insurance	17	12	17	12	16	19

[90] The number of IT inspections in the respective segments has the following breakdown: Banks/finance (7), Insurance (1), Investment firms (4), Other institutions in the securities market (4), Data processing centres (2) and External accountants/External accounting firms (4).

[91] Of which four on-site inspections of bank groups and three at insurance companies, all conducted under the auspices of the Swedish Supervisory body, Finansinspektionen, with participants from the FSA.

Insurance brokers	2	4	3	6	4	6
Pension funds	7	13	12	5	8	5
Investment firms	25	23	25	20	20	23
Other institutions in the securities market (incl. management companies for securities funds	12	14	2	10	9	13

332. ***Recommendation 32 (Statistics collection related to ongoing supervision and monitoring):*** Norway maintains the statistics relating to the number of on-site examinations conducted by supervisors, broken down by the type of Reporting FI/BP. Norway does not maintain statistics concerning sanctions imposed for failing to comply with AML/CFT obligations.

3.13.2 Recommendations and Comments

333. The self-assessment reports used to identify priority FIs for inspection visits should be revised to include questions relating to AML/CFT. Norway should ensure that AML/CFT assessments of Reporting FIs occur more regularly, particularly in high risk institutions. Norway should collect and maintain statistics concerning the number and type of sanctions applied.

3.13.3 Compliance with Recommendations 23 (criteria 23.4, 23.6-23.7), 29 & 32 (rating & factors underlying rating)

	Rating	Summary of factors relevant to s.3.13 underlying overall rating
R.23	LC[92]	• There are no factors relevant to s.3.13 underlying the overall rating. However, see the factors mentioned in ss.3.10 and 3.11 of this report.
R.29	LC[93]	• FIs are obliged to produce self-assessment reports that are used by the FSA to determine which FIs will be visited on-site. However, these self-assessments are based on the prudential supervision and contain no AML/CFT questions. • AML/CFT assessments of Reporting FIs by the FSA are an integral part of regular visits but seem to be too limited. For example, for a larger bank, the FSA indicated that the AML/CFT component of a regular examination took 2 days of off-site studies and 1 hour during the on-site. Moreover, for smaller FIs, the FSA indicated that AML/CFT assessments are not held annually, but only when there are indications that an assessment would be necessary. The assessors found that some institutions, that were deemed to be high risk, had just been assessed for the first time in 7 years. Not surprisingly, the assessment found some major shortcomings (like lack of a good AML/CFT compliance handbook within the institutions) that should normally not be found in countries that have implemented the FATF standard for some time.
R.32	PC[94]	• Norway does not maintain statistics concerning sanctions imposed for failing to comply with AML/CFT obligations.

3.14 Money or value transfer services (SR.VI)

3.14.1 Description and Analysis

334. ***Special Recommendation VI:*** Foreign exchange activity (i.e. foreign exchange transactions and international money transfers[95]) may only be carried out by banks, finance companies licensed by the

[92] This is an overall rating for compliance with Recommendation 23, based on the assessments in sections 3.10, 3.11 and 3.13 of this report.

[93] This is an overall rating for compliance with Recommendation 29, based on the assessments in sections 3.10 and 3.13 of this report.

[94] This is an overall rating for compliance with Recommendation 32, based on the assessments in sections 2.5, 2.6, 3.13, 6.3, 6.4 and 6.5 of this report.

Ministry of Finance and EU/EEA branches of such undertakings (FIA chapter 4a). Consequently, they are subject to the same AML/CFT requirements set out in paragraphs 201 to 328 above. Although technically the Ministry of Finance may make exceptions to this requirement, to date no exceptions have been made (FIA s.4a.1). There have only been two MVTS providers that have been or are authorised to operate in Norway (one MVTS provider has taken over the other's business). Norway has implemented a licensing regime for MVTS providers (as opposed to a registration system) and, in fact, the only authorised MVTS provider in Norway is an EU branch of a bank. Both held/hold finance company/banking licences but only operate in the foreign exchange and money remittance sectors. As there are no agents of MVTS providers conducting business in Norway, the obligation under SR VI to maintain a current list of such agents does not apply. As the only authorised MVTS provider is an EU/EEA branch of a bank, the MVTS provider is subject to the FATF Recommendations, including Recommendations 4-11, 13-15 and 21-23, and SR VII. However, as with all other Reporting FIs in Norway, overall implementation of Recommendations 5-7, 15 and 22, and SR VII is very inadequate. This negatively impacts on the effectiveness of AML/CFT measures in the MVTS and other financial institution sectors. Moreover, there are specific problems in the MVTS sector relating to the effectiveness of the reporting system. Reporting in the sector has diminished recently in part, it seems, because of a breakdown of communication between the MLU and the MVTS provider. Whatever the reason, Recommendation 13 has not been implemented effectively in this sector.

335. The FSA is responsible for monitoring MVTS operators and ensuring that they comply with the licensing requirements and the FATF Recommendations. In this regard, the FSA has the same powers to sanction as described in paragraphs 308 and 312 above. It is illegal to provide MVTS without authorisation. Norway has detected some underground banking. ØKOKRIM has conducted two criminal investigations involving hawala. These cases initiated from STRs submitted to the MLU by banks (the hawala companies were using Norwegian banks to transfer money abroad). Although there was some suspicion initially of possible terrorist financing, that aspect was not a specific subject in the investigation. Even though carrying out unauthorised banking services is a breach of the FIA and, as such, may be dealt with as an administrative matter by the FSA, in serious cases (such as the ones referred to above), the law enforcement authorities may become involved and may investigate. In such cases, criminal charges could have resulted. However, there are some concerns about how effectively the MVTS provider (which is a bank) was supervised for most of the first year of its operation. In 2003, the MLU received information on approximately 2 500 MVTS transactions, and in 2004 the number of transactions reported exceeded 5 000. These STRs were submitted by the old MVTS provider. The successor MVTS provider commenced operations in early 2004, but reports have only been filed once by it. The MLU indicated that it received only one disc with 75 to 100 reports from the new MVTS provider during 2004, and no reports during 2005 until the date of the interview. The information contained on that one disc was, in the MLU's opinion, inadequate. This problem was only brought to the attention of the FSA days before the on-site visit and corrective action was taken following the on-site visit. Nevertheless, it is still troubling that the FSA was unaware that the only MVTS provider in Norway was not reporting to the MLU when the problem had been ongoing for almost a year.

3.14.2 Recommendations and Comments

336. The FSA should take immediate steps (including the application of sanctions, if necessary) to correct the problems with reporting in this sector. Additionally, the FSA should improve the effectiveness of its monitoring and supervision of this sector. Norway should take steps to properly implement Recommendations 5-7, 15 and 22, and SR VII. These measures should apply to all Reporting FIs, including MVTS operators.

[95] In this context, an international money transfer refers to the execution of all or parts of a payment order where moneys are made available to the recipient in a country other than the country in which the payment order was issued.

3.14.3 Compliance with Special Recommendation VI

	Rating	Summary of factors underlying rating
SR.VI	PC	• As with all other Reporting FIs in Norway, overall implementation of Recommendations 5-7, 15 and 22, and SR VII is very inadequate. This negatively impacts on the effectiveness of AML/CFT measures in the MVTS and other financial institution sectors. • There are specific problems in the MVTS sector relating to the effectiveness of the reporting system. Reporting in the sector has diminished recently in part, it seems, because of a breakdown of communication between the MLU and the MVTS provider. Whatever the reason, Recommendation 13 has not been implemented effectively in this sector. • There are some concerns about the effectiveness of supervision and sanction in the MVTS sector. In 2003, the MLU received information on approximately 2 500 MVTS transactions, and in 2004 the number of transactions reported exceeded 5 000. These STRs were submitted by the old MVTS provider. The successor MVTS provider commenced operations in early 2004, but reports have only been filed once by it. Although this problem has been brought to the attention of the FSA, no corrective action had been taken at the time of the on-site visit. However, subsequently, the FSA has started action to remedy this deficiency.

4 PREVENTIVE MEASURES – DESIGNATED NON-FINANCIAL BUSINESSES AND PROFESSIONS

337. Real estate agents, dealers in precious metals and stones, lawyers and other independent legal professionals, auditors, and accountants (collectively referred to as Reporting Businesses and Professions or Reporting BPs) are subject to AML/CFT obligations under the MLA and MLR. The following DNFBPs do not exist in Norway: land-based casinos, notaries and a separate business sector for trust and company service providers. Throughout section 4 of this report, unless stated otherwise, the AML/CFT obligations and comments applicable to Reporting FIs also apply to Reporting BPs.

338. Overall, the ratings for both Recommendation 12 and 16 have been lowered due to concerns about the scope of application of AML/CFT obligations (in relation to company service providers) Norway does not have a defined business sector providing trust/company services (trusts are not recognised in Norway and the large majority of company service business is handled by lawyers). However, there is no legal prohibition from other persons establishing such businesses in Norway. Consequently, although lawyers who provide company services are subject to AML/CFT obligations, a natural/legal person that is not a Reporting FI or Reporting BP could provide company services in Norway and would not be subject to AML/CFT obligations. Overall, it should be made clear that any person who provides company services is subject to the MLA and MLR. Clarifying the rules could include codifying the current practice by amending the law to restrict the provision of company services to only certain groups (e.g. lawyers).

4.1 Customer due diligence and record-keeping (R.12) (applying R.5 to 10 to DNFBP)

4.1.1 Description and Analysis

339. ***Applying Recommendation 5:*** The same serious deficiencies in the implementation of Recommendation 5 apply equally to Reporting FIs and Reporting BPs. In other words, customer identification requirements have been implemented, but full CDD requirements have not. Due to the nature of their work the following businesses/professions do not have occasional clients: accountants and auditors, lawyers, independent legal professionals and real estate agents. Providing assistance to an occasional customer implies that a customer relationship has been established. They enter into a business relationship with their customers when carrying out their business. For lawyers and accountants, entering into a business relationship includes accepting an assignment from a client (MLA s.2). Consequently, rules concerning occasional customers are not applicable to these groups.

340. *Real estate agents:* Real estate agents are obligated to identify their clients when carrying out real estate business. Real estate business is defined as acting as an intermediary (including being responsible for the settlement) in connection with: (i) the purchase and sale of real estate; (ii) entering into and transferring deeds of tenure and leases relating to real estate; (iii) the purchase and sale of shares, documents of title, mortgage deeds or other documents of title conveying the right to rent housing or other floor space in buildings; (iv) the purchase and sale of interests in companies if the sale is primarily aimed at transferring property rights; or (v) the purchase and sale of timeshares in holiday homes (Real Estate Business Act (REBA) s.1-1).

341. *Dealers in precious metals and dealers in precious stones:* Dealers in precious metals and stones are not obliged to identify all of their customers. The duty to carry out CDD measures only applies when carrying out: (i) cash transactions involving NOK 40 000 (EUR 4 800/USD 6 300) or more or a corresponding amount in foreign currency where it is suspected that a transaction involves money laundering or terrorist financing; or (ii) any cash transaction involving NOK 100 000 (EUR 12 100/USD 15 800) or more or a corresponding amount in foreign currency (MLR s.3). Where transactions comprise a series of operations that appear to be related with each other, these threshold amounts shall be computed on a collective basis. (MLA s.4 no. 8; MLR s.3).

342. *Lawyers and other independent legal professionals:* Lawyers and other persons who provide independent legal assistance on a professional or regular basis are obligated to identify their clients when assisting or acting on behalf of clients in planning or carrying out financial transactions, real estate transactions or transactions involving high-value goods exceeding NOK 40 000 (EUR 4 800/USD 6 300) (MLR s.2). The term *planning* is deemed to include preparations (MLA Prep. Works). The obligation also applies to preparing or carrying out transactions related to: (i) the purchase and sale of real estate; (ii) the management of the client's money, securities or other assets; (iii) the management of bank, savings or securities accounts; (iv) the organisation of contributions for the creation, operation or management of companies; and (v) the creation, operation or management of legal persons or arrangements, and buying and selling business entities (MLA Prep. Works, explanation of the term *financial transaction).* The obligation to identify customers also applies to lawyers and other independent legal professionals in the situations mentioned in article 2a of the second EU directive (i.e. when buying and selling real estate or business entities; managing client money, securities or other assets; opening or managing bank, savings or securities accounts; organising contributions necessary for the creation, operation or management of companies; or providing trust and company services) (MLA Prep. Works pp.38 and 103).

343. ***Applying Recommendation 6:*** Norway has not implemented any AML/CFT measures concerning Recommendations 6 that are applicable to Reporting BPs.

344. ***Applying Recommendations 8-9:*** Reporting BPs are not allowed to establish non-face-to-face business or introduced business.

345. ***Applying Recommendation 10:*** Record keeping requirements are generally satisfactory—other than the concerns relating to scope (in relation to company service providers) . The obligations for real estate agents actually exceed the five-year record keeping minimum; they are obligated to retain all documents in connection with a real estate transaction for at least 10 years (Regulations of 20 March 1990 No. 177 on Estate Agents, s.4-5; MLR 15).

4.1.2 Recommendations and Comments

346. Norway should implement Recommendations 5 and 6 fully and make these measures applicable to both Reporting FIs/BPs.

4.1.3 Compliance with Recommendation 12

	Rating	Summary of factors relevant to s.4.1 underlying overall rating

R.12	PC[96]	• Overall, the ratings for Recommendation 12 have been lowered due to concerns about the scope of application of AML/CFT obligations (in relation to company service providers). • The same serious deficiencies in the implementation of Recommendation 5 apply equally to Reporting FIs and Reporting BPs. In other words, customer identification requirements have been implemented, but full CDD requirements have not. • Norway has not implemented any AML/CFT measures concerning Recommendations 6 that are applicable to Reporting BPs.,

4.2 Monitoring of transactions and relationships (R.12 & 16) (applying R.11 & 21 to DNFBP)

4.2.1 Description and Analysis

347. ***Applying Recommendations 11 and 21:*** The obligations on DNFBPs to monitor their transactions and relationships are generally sufficient, other than the concerns relating to scope (in relation to company service providers). Because many of the DNFBP sectors only recently became subject to AML/CFT obligations, it is very early to be assessing the effectiveness of the system. However, some of the DNFBP sectors met with (particularly real estate agents, accountants and auditors, and dealers in precious metals/stones) were unclear as to why they were subject to the obligation. All DNFBP sectors asked for more specific guidance in how to meet their AML/CFT obligations. Considering the calls for more guidance as voiced by these sectors (particularly dealers in precious metals/stones) during the on-site visit, there are preliminary concerns about the effectiveness of implementation for both Recommendation 11 and 21. However, it should be noted that an acceptable level of reporting is occurring in all DNFBP sectors (considering how new the reporting obligations are for these sectors)—except in the case of dealers in precious metals/stones. It should also be noted that the FSA has established a working group (that includes representatives from industry organisations, ØKOKRIM and the FSA) that is currently working on guidelines (in the form of a circular) for auditors and external accountants. As well, the FSA continues to be heavily involved in training seminars (including close co-operation with the private sector on training issues), education and giving day-to-day advice by telephone. The Supervisory Council is currently participating in a working group that was created by the Ministry of Justice and which also consists of ØKOKRIM, the FSA and a representative from the NBA that is working on developing guidance for lawyers on their AML/CFT obligations. This work began in August 2004.

4.2.2 Recommendations and Comments

348. Supervisors in the DNFBP sectors should issue detailed and sector-specific guidance as soon as possible concerning what sorts of transactions could be considered unusual and related to ML/FT.

4.2.3 Compliance with Recommendation 12 and 16

	Rating	Summary of factors relevant to s.4.2 underlying overall rating
R.12	PC[97]	• Overall, the ratings for Recommendation 12 have been lowered due to concerns about the scope of application of AML/CFT obligations (in relation to company service providers).
R.16	LC[98]	• Overall, the ratings for Recommendation 16 have been lowered due to concerns about the scope of application of AML/CFT obligations (in relation to company service providers).

[96] This is an overall rating for compliance with Recommendation 12, based on the assessments in sections 4.1, 4.2 and 4.5 of this report.

[97] This is an overall rating for compliance with Recommendation 12, based on the assessments in sections 4.1, 4.2 and 4.5 of this report.

[98] This is an overall rating for compliance with Recommendation 16, based on the assessments in sections 4.2, 4.3, 4.4 and 4.5 of this report.

4.3 Suspicious transaction reporting (R.16) (applying R.13 & 14 to DNFBP)

4.3.1 Description and Analysis

349. ***Applying Recommendation 13:*** The obligations on DNFBPs to report suspicious transactions is satisfactory, other than the concerns relating to scope (in relation to company service providers) (see paragraph 333 above). For most DNFBPs, AML/CFT obligations are quite new. Consequently, it is very early to be assessing the effectiveness of the system. However, most of the DNFBP sectors met with (particularly real estate agents, accountants and auditors, and dealers in precious metals and stones) were unclear as to why they were subject to the obligation.[99] All DNFBP sectors asked for more specific guidance in how to meet their AML/CFT obligations. Considering the confusion voiced by these sectors during the on-site visit, there are concerns about the effectiveness of implementation for Recommendation 13. Nevertheless, it should be noted that all DNFBP sectors are reporting (with the exception of dealers in precious metals/stones) and, considering how recently these reporting obligations were implemented, these reporting levels would seem to be sufficient at this stage. The obligations on DNFBPs to monitor their transactions and relationships are generally sufficient, other than the concerns relating to scope and effectiveness of implementation by dealers in precious metals/stones (see paragraphs 333 above). Because many of the DNFBP sectors only recently became subject to AML/CFT obligations, it is very early to be assessing the effectiveness of the system. However, some of the DNFBP sectors met with (particularly real estate agents, accountants and auditors, and dealers in precious metals/stones) were unclear as to why they were subject to the obligation. All DNFBP sectors asked for more specific guidance in how to meet their AML/CFT obligations.

NUMBER OF STRs RECEIVED: BREAKDOWN BY SOURCE	
Type of Reporting BP filing the STR	2004
Lawyers	17
Accountants	8
Authorised accountants	25
Real estate agents	4

350. *Dealers in precious metals and stones:* Dealers in precious stones and metals are obliged to report to the FIU if they suspect that a transaction in cash of NOK 40 000 (EUR 4 800/USD 6 300) or more, is associated with the proceeds of a criminal act or terrorist financing (MLA s.7, s.4 no. 8).

351. *Lawyers and other independent legal professionals:* Lawyers and other independent legal professionals are only obliged to report transactions when there is a suspicion that a transaction is associated with the proceeds of crime or terrorist financing and when they assist or act on behalf of clients in planning or carrying out financial transactions (MLA s.4 no.7). The words *carrying out* include the situation of *engaging in*. Lawyers/independent legal professionals not obliged to report about matters that come to their knowledge in the course of their work on ascertaining a client's legal position (MLA s.12). This exemption applies when the lawyer/independent legal professional receives information initially in order to decide whether, or what kind of legal assistance that may be provided. Additionally, lawyers/independent legal professionals are not obliged to report prior to, during and subsequent to legal proceedings when such matters are directly associated with the legal dispute (MLA s.12). Unless the possibility of legal proceedings is pretty clear, this exemption does not apply. If the information that comes to the knowledge of the lawyer has nothing to do with the legal dispute, a

[99] It is encouraging to note, however, that since the on-site visit, there has been a positive trend of STRs being received from DNFBP sectors. In particular, in recent months, the MLU has received STRs as follows: 18 from lawyers, 4 from real estate agents, 9 from external accountants and 38 from auditors—all of which are considered to be "good reports" that have triggered several criminal investigations.

reporting obligation may arise, regardless of the duty of secrecy. However, if the information is related to a request for assistance in another (a new) matter, the lawyer may not be regarded as having accepted an assignment related to it, and then the law does not apply.

352. *Auditors:* The exceptions set out in the preceding paragraph also apply to auditors and other advisers with a reporting obligation when such persons assist a lawyer or other person who provides legal assistance on a professional or regular basis.

353. ***Applying Recommendation 14:*** The DNFBP sectors are prohibited from disclosing that an STR or related information is being reported to the MLU. In most of the DNFBP sectors, this obligation has been implemented adequately. However, there is some concern with the way this obligation is implemented with regards to lawyers/independent legal professionals. If a lawyer/independent legal professional does not accept the assignment, he may tell the client that he does not wish to do so because it would imply an obligation to file a report to the MLU. This is not considered as "tipping off" because a customer relationship has not yet been established and consequently the obligations in the MLA/MLR do not apply. The Supervisory Council confirmed that it would advise a lawyer that it is acceptable to advise a client the reason why the customer relationship is not being established. There is concern that this creates the possibility that a criminal could shop from lawyer to lawyer and test out different theories to determine what would have to be reported to the MLU and what would not.

4.3.2 Recommendations and Comments

354. Supervisors in the DNFBP sectors should issue additional detailed and sector-specific guidance as soon as possible concerning what sorts of transactions could be considered unusual and related to money laundering or terrorist financing. It would be preferable that lawyers be appropriately restricted or guided concerning what to advise a potential client when refusing to establish a customer relationship because it would imply an obligation to file a report to the MLU. In such circumstances, it should be sufficient to advise the potential client that the case cannot be accepted because of it would place the lawyer in a conflict of interest, rather than specifying that it would be the obligation to report to the FIU. However, this recommendation does not affect the rating.

4.3.3 Compliance with Recommendation 16

	Rating	Summary of factors relevant to s.4.3 underlying overall rating
R.16	LC[100]	• Overall, the ratings for Recommendation 16 have been lowered due to concerns about the scope of application of AML/CFT obligations (in relation to company service providers). • Considering the calls for more guidance as voiced by these sectors (particularly dealers in precious metals/stones) during the on-site visit, there are preliminary concerns about the effectiveness of implementation for Recommendation 13. However, it should be noted that reporting is occurring in all DNFBP sectors—except dealers in precious metals/stones.

4.4 Internal controls, compliance & audit (R.16) (applying R.15 to DNFBP)

4.4.1 Description and Analysis

355. ***Applying Recommendation 15:*** The obligations on DNFBPs to establish internal controls, compliance and audit systems are being implemented satisfactorily. In fact, all of the representatives from the DNFBP sector that the assessors met with had implemented some internal controls. However, there are still overall concerns relating to sufficiency of scope (in relation to company service providers).

[100] This is an overall rating for compliance with Recommendation 16, based on the assessments in sections 4.2, 4.3, 4.4 and 4.5 of this report.

356. *Real estate agents:* Real estate agents are obligated to establish internal controls and communication routines that ensure that the obligation to investigate suspicious transactions is complied with (MLR s.10). They are also obligated to operate in an appropriate manner in accordance with the law (FS Act s.3). Real estate agents are required to assign a person in the management with a special responsibility for following up the AML requirements and internal procedures; however, there is no legal requirement for them to establish a separate internal audit function.

357. *Accountants and auditors:* Accountants and auditors are obligated to establish internal controls and communication routines that ensure that the obligation to investigate suspicious transactions is complied with (MLR s.10) and to operate in an appropriate manner in accordance with the law (FS Act s.3). However, there is no legal requirement for these groups to establish a separate internal audit function.

4.4.2 Recommendations and Comments

358. Other than the overall concerns about sufficiency of scope (with regards to company service providers), the assessors have no additional comments with regards to this section.

4.4.3 Compliance with Recommendation 16

	Rating	Summary of factors relevant to s.4.4 underlying overall rating
R.16	LC[101]	• Overall, the ratings for Recommendation 16 have been lowered due to concerns about the scope of application of AML/CFT obligations (in relation to company service providers).

4.5 Regulation, supervision and monitoring (Applying R.17 and 24-25 to DNFBP)

4.5.1 Description and Analysis

359. ***Applying Recommendation 17:*** The DNFBP sectors are subject to sanctions for breaches of AML/CFT obligations, although it is unclear whether such sanctions could be applied to directors or senior management of DNFBPs. However, there are still overall concerns relating to sufficiency of scope (in relation to company service providers).

360. *Real estate agents:* Real estate agents are subject to the administrative sanctions mentioned in the Financial Supervisory Act and section 17 of the MLA. Sanctions are regularly used in connection with the FSA's inspections of real estate agents; however, none related to AML/CFT.

361. *Dealers in precious metals and stones:* Dealers in precious metals and stones are not monitored or supervised for compliance with AML/CFT obligations and are not subject to administrative sanctions, and there is no indication that Norway has considered this issue following a risk-based approach. In these circumstances, sanctions cannot be applied effectively to this sector.

362. *Lawyers and independent legal professionals:* The Supervisory Council audits lawyers to ensure that AML/CFT control routines are in place. If a lawyer/independent legal professional commits a crime, he/she can have his/her licence removed. Depending on the seriousness of the crime and the attendant circumstances, there is the possibility that a lawyer may not be able to have his/her licence reinstated. The Supervisory Council conducts a number of audits every year and will generally follow up on any economic irregularities that appear. If any irregularities that may be related to breaches of AML/CFT obligations, the Supervisory Council will follow up on a priority basis. Because it is not clear that the Supervisory Council has sufficient resources to supervise all of the persons/entities it is responsible for, it is not clear how effectively sanctions are applied to this sector.

[101] This is an overall rating for compliance with Recommendation 16, based on the assessments in sections 4.2, 4.3, 4.4 and 4.5 of this report.

363. *Accountants and auditors:* Accountants and auditors are subject to the administrative sanctions mentioned in the FSA and section 17 of the MLA. However, the FSA has not started conducting inspections of this sector and, consequently, has not applied sanctions. For now, sanctions are not being effectively applied to this sector.

364. ***Recommendation 24—****Casinos:* Although there are no land-based casinos in Norway, some internet gaming does exist; however, the sector is very limited and closely regulated. There is no explicit prohibition against a legal person having ownership interests in internet casinos. However, Norway reports that if a Norwegian company or natural person were discovered owning or operating an internet casino that is accessible in Norway, the activity could be stopped according to existing gaming legislation (Act on Lotteries s.11; Act Concerning Money Games s.2 para.3). These provisions prohibit the marketing and promotion of games that do not have the necessary permission that is required under section 6 of the Act on Lotteries. However, Norway has not taken any measures to identify whether there are any Norwegian residents/citizens who are currently: (i) owning or operating an internet casino; (ii) owning or operating a company that runs an internet casino; or (iii) owning or operating a server that is located in Norway and which is hosting an internet casino. Moreover, because Norway has not implemented customer due diligence obligations on financial institutions, such cases are unlikely to come to light through such persons opening a bank account or conducting other types of financial activity. Moreover, Norway has not issued any guidance to Reporting FIs or Reporting BPs alerting them to the possible existence of such entities and advising them of how to treat them.

365. *Real estate agents:* To be authorised to carry out activity as real estate agent, a person must either have a licence from the FSA or be a licensed lawyer who has also provided security (REAA s.1-2). The FSA supervises and is empowered to apply administrative sanctions to real estate agents. However, there is concern that the FSA does not have sufficient resources to effectively supervise real estate agents in addition to the other entities that it is responsible for. During on-site visits, the FSA checks AML-procedures and routines (as well as other areas). Real estate agents became subject to the provisions of the MLA and MLR as of 1 January 2004. The FSA has conducted 20 inspections of real estate agents (out of a total 1 683 real estate agencies, real estate agents and co-operative building associations) during which AML/CFT compliance was checked. The FSA has conducted one on-site inspection of a real estate agent without prior notice; however, this case did not involve AML/CFT. The following chart sets out the number of on-site inspections of real estate agencies that been carried out in the past six years. It should be noted that none of these inspections included AML/CFT checks. Norway reports that the drop in real estate agency inspections in 2003 was due to an urgent reallocation of resources from this area to a major rule-drafting effort in 2004 concerning amendments to the estate agency regulations.

NUMBER OF ON-SITE INSPECTIONS CONDUCTED BY THE FSA ON REAL ESTATE AGENCIES						
	1998	1999	2000	2001	2002	2003
General supervisory inspections	27	68	62	60	71	12
Inspections with an AML/CFT component	0	0	0	0	0	0

366. *Dealers in precious metals and stones:* Dealers in precious metals and stones are obliged to register their activity or company in Brønøysundregistrene; however, they are not obligated to obtain a licence or authorisation to carry out this business. The sector is not supervised or monitored by any agency, although industrial associations (such as the Jewellers Association and the NHO) play a role in helping members to understand and apply the new legal requirements.

367. *Lawyers and other independent legal professionals:* To practise law, one must receive a license issued by the Supervisory Council (CLA s.218). To obtain a license, a person must have (among other things) a law degree (5 years studies at the University) and documentation establishing blameless conduct. As well, an auditor must be engaged who will check the lawyer's compliance with AML

legislation (i.e. whether routines on control and reporting are established). The Supervisory Council supervises and is authorised to apply sanctions under section 17 of the MLA and section 225 of the Courts of Law Act (CLA) to lawyers and other independent legal professionals. The Supervisory Council is an independent body that carries out between 50-70 audits per year of law firms and all of the lawyers contained therein, either on the basis of received information or as random checks. The auditors examine all of the lawyers' files and books to determine whether the lawyers are complying with their legal obligations, including those related to AML. Although the auditor of the Supervisory Council has not received any specific AML training, he is fully apprised of the AML obligations that lawyers must comply with. In serious cases (including those relating to breaches of AML/CFT) the Supervisory Council may propose to the Advocate Licence Committee (see below) that the lawyer/legal professionals' licence be withdrawn. To date, the Supervisory Council has only uncovered one case of money laundering by a lawyer. However, every year, approximately five cases of fraud by lawyers are uncovered. Lawyers who work in-house are not subject to the obligations in the MLA; however, the Supervisory Council still audits them and supervises them as set out above.

368. The NBA is also responsible for ensuring compliance in this sector. Although lawyers can practise law without being members of the NBA, most lawyers in Norway (about 95%) do belong to it. The NBA has established ethical guidelines for lawyers. It has organised local disciplinary committees, which mainly deal with cases concerning possible contraventions of these ethical guidelines. In principle the local disciplinary committees are also competent in cases regarding other professional duties that apply to lawyers. Although the board of the NBA in certain cases is allowed to take up a case ex officio and submit it to the local committee, in practice the committees most often act on complaints made against NBA members. Additionally, the NBA can handle cases on non-members provided that they have consented. The decisions of the NBA's local committees may be appealed to the Disciplinary Committee which is appointed by the Government and handles cases in first. The Secretariat of the Disciplinary Committee is the NBA. The Disciplinary Committee is also competent in cases in first instances involving non-members of the NBA or second instances (i.e. complaints over decisions made by the regional committees). If the Supervisory Council or Disciplinary Committee find that it is necessary to withdraw a lawyer's license, the case will be submitted to the Advocate Licence Committee (for which the Supervisory Council serves as Secretariat). The Advocate Licence Committee deals with serious cases that might lead to loss or suspension of the licence. It handles cases that are referred to it by the Disciplinary Committee or the Supervisory Council.

369. ***Accountants and auditors:*** External accounting activity is a regulated profession in Norway and requires government authorisation. The FSA is responsible for licensing external accountants (both natural and legal persons). Licensed external accountants have higher qualifications than ordinary accountants (a higher qualification in economics equivalent to at least two years' full-time higher economic education and the equivalent of two years' relevant experience). The FSA is also responsible for supervising external accountants and checking that their activities comply with the applicable laws and regulations (including AML/CFT legislation). However, there is concern that the FSA does not have sufficient resources to effectively supervise accountants and auditors in addition to the other entities that it is responsible for. In addition to the MLA and MLR, external accountants are subject to the provisions of the Authorisation of External Accountants Act (AEAA). The AEAA regulates natural/legal persons that provide accounting or bookkeeping services for others on a commercial basis. NARF (which is the major professional body for Norway's authorised external accountants) is currently developing a quality control programme for accountants which is aimed at establishing a system which is similar to one currently in place for auditors.

370. Auditors must be authorised to practice (AA). To obtain an authorisation, a person must have completed approved theoretical training and had three years of varied experience. Practising auditors are required to provide security of NOK 5 million (EUR 606 000/USD 791 000) and meet the post-qualifying training requirements. Two categories of auditors are authorised to provide statutory auditing in accordance with the Eighth Council Directive of the European Communities 84/253/EEC—state authorised auditors and registered auditors (AA). Both categories are also entitled

to provide audit services to any company (with the exception of listed companies, which are subject to auditing by state authorised auditors only). No other Norwegian certificate grants the right to provide statutory auditing and audit services. Auditing firms must also obtain special authorisation to carry out auditing activities. To obtain authorisation, an auditing firm must be more than 50% owned by state authorised auditors, and the majority of the members of firms' boards of directors must be state authorised auditors. Requirements laid down in articles of association, and requirements as to financial probity, also apply.

371. The FSA is empowered to supervise and apply administrative sanctions to accountants and auditors (both natural/legal persons). As of October 2004, the FSA had not checked compliance with AML/CFT measures during its on-site inspections of state-authorised auditors, registered auditors or authorised external accountants because the scope of the reporting obligation has not yet been fully clarified for these sectors.[102] Effective from 2003, the FSA has formalised an agreement with the NIPA concerning guidelines for co-ordinating the control of auditors. These guidelines entail that all auditors/audit firms with audit responsibility are to be checked on five-year cycles. The quality control of auditors entails checking compliance with generally accepted auditing standards, laws and regulations. This requires a thorough assessment of the appropriateness of auditing methods, whether the scope of audit procedures is sufficient, whether the auditor's assessments and conclusions accord with the result of the audit procedures and whether satisfactory supporting documentation for the audit is available. This includes also auditors' compliance with the MLA and MLR. The NIPA imposes sanctions for malpractice and misconduct, in addition to following up inspections by the FSA. The following chart sets out the number of on-site inspections of auditors, external accountants and external accounting firms that have been carried out in the past six years. However, none of these inspections included an AML/CFT component.

NUMBER OF ON-SITE INSPECTIONS CONDUCTED BY THE FSA ON AUDITORS & ACCOUNTANTS						
	1998	1999	2000	2001	2002	2003
General supervisory inspections for auditors	82	128	80	73	32	19
General supervisory inspections for external accountants / external accounting firms[1 and 3]	–	47	147	62	41	35
Inspections for auditors, accountants or accounting firms that included an AML/CFT component	0	0	0	0	0	0

372. The DnR is the professional body for Norway's state-authorised and registered auditors. DnR members are subject to quality controls that are based, in part, on the International Standards on Auditing and Related Services (ISA) requirements as adapted to Norwegian legal requirements.

373. ***Applying Recommendation 25:*** In April 2004, the FSA issued general AML/CFT guidelines to all Reporting FIs and to the following Reporting BPs: real estate agents and housing associations that act as real estate agents; lawyers who are registered as real estate agents; authorised external accountants; and state-authorised and registered public auditors (Circular 9/2004). Circular 9/2004 is distributed to all Reporting FIs (including insurance companies and brokers, investment firms, management companies for securities funds and pension funds) and to real estate agents, state-authorised external accountants and registered public accountants. The FSA also issues guidelines on an ad hoc basis to real estate agents, accountants and auditors.

374. *Dealers in precious metals and stones:* Although the FSA has not specifically issued guidelines to dealers in precious metals and stones and Circular 9/2004 is not directed at this sector, it is

[102] The FSA intends to include compliance with AML measures as part of its on-site inspections once the scope of the reporting obligation for these sectors has been fully clarified.

indirectly relevant to the sector because many of the general provisions (which also apply to dealers in precious metals and stones) are further explained in this circular. Consequently, the MLU has taken the initiative to pass on information about Norway's new AML/CFT legislation, including the new reporting obligation for dealers in high-value goods, to industry organisations such as NHO and HSH.

375. *Lawyers and independent legal professionals:* The NBA has issued binding ethical guidelines for lawyers that are founded on secondary legislation. Part of these guidelines specifically refer to money laundering and state that a lawyer shall desist from an assignment when there is reason to believe that a transaction will imply money laundering, and the client is determined to proceed with the transaction (para.3.1.8). The NBA has also compiled a template for internal controls and communication routines. The NBA has published this template on the Internet. Additionally, the Ministry of Justice & Police has appointed a commission under its leadership, consisting of representatives from the NBA, the Supervisory Council, the MLU and the FSA. The AC/AML Unit is also involved in this work. The purpose of this commission is to draft AML/CFT guidelines for legal professionals. The commission was supposed to finalise a draft proposal by the end of 2004. However, the work is not yet completed. Then, the Ministry of Justice & Police intends to issue these guidelines to this sector. When the MLA came into effect, the Supervisory Council sent a letter to each lawyer in Norway. The letter contained a sentence advising lawyers that the provisions of the new MLA applied to them. After that letter was issued, the Supervisory Council received a few inquiries seeking elaboration about the responsibilities under the MLA. However, not many inquiries were received. To date, no formal guidance has been issued concerning these obligations; however, the inquiries that were received were responded to.

4.5.2 Recommendations and Comments

376. An authority should be designated to monitor and supervise dealers in precious metals/stones for compliance with AML/CFT obligations. Norway should be aware of issues relating to the illicit operation of internet casinos in Norway, and should be prepared to address these problems. The FSA should be given more resources for the purpose of supervising and monitoring. The FSA should issue more tailored and sector-specific guidance to DNFBPs concerning how to properly implement their AML/CFT obligations. By designating the FSA responsible for monitoring real estate agents, accountants and auditors for compliance with AML/CFT obligations, Norway has included these DNFBP sectors under the same supervisory regime that applies to the financial institutions sectors. Although this is commendable, it creates concerns about the sufficiency of the FSA's resources to supervise all of these entities.

4.5.3 Compliance with Recommendations 12 and 16 (DNFBP), 24 & 25 (criteria 25.1, DNFBP)

	Rating	Summary of factors relevant to s.4.5 underlying overall rating
R.12 and R.16	PC (R.12)[103] LC (R.16)[104]	• Overall, the ratings for Recommendations 12 and 16 have been lowered due to concerns about the scope of application of AML/CFT obligations (in relation to company service providers). • There is also concern that sanctions cannot be applied effectively to dealers in precious metals/stones since there is no designated authorities responsible for supervising their compliance with AML/CFT obligations.
R.24	LC	• Norway has not taken any measures to identify whether there are any Norwegian residents/citizens who are currently: (i) owning or operating an internet casino; (ii) owning or operating a company that runs an internet casino; or (iii) owning or operating a server that is located in Norway and which is hosting an internet casino. Moreover, because Norway has not implemented customer due diligence obligations on financial institutions, such cases are unlikely to come to light through such

[103] This is an overall rating for compliance with Recommendation 12, based on the assessments in sections 4.1, 4.2 and 4.5 of this report.

[104] This is an overall rating for compliance with Recommendation 16, based on the assessments in sections 4.2, 4.3, 4.4 and 4.5 of this report.

		persons opening a bank account or conducting other types of financial activity. Moreover, Norway has not issued any guidance to Reporting FIs or Reporting BPs alerting them to the possible existence of such entities and advising them of how to treat them. • Dealers in precious metals and stones are not monitored or supervised for compliance with AML/CFT obligations and are not subject to administrative sanctions, and there is no indication that Norway has considered this issue following a risk-based approach. • By designating the FSA responsible for monitoring real estate agents, accountants and auditors for compliance with AML/CFT obligations, Norway has included these DNFBP sectors under the same supervisory regime that applies to the financial institutions sectors. Although this is commendable, it creates concerns about the sufficiency of the FSA's resources to supervise all of these entities.
R.25	PC[105]	• Almost every reporting entity that the assessors met with asked for more specific and tailored guidance concerning AML/CFT obligations. (This language is consistent with language in table 1.)There was a breakdown in feedback in 2004 and face-to-face feedback was dropped.

4.6 Other non-financial businesses and professions

Modern secure transaction techniques (R.20)

4.6.1 Description and Analysis

377. ***Recommendation 20:*** In addition to the non-financial businesses and professions that are designated according to FATF Recommendations 12 and 16, the obligations under the MLA and MLR also apply to: (i) auctioneering firms and commission agents in connection with cash transactions of NOK 40 000 (EUR 4 800/USD 6 300) or more or a corresponding amount in foreign currency; and (ii) pawnshops (When a pawnshop grants credit against collateral, it becomes a financial institution pursuant to the Financial Services Act. Consequently, it must comply with all of the MLA and MLR) (MLA s.4). Independent investment advisers (that are not a bank, investment firm or accountant) are not regulated and supervised. However, if a Reporting FI has entered an agreement with such an adviser the Reporting FI itself assumes full and complete responsibility for ensuring compliance with AML legislation (MLA s.4; Circular 9/2004 p.22).

378. Norway has been taking steps to encourage the development and use of modern and secure techniques for conducting financial transactions that are less vulnerable to money laundering. The use of bankcards in Norway is now widespread, and the volume of cash in circulation relative to gross domestic product is low and decreasing. Additionally, Norwegian authorities, including the central bank, have encouraged the banking sector to establish an efficient infrastructure for electronic fund transfers. However, some sectors in the Norwegian economy use cash payments of up to several hundred thousand Norwegian kroner between commercial undertakings. This method of payment is particularly prevalent in the construction industry. Norway is considering whether rules should be introduced prescribing that commercial undertakings should normally use a bank when making payments to other commercial undertakings (i.e. prohibiting cash payments) (Action Plan 2004 chapter 11.2).[106]

4.6.2 Recommendations and Comments

379. Norway should continue to take measures to encourage the development and use of modern and secure techniques for conducting financial transactions that are less vulnerable to money laundering.

[105] This is an overall rating for compliance with Recommendation 25, based on the assessments in sections 3.7, 3.12 and 4.5 of this report.

[106] Such rules would be triggered by a threshold (i.e. they would apply to transactions over NOK 5 000 to 10 000 (EUR 610 to 1 210 / USD 790 to 1 580) in value. Although these measures are primarily directed at preventing tax crime, their implementation will also impact on the ability to launder money through companies.

4.6.3 Compliance with Recommendation 20

	Rating	Summary of factors underlying rating
R.20	C	• Recommendation 20 is fully observed.

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

380. ***Recommendation 33:*** The following types of legal persons exist in Norway: (a) Companies – limited companies and public limited companies; (b) Partnerships - general partnerships, general partnerships with shared liability, and limited partnerships; (c) Societies - house building co-operatives, housing co-operatives and co-operative societies; and (d) Organisations – Foundations, savings banks and associations.

381. Norway has several registries for legal persons. All Norwegian legal persons, and Norwegian and foreign companies or other legal persons conducting business activities in Norway are obligated to register with one or more registers. Different registers contain information identifying the legal person's directors, senior managers and shareholders. Some types of legal persons must also register their company accounts. Some of the information is readily accessible as many of these registers are publicly available. The shares in all companies are registered and there are no bearer shares.

382. Registered information concerning a particular legal person can be readily retrieved by virtue of Norway's single number identification system which ensures that, no matter which registry(ies) a legal person is registered with, it is always identified by the same unique identification number. Consequently, only one number needs to be checked. This ensures that information is not overlooked because it is stored under a different identification number or because there are double entries (under different numbers) for the same legal person.

383. Norway has implemented measures to ensure that registry information is kept accurate and up-to-date. For instance, following a change in its directors or senior management (in the case of public or limited companies registered in the Securities Register), a legal person is obligated to notify the applicable registers, within a reasonable time, to update this information. Legal persons that do not comply with this obligation can be sanctioned. In the case of public companies and limited companies that are registered in the Securities Register, current shareholder information is also available. Norway has also implemented a system whereby information that is updated/changed in one registry is automatically updated/changed in the others (something which is facilitated by the single number identification system). The following is a brief description of Norway's registers and the information that is available in each.[107]

384. ***Central Co-ordinating Register for Legal Persons (Central Co-ordinating Register) and associated registers:*** All Norwegian legal persons must register with the Central Co-ordinating Register. The Central Coordinating Register provides all new companies with a nine-digit organisation number, which is used to identify the legal person in all public business and industry registers. This helps public authorities to collaborate when collecting information on legal persons, prevents manipulation of such information and ensures precise identification of all legal persons. The following registers are specifically associated to the Central Co-ordinating Register and collect their information from it—the Register of Employers, the Value Added Tax Registration List, the Statistics Norway's Company Register, the County Governors' Register of Foundations, the Corporate Taxation Data Register and the Business Register.

385. ***Register of Business Enterprises (Business Register):*** All Norwegian and foreign business enterprises conducting business in Norway (including companies, partnerships, one-man businesses, etcetera) must register with the Business Register (which is one of the associated registers listed above). *Conducting business* refers to actually running an enterprise, but does not extend to merely holding/operating a bank account. The objective of this register is to provide the public with an updated overview of important information on a business enterprise. The Business Enterprise Registration Act establishes the rules for registering with the Business Register. The information contained in the register relates to the control of the entity. For instance, Norwegian limited companies must submit information on: the articles of association; the date of the company's formation; the company's registered address; the municipality of the business enterprise; the board members and deputy board members (if any); the serving chairman of the board; the general manager (managing director); the person(s) who represents the enterprise externally; and the person(s) who has the power to sign documents on behalf of the company. The registration for foreign companies conducting business in Norway shall include, *inter alia*, information about the business' proprietors and board members. Additional information on foreign companies that conduct business in Norway may also be available if the company has established a bank account. Section 16 of the Financial Contracts Act states that an agreement establishing a bank account must contain the proprietor's name, address, personal identification number or organisation number. Business enterprises are also required by law to submit certain notifications to the Business Register. For instance, notifications shall enclose certain documents such as a certified copy of the memorandum of association, or declarations from the auditor or board member that they accept the election. The Registrar shall verify whether the notifications are submitted, the basis for them and their formulation are in accordance with the law, although it does not verify the facts behind the submitted notifications. If a business enterprise is required to submit a notification on a particular matter, but fails to do so or does so inaccurately, that matter cannot be brought to bear against a third party unless the third party was aware of (or should have been aware of) the matter. Any person has the right to access the information that is recorded in the Business Register. Additionally, some of that information must be made public in the National Gazette.

386. ***Register of Company Accounts:*** All Norwegian limited companies, public limited companies, savings banks, mutual insurance companies and petroleum enterprises are obliged to submit their annual accounts (including the auditor's report) to the Register of Company Accounts (Act relating to Company Accounts) within one month of being adopted by the annual general meeting (or by 1 August at the latest). If the annual accounts are submitted too late, the company must pay a default fine. If the annual accounts have not been submitted within six months after the deadline expires, the Bankruptcy Court may force dissolution of the company. The company's own Board of Directors is responsible for ensuring that the content of the annual accounts and report complies with the requirements set out in the Act relating to Company Accounts. The Register of Company Accounts only confirms that all of the necessary documentation is been attached, and that the annual accounts were adopted by the company's annual general meeting. The Register of Company Accounts stores the annual accounts and reports for ten years and makes them publicly available

387. ***Securities register:*** Norwegian public limited companies must set up their register of shareholders in a Securities Register that is maintained in Norway (Act no.64 of 5 July 2002). Private limited companies may choose between establishing their register in the Securities Register or in a Book of Shareholders. However, if a private limited company chooses to maintain a Book of Shareholders, it shall be publicly available at the company's address in Norway.

388. ***Corporate Taxation Data Register (the Corporate Taxation Register)***: Since 31 December 2004, Norway has implemented a Corporate Taxation Register that contains information identifying the shareholders of Norwegian legal persons who are obligated to pay tax in Norway. Such information is collected primarily for tax purposes, but is also accessible to the police and the MLU once a criminal investigation has begun and there is a cause to suspect that an offence punishable by a sentence of imprisonment for more than six months has been committed. A legal person is obligated to update the

information in this register once a year and it is a criminal offence to not give the required information to the tax authorities.

389. ***Register of Foundations (stiftelser):*** A new Act on Foundations was adopted on 15 June 2001. This Act came into force on 1 January 2005. Under this Act, all foundations are registered in a national Register of Foundations which will be maintained by a national supervisory agency. The registration shall include, *inter alia*, the name of the founder, the members of the board, which assets that go into the foundation, and special rights given to the founder. The foundation may not distribute capital or other benefits to the founder. The supervisory agency shall have access to all information necessary to perform effective supervision of the foundation.

390. In addition, to the publicly available registers, Norway also obligates all Norwegian private and public limited companies to establish and maintain a register of all shareholders, including their name, date of birth and address, (or for legal entities—business name, organisation number and address). The register of shareholders much be kept up-to-date at the company's head office and must be available to the public. When a new owner has reported and documented his acquisition of a share, the company is obligated to register the new owner without delay. If the register is kept electronically, a transcript no older than three months shall be available. Upon request, the company is obligated, within a week, to present an alphabetical list of changes in ownership which has taken place after the transcript was made. Foreign companies are allowed to own shares of Norwegian companies. In such cases, the register of shareholders will reflect the name, organisation number and address of the foreign company. If the Norwegian authorities need to know information about the foreign company's chain of ownership, they are entitled to ask foreign company for that information. However, the information accessible in the foreign company will normally depend on what information their home state requires the company to register about their owners. The Norwegian authorities have no legal competence to regulate foreign companies that are established abroad. To facilitate information exchange as regards shareholders which are foreign companies, the FSA has entered into MOUs with all of the European countries and some other countries.

391. The measures described above ensure that accurate, adequate and reasonably current information concerning the ownership and control of Norwegian legal persons is readily accessible to competent authorities in a timely fashion. However, it should be noted that these measures do not relate to information concerning beneficial ownership (as that term is used in the FATF Recommendations). The Glossary of the FATF Recommendations defines *beneficial owner* as "the natural person(s) who ultimately owns or controls a customer and/or the person on whose behalf a transaction is being conducted. It also incorporates those persons who exercise ultimate effective control over a legal person or arrangement". While the concept of beneficial ownership (as that term is legally understood in common law systems) is not recognised in a civil law system like Norway's, it should be noted that the FATF definition remains applicable factually, in relation to ultimate effective control. This definition is also applicable to financial institutions as part of the obligations under Recommendation 5 to identify beneficial owners.

392. Nevertheless, Norway has implemented the following additional measures that go some way to ensuring that the person who exercises ultimate effective control over a legal person can be identified. First, buying/selling acquisition of shares in listed companies are subject to disclosure rules. Such acquisitions above certain thresholds should be reported to the stock exchange (in addition to the shareholder registry rules).

393. Second, Norwegian law prohibits the buying/selling of shares (of public limited and limited companies that are registered in the Securities Register) through a nominee, except for foreign investors and only then with safeguards to ensure transparency. For instance, only a bank or another administrator (such as a securities firm or management company for securities) who has been specially licensed by the FSA to act as a nominee may act as a nominee. Such a nominee may be registered as the owner on behalf of the foreign shareholder. However, to ensure transparency of the nominee relationship, the register of shareholders (which must be publicly available) must include the nominee's name and

address, and state that he/she is a nominee of the shares. Additionally, the nominee's license sets out conditions requiring the nominee to maintain information identifying the beneficial owner and to give all information concerning the beneficial owner of the shares to the authorities upon request.

394. Third, bearer shares do not exist in Norway. Consequently, there is transparency concerning the identity of the owner of a share.

5.1.2 Recommendations and Comments

395. Norway's system of several public registries and registers of shareholders held by companies (which are also publicly available) ensure that accurate, adequate and reasonably current information concerning the ownership and control of Norwegian legal persons is readily accessible to competent authorities in a timely fashion. Additionally, the following rules provide a measure of transparency concerning beneficial ownership: (i) shareholders acquiring shareholdings (above certain thresholds) in listed public companies must disclose themselves; (ii) prohibiting the buying/selling of shares (of all that are registered in the Securities Register) through a custodian is prohibited, except in very limited cases and only then with safeguards to ensure transparency; and (iii) bearer shares are prohibited.

396. Nevertheless, concerning beneficial ownership, additional steps could be taken such as obligating shareholders (particularly shareholders who are legal persons) to: (i) disclose whether another person is the ultimate controller of those shares; and (ii) provide information identifying the ultimate controller. This could include obligating legal persons who are shareholders to provide identification information down to the natural person who ultimately controls the shares. An additional measure would be to obligate legal persons to record the information so disclosed (concerning beneficial ownership) in its register of shareholders and ensuring that (as now) the register of shareholders is publicly available. Norwegian law enforcement and prosecutorial are not prohibited from requesting shareholders or legal persons to provide information concerning beneficial ownership; however, the measures described above would provide much more timely access to this sort of information.

5.1.3 Compliance with Recommendations 33

	Rating	Summary of factors underlying rating
R.33	LC	• Norway could provide much more timely access to information concerning beneficial ownership.

5.2 Legal Arrangements – Access to beneficial ownership and control information (R.34)

5.2.1 Description and Analysis

397. ***Recommendation 34:*** Norwegian law does not recognise the legal concept of a trust, including trusts created in other countries. Equally, Norway advised that there are no other legal arrangements that are of a similar nature to a trust, or which would otherwise meet the definition of a "legal arrangement" as defined in the FATF Recommendations. Nevertheless, Norwegian lawyers do, from time to time, handle trusts located abroad. Norway reports that when handling trusts abroad, Norwegian lawyers are subject to the same legal regime as when assisting Norwegian persons/entities, including the obligations under the MLA/MLR (i.e. customer identification, record keeping, STR reporting, etcetera).

5.2.2 Recommendations and Comments

398. Recommendation 34 is not applicable in the Norwegian context.

5.2.3 Compliance with Recommendations 34 - Not applicable

	Rating	Summary of factors underlying rating
R.34	NA	• Recommendation 34 is not applicable in the Norwegian context.

5.3 Non-profit organisations (SR.VIII)

5.3.1 Description and Analysis

399. ***Special Recommendation VIII:*** Although Norway has not yet carried out a review of the laws and regulations that relate to non-profit organisations (NPOs) that may be abused for the financing of terrorism, it has given some consideration to the above-noted risks associated with this sector. To address this issue, the FNH has submitted a proposal to the FSA that would require all legal persons to register in a public register as a condition to establishing business relationships with a financial institution. The proposal suggests a simplified registration in the Central Co-ordinating Register and the assignment of a separate number series to keep these legal persons separate from ordinary registered legal persons. The Government will take the initiative to assess registration obligation of legal persons that wish to establish business relationships with a financial institution (Action Plan 2004). Currently, charitable organisations, associations, investment clubs and collection accounts are not obligated to register in the Business Register (Circular 9/2004 s.2.5). Consequently, when such groups open bank accounts, they must do so in the name of one of their members (a natural person) (MLR s.6). The FSA specifically advises Reporting FIs/BPs that so-called collection accounts for charitable organisations should not be exempt from the requirements to produce identity documents (Circular 9/2004 s.2.4).[108] Nevertheless, this situation is unsatisfactory for the bank because it hinders its ability to identify the actual owners of the funds in an account pursuant to its obligations under the Money Laundering Act and Regulations. Nor is this a satisfactory situation for the natural person who is registered as the account holder, because this person is subject to tax on the funds concerned (Action Plan 2004 pp.38-39).[109] The system is further weakened by the fact that Recommendation 5 has not been implemented with regards to beneficial ownership. Norway has not implemented measures to ensure that terrorist organisations cannot pose as legitimate NPOs, or to ensure that funds/assets collected by or transferred through NPOs are not diverted to support the activities of terrorists or terrorist organisations.

5.3.2 Recommendations and Comments

400. Norway should conduct a review of the adequacy of its laws and regulations relating to NPOs that can be abused for the financing of terrorism. Norway should implement measures to ensure that terrorist organisations cannot pose as legitimate NPOs. Norway should implement measures to ensure that funds or other assets collected by or transferred through NPOs are not diverted to support the activities of terrorists or terrorist organisations.

[108] The exemption referred to here is set out section 5 of the MLR. When a customer is unable to produce the identity documents required by section 4 of the MLR, the Reporting FI may still establish a customer relationship or carry out the requested transaction if: (i) the Reporting FI is certain of the customer's identity; (ii) the Reporting FI has reason to believe that the customer does not possess identity documents; and (iii) it is unreasonable in view of the customer's age or state of health to require him/her to obtain identity documents. Nevertheless, even in these cases, the Reporting FI must still obtain and register the identification data required by section 6 of the MLA by other means.

[109] The Act on Foundations (which was adopted on 15 June 2001 and is not yet in force) will require all foundations to register the name of the founder, the members of the board, which assets that go into the foundation, and special rights given to the founder in a national Register of Foundations. Foundations will be prohibited from distributing capital or other benefits to the founder. The supervisory agency shall have access to all information necessary to perform effective supervision of the foundation

5.3.3 Compliance with Special Recommendation VIII

	Rating	Summary of factors underlying rating
SR.VIII	NC	• Norway has not yet carried out a review of the laws and regulations that relate to non-profit organisations (NPOs) that may be abused for the financing of terrorism. • Norway has not implemented measures to ensure that terrorist organisations cannot pose as legitimate NPOs, or to ensure that funds/assets collected by or transferred through NPOs are not diverted to support the activities of terrorists or terrorist organisations. • The system is further weakened by the fact that Recommendation 5 has not been implemented with regards to beneficial ownership.

6 NATIONAL AND INTERNATIONAL CO-OPERATION

6.1 National co-operation and coordination (R.31)

6.1.1 Description and Analysis

401. ***Recommendation 31:*** Norway has implemented mechanisms that facilitate domestic co-operation at both the operational and policy levels. On an operational level, the FSA is authorised to co-operate with ØKOKRIM, domestic enforcement authorities, as well as with other domestic and foreign supervisors for AML/CFT purposes. The police and Prosecution Authority (including the MLU) are exempt from their duty of confidentiality for the purpose of preventing and investigating crime (CPA s.61a). This exemption allows all domestic competent authorities that are involved in AML/CFT efforts to co-operate and co-ordinate their efforts. Twice a year, the management of ØKOKRIM and the management of the FSA, the Tax Directorate and the Customs Directorate meet to discuss, among other things, AML/CFT matters. Regular contact meetings also take place between the MLU, the FSA, the Tax Directorate, the Customs Directorate, Norges Bank and the National Insurance Administration. These meetings comprise general and specific AML topics and matters, and have been going on for many years. Recently, a new and permanent forum on terrorist financing was initiated consisting of representatives from the PST, ØKOKRIM, Oslo Police District and the Customs Directorate. Its first meeting was held in November 2004. The objective of the forum is to co-ordinate CFT efforts and to exchange information about trends and observations as well as methods to fight terrorist financing. These authorities also have contact on an ad-hoc basis. Since 2003, co-operation between the MLU and PST has increased. Information about persons and organisations contained in STRs are regularly exchanged based on special forms developed in co-operation with the PST. Contact also takes place between the MLU's designated special terrorist financing investigator and designated contact persons at the PST. Responses to the PST's requests for information from the MLU, are stored in the database ("Non bank requests"-base). Requests from the PST are also stored in an own file. If information from STRs form the basis for investigation, it will be determined who shall undertake the investigation—the ordinary police or the PST. As well, ØKOKRIM and the PST have established an interdisciplinary operative forum against terror financing. The participants are staff members from ØKOKRIM, the PST, the Police District of Oslo, the Customs Directorate, the Tax Crime Unit in Akershus, and soon also the Police Foreign Unit (*Politiets utlendingsenhet*). The New National Bureau of Crime Investigation will also participate.

402. Although formal meetings do take place, solid outcomes do not always seem to result. Norway acknowledges that there is still room for improvement in more effective interagency co-operation.

403. The Action Plan 2004 purports to set out a plan of co-operation and co-ordination among all government bodies with regards to the implementation of AML/CFT measures. The EMØK (the Senior Public Officials Group on Economic Crime) which is comprised of senior government officials from ØKOKRIM and the Ministries of Justice & Police, Finance, Trade & Industry, Labour & Social Affairs, and Modernisation. It is specifically mandated to follow up on the implementation of the Action Plan 2004. This includes identifying possible budgetary needs, and communicating those findings as part of the ordinary annual budget procedures. Budgets for the police and Prosecution Authority have steadily risen in

recent years. However, the Norwegian government acknowledges that there is room for improvement regarding the ability of police and the Prosecution Authority to investigate and prosecute economic crime cases, including ML cases. This lead to the recommendation in the Action Plan 2004 that all police districts should establish multi-professional economic crime teams with expertise in legal, police and economic matters. It was also emphasised that it was important to ensure that the teams actually function as teams, have an adequate size, are stable, and have the right personnel with appropriate training and competence to enable them to deal with large and complex economic crime cases. Although the original deadline for implementing these teams was the end of 2004, that deadline has been extended to 01 July 2005. Norway reports that as of 25 April 2004, the process is near completion with only one police district still in the process of planning its team.

6.1.2 Recommendations and Comments

404. Norway should take steps to improve co-ordination at all levels. Norway should ensure that sufficient resources are allocated to implement the recommendations in the Action Plan 2004.

6.1.3 Compliance with Recommendation 31

	Rating	Summary of factors underlying rating
R.31	LC	• Although formal meetings do take place, solid outcomes do not always seem to result. • There is still room for improvement in more effective interagency co-operation.

6.2 The Conventions and UN Special Resolutions (R.35 & SR.I)

6.2.1 Description and Analysis

405. ***Recommendation 35 and Special Recommendation I:*** Overall, Norway has largely implemented all three Conventions and is, consequently, largely compliant with Recommendation 35.

406. *Implementation of the Vienna Convention:* Norway became a party to the Vienna Convention on 14 November 1994 and has fully implemented the vast majority of those elements of it that are relevant to the FATF Recommendations. The remaining minority of elements are largely implemented.

407. *Implementation of the Palermo Convention:* Norway became a party to the Palermo Convention on 23 September 2003 and has fully or largely implemented the vast majority of those elements of it that are relevant to the FATF Recommendations. There is, however, one element that is insufficiently implemented. Article 6(2)(e) of the Convention obligates countries to make self-laundering an offence unless it is contrary to fundamental principles of domestic law. As set out in paragraph 79 above, self-laundering is not an offence in Norway, but this cannot be justified on the basis of its being contrary to a fundamental law.

408. *Implementation of the Terrorist Financing Convention:* Norway signed the Terrorist Financing Convention on 1 October 2001 and ratified it on 14 August 2002. Norway has fully or largely implemented the majority of those elements of the Terrorist Financing Convention that are relevant to the FATF Recommendations. However, article 18(1)(b) of the Convention which requires countries to implement efficient measures to identify customers in whose interest accounts are opened is insufficiently implemented. As set out in paragraphs 212, 230, 375 and 381 above, Norway's implementation of Recommendation 5 does not include adequate measures to ascertain the identity of beneficial owners.

409. Overall, Norway has largely implemented the Terrorist Financing Convention and S/RES/1267(1999); however, it's implementation of S/RES/1373(2001) is inadequate. Consequently, overall, Norway is only partially compliant with Special Recommendation I.

410. *Implementation of S/RES/1267(1999):* Norway has largely implemented the basic legal provisions of S/RES/1267(1999) and its successor resolutions that relate to the FATF

Recommendations. However, although Norway has implemented measures that penalise breaches of freezing orders issued pursuant to S/RES/1267(1999), it does not monitor or supervise for compliance with this requirement (as required by section 8 of the resolution).

411. *Implementation of S/RES/1373(20001):* Norway's implementation of S/RES/1373(2001) is not adequate enough (see paragraphs 133 to 138 of this report). No effective mechanisms exist for communicating actions taken under S/RES/1373(2001) to the financial sector. Moreover, there are no specific measures in place to monitor compliance with the obligations pursuant to S/RES/1373(2001).

412. *Additional elements:* Norway has gone farther than the FATF Recommendations require by participating in other international conventions that are relevant to AML/CFT. For instance, Norway has been a party to the Strasbourg Convention since 16 November 1994. Norway has also ratified the following binding international instruments considered relevant in the fight against terrorism: (i) the Convention for the Suppression of Unlawful Seizure of Aircraft; (ii) the Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation; (iii) the Convention on the Prevention and Punishment of Crimes against Internationally Protected Persons, including Diplomatic Agents; (iv) the International Convention against the Taking of Hostages; (v) the Convention on the Physical Protection of Nuclear Material; (vi) the Protocol for the Suppression of Unlawful Acts of Violence at Airports Serving International Civil Aviation, supplementary to the Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation; (vii) the Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation; (viii) the Protocol for the Suppression of Unlawful Acts against the Safety of Fixed Platforms located on the Continental Shelf; (ix) the International Convention for the Suppression of Terrorist Bombings; and (x) the International Convention for the Suppression of the Financing of Terrorism (1999).

6.2.2 Recommendations and Comments

413. Norway should fully implement: article 6(2)(e) of the Palermo Convention by making self-laundering a criminal offence; article 18(1)(b) of the Terrorist Financing Convention by implementing effective measures to identify beneficial owners; article 18(1)(b) of the Terrorist Financing Convention by implementing effective measures to identify beneficial owners; section 8 of S/RES/1267(1999) by implementing measures to supervise and monitor reporting entities for compliance with freezing orders issued pursuant to this resolution; and S/RES/1373(2001).

6.2.3 Compliance with Recommendation 35 and Special Recommendation I

	Rating	Summary of factors underlying rating
R.35	LC	• Implementation of the Palermo Convention: Article 6(2)(e) of the Convention obligates countries to make self-laundering an offence unless it is contrary to fundamental principles of domestic law. Self-laundering is not an offence in Norway, but this cannot be justified on the basis of its being contrary to a fundamental law. • Implementation of the Terrorist Financing Convention: Article 18(1)(b) of the Convention requires countries to implement efficient measures to identify customers in whose interest accounts are opened is insufficiently implemented. Norway's implementation of Recommendation 5 does not include adequate measures to ascertain the identity of beneficial owners.
SR.I	PC	• Implementation of the Terrorist Financing Convention: Article 18(1)(b) of the Convention requires countries to implement efficient measures to identify customers in whose interest accounts are opened is insufficiently implemented. Norway's implementation of Recommendation 5 does not include adequate measures to ascertain the identity of beneficial owners. • Implementation of S/RES/1267(1999): Although Norway has implemented measures that penalise breaches of freezing orders issued pursuant to S/RES/1267(1999), it does not monitor or supervise for compliance with this requirement (as required by section 8 of the resolution). • Implementation of S/RES/1373(2001): Norway's implementation of S/RES/1373(2001) is not adequate enough. No effective mechanisms exist for communicating actions taken under S/RES/1373(2001) to the financial sector. Moreover, there are no specific measures in place

		to monitor compliance with the obligations pursuant to S/RES/1373(2001).

6.3 Mutual Legal Assistance (R.32, 36-38, SR.V)

6.3.1 Description and Analysis

414. ***Recommendation 36 and Special Recommendation V:*** Norway's mutual legal assistance measures apply equally to ML matters (Rec.36) and FT matters (SR. V). Norway does not have a separate mutual legal assistance act. Provisions regulating mutual legal assistance in the Norwegian legal framework are to be found in different laws and regulations. For instance, the Extradition Act (EA) contains a separate chapter (chapter V) on mutual legal assistance. Norwegian legislation provides for the possibility of giving effect to requests for mutual legal assistance irrespective of the existence or applicability of a treaty. It also contains provisions regulating letters rogatory, including which authorities are competent to issue them (CPA, ss.46-50; Regulation relating to the administration of the prosecution authorities, chapter 6). The conditions that apply to handling a mutual legal assistance request depend upon: (i) whether and which convention is applicable; and (ii) if the request involves coercive measures.

415. *Mutual legal assistance requests from countries other than Schengen or Nordic countries:* For mutual legal assistance requests from countries (other than the Schengen or Nordic countries) that relate to coercive measures, Norway applies some of the conditions (including dual criminality) as it does to extradition requests (EA s.24(3)). These conditions are: (i) the offence must be punishable under Norwegian law (dual criminality); (ii) if the request relates to a military offence, the act must be punishable under ordinary Norwegian criminal law (EA s.4); (iii) the underlying offence must not be a political offence (EA s.5); and (iv) there can be no grounds for believing that there is a grave danger that the person will be persecuted by reasons of race, religion, political conviction or other serious reasons (EA s.6). If a request does not entail the use of coercive measures (such as search and seizure), assistance may be provided without the need to establish dual criminality.

416. *Mutual legal assistance requests from European countries (other than Schengen or Nordic countries):* The provisions of the European Convention on Mutual Legal Assistance (ECMLA) apply to all mutual legal assistance requests from other ECMLA signatories (other than Schengen and Nordic countries).[110] Norway ratified the ECMLA on 12 June 1962 and, in doing so, made a reservation to article 5. The reservation implies that requests for search and seizure are subject to the following conditions: (i) the underlying offence must be punishable under the law of Norway and the requesting country (dual criminality); (ii) the underlying offence must be extraditable in the requesting country; and (iii) the execution of the letters rogatory is consistent with the law of the requesting country. However, this reservation has been modified in relation to the Schengen and Nordic countries (EA s.24(3)).

417. *Mutual legal assistance requests from Schengen countries (other than Nordic countries)*: For mutual legal assistance requests from Schengen countries[111] (other than the Nordic countries), there is

[110] The Schengen agreement was signed on 14 June 1985 by Belgium, France, Germany, Luxembourg and the Netherlands for the purpose of ending border checkpoints and controls between those countries, and harmonising external border controls. Originally separate from the EU (then the European Community), Schengen has since become an EU competence. As of 29 January 2005, there were 46 signatories to the ECMLA: Albania, Andorra, Armenia, Austria, Azerbaijan, Belgium, Bosnia and Herzegovina, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Georgia, Germany, Greece, Hungary, Iceland, Ireland, Israel, Italy, Latvia, Liechtenstein, Lituania, Luxembourg, Malta, Moldova, Netherlands, Norway, Poland, Portugal, Romania, Russian Federation, San Marino, Servia and Montenegro, Slovakia, Slovenia, Spain, Sweden, Switzerland, the former Yugoslave Republic of Macedonia, Turkey, Ukraine and United Kingdom.

[111] As of 29 January 2005, the there were 26 signatories to the Schengen Convention: Austria, Belgium, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Slovakia, Slovenia, Spain, Sweden and Switzerland.

no requirement that the underlying offence be extraditable according to Norwegian law (EA s.24(3)). However, dual criminality still applies.

418. *Mutual legal assistance requests from Nordic countries*: Norway has implemented streamlined and effective measures for handling mutual legal requests from Nordic countries. For mutual legal assistance requests originating from Nordic countries (Denmark, Finland, Iceland and Sweden), there is no requirement that the underlying offence be extraditable according to Norwegian law and (unless the underlying offence is a political offence) dual criminality does not apply, even if the assistance sought requires the use of coercive measures (EA s.24(3)).

419. Requests for coercive measures must: (i) be accompanied by a decision issued by the competent authority of the requesting state; (ii) include information on the nature, time and place of the criminal offence; and (iii) explain that the use of coercive measure is in accordance with the legislation of the requesting state. Then, the request must be carried out in compliance with Norwegian law and procedures (i.e. the CPA). The same range of coercive measures and criminal procedures that are available in domestic proceedings are available in mutual legal assistance requests that relate to ML/FT investigations, prosecutions and related proceedings (EA s.24(1)). In both the domestic and mutual legal assistance contexts, application of these measures is governed by the same general regulation on coercive measures and criminal procedure. When providing mutual legal assistance, Norway can order the production and seizure of information, documents of evidence, including financial records from financial institutions independent of whether legal professional secrecy applies. Courts have jurisdiction to order production of bank records (CPA ss.210-210c) and/or seizure of records (CPA s.203). For instance, the court may decide that a bank shall produce bank information in a corruption case. The production order will be made on the condition that the evidence may be significant in the case and that the possessor is obliged to give statement as witness in the case. Seizure may be terminated on the decision of the prosecution authority or the court. Norway also has the ability to compel witness testimony in mutual legal assistance matters (CPA s.237)**.** The use of coercive measures such as charging and seizing is set out in Chapter 16 and 17 of the CPA. There is no rule under Norwegian law that a mutual legal assistance request must be refused if the offence is considered to involve fiscal matters, or if there is an applicable law requiring maintenance of secrecy or confidentiality.

420. As a general rule, mutual legal assistance requests must be forwarded through the Ministry of Justice & Police which is the designated central authority pursuant to a number of conventions. Requests for judicial assistance are treated as matters of urgency within the Ministry of Justice & Police. To facilitate a prompt response, a circular letter describing the mutual legal assistance procedure is distributed by the Ministry of Justice & Police to the courts and prosecuting authorities. Additionally, Ministry staff are available every weekday to answer questions submitted by telephone, e-mail and post. Other channels of communication in relation to mutual legal assistance are also available. Pursuant to the Strasbourg Convention and the COE Corruption Convention, the Norwegian FIU (the MLU) is the designated central authority. Co-operation between Nordic and Schengen countries is streamlined in that it is channelled directly between the judicial authorities. Additionally, the King in Council (the cabinet of all ministers of the Government) may designate another central authority or decide that requests may be forwarded directly to a judicial authority; however, to date no further designations have been made. In this regard, there is co-operation between the FSA and its counterpart regulators. No information concerning how long it takes to process a mutual legal assistance or extradition request is available, but Norwegian authorities say that they give them priority.

421. The figures below related to mutual legal assistance involve all the requests handled by the Ministry of Justice & Police, including requests for charging, seizing and confiscation. The numbers provided do not include the requests for mutual legal assistance sent directly between the judicial authorities pursuant to the Schengen convention or the Nordic agreement for mutual legal assistance

dated 26 April 1974. The following chart sets out the total number of requests for mutual legal assistance in criminal cases, which were sent/received through the Ministry of Justice & Police.

NUMBER OF MUTUAL LEGAL ASSISTANCE REQUESTS TO/FROM NORWAY				
Mutual Legal Assistance	2000	2001	2002	2003
To Norway	245	315	257	202
From Norway	91	76	40	76
Total	336	391	297	278

422. Mutual legal assistance (other than that provided to the Schengen and Nordic countries) must always proceed by letters rogatory. The following chart sets out the total number of rogatory letters that were forwarded to and received by ØKOKRIM on the basis of the OECD Bribery Convention. In the chart below, "F" means the annual number of rogatory letters forwarded and "R" means the annual number of rogatory letters received. It should also be noted that the figures in this chart refer to the first rogatory letter from the authorities in each investigation case; they do not include later additional rogatory letters from the same authorities within the same cases (i.e. follow-up requests). It should be noted that it is not efficient to proceed by way of letters rogatory.

NUMBER OF LETTERS ROGATORY TO/FROM NORWAY									
2000		2001		2002		2003		2004	
F	R	F	R	F	R	F	R	F	R
2	1	-	-	1	2	4	1	-	-

423. Norway has no internal legislation that stipulates an obligation to ensure the prosecution of cases that are subject to prosecution in more than one country. However, some of the international conventions that Norway has signed and ratified contain a clause saying that a state party in the territory of which an alleged offender is present, shall, if it does not extradite that person, be obliged to submit the case without undue delay to its competent authorities for the purpose of prosecution, through proceedings in accordance with the laws of that State (*aut dedere aut judicare*) (e.g. article 10 of the Terrorist Financing Convention). By ratifying a convention which contains such a clause, Norway becomes (to a certain extent) obliged to prosecute cases that are subject to prosecution in more than one country. Norway is co-operating closely on a global and region level to avoid conflicts regarding investigation and prosecution of cases concerning transnational crime.

424. Overall, the system for providing mutual legal assistance to Nordic countries is straightforward and subject to very few restrictions. Given Norway's geographical proximity, it would be reasonable to assume that most of the mutual legal assistance requests it receives will have originated in other Nordic countries. The system for mutual legal assistance to Schengen countries is also more streamlined in that it is not necessary for the underlying offence to be extraditable in Norway. However, in all cases involving mutual legal assistance requests from non-Nordic countries (where coercive measures are being sought), dual criminality applies. Additionally, for non-Schengen countries some of the other requirements that apply to extradition requests also apply. This may be overly restrictive and may impede the system's effectiveness if the principle of dual criminality is interpreted too strictly. For instance, because conspiracy to commit ML is not fully criminalised in Norway, it is not clear whether mutual legal assistance could be provided in cases where the mutual legal assistance request relates to self-laundering or a conspiracy to commit ML where the conspiracy does not occur in the context of an organised criminal group. This same problem may arise in relation to mutual legal assistance requests relating to collecting funds/assets for a terrorist/terrorist organisation.

425. ***Recommendation 37 and Special Recommendation V:*** Norway's dual criminality provisions apply equally to ML matters (Rec.37) and FT matters (SR V). Except where the mutual legal assistance request originates in a Nordic country, the requirement of dual criminality must be met where coercive

measures are being sought. The requirement of dual criminality is broadly worded – the foreign offence in respect of which assistance is sought need only be correspondingly punishable under Norwegian law. Where the measure sought is not a coercive measure, there is no requirement for dual criminality. For extradition and those forms of mutual legal assistance where dual criminality is required, Norway has no legal or practical impediment to rendering assistance, provided that both Norway and the requesting country criminalise the conduct underlying the offence. There do not appear to be any particular technical differences which would pose an impediment to the provision of mutual legal assistance in this regard. However, the application of dual criminality may create an obstacle to mutual legal assistance in cases involving ML/FT activities that have not been properly criminalised in Norway (see paragraph 408 above).

426. ***Recommendation 38 and Special Recommendation V:*** Norway's measures to give effect to foreign orders for charging, seizing and confiscation apply equally to ML matters (Recommendation 38) and FT matters (SR V). Requests for confiscation from foreign countries are not regulated through the EA. The applicable regulation depends on whether the Vienna or Strasbourg Convention applies. Member states of these Conventions are subject to Regulation no. 90 (dated 2 February 1995) regarding extension of the scope of Act no. 67 (dated 20 July 1991) on transfer of convicted persons (Act. No.67), ss.1 and 9. According to Act no.67, foreign decisions on penalty sanctions, including confiscation, can be executed in Norway. However, this requires a separate Norwegian decision of confiscation, either by the court or by the police through a writ.[112] This does not mean that Norway starts its own case or recalls all of the evidence. On the contrary, the process is much simpler and involves verifying that the Vienna or Strasbourg Convention applies and then proceeding according to the requirements set out in the Conventions themselves (see Article 5 and 7 of the Vienna Convention and Articles 13-18 of the Strasbourg Convention). These requirements are not particularly onerous. For instance, Article 14 of the Strasbourg Convention provides that the country receiving the request shall be bound by the findings of fact as they are stated in the conviction or judicial decision of the requesting party (in so far as a conviction or judicial decision is implicitly based on them). The Vienna Convention contains no such explicit provision; however, Article 5 provides that a request must be accompanied by a copy of the confiscation order and a statement of the facts/information relied upon by the requesting party. However, Article 7(15)(c) of the Vienna Convention and Article 18(4)(a) of the Strasbourg Convention raise concern that the problems with dual criminality (as described in paragraph 408-409 above) may affect enforcement of confiscation orders that were issued on the basis of a conviction for one of the ML/FT activities that have been not properly criminalised in Norway. In general, however, other than the concern about dual criminality mentioned above, it would seem that the system for enforcing orders from European countries under the Strasbourg Convention works quite well. The mechanism under the Vienna Convention is less clear, but still acceptable—although its use is limited to drug-related freezing/seizing/confiscation orders from countries that are parties to the Convention.

427. The mechanisms to give effect to foreign freezing/seizing/confiscation orders outside the contexts described above is much less satisfactory. If the foreign state requesting confiscation is not a signatory to the above-mentioned conventions, the same general rules concerning domestic confiscation would apply. In such cases, assistance may be provided in the confiscation of laundered property from, proceeds from, instrumentalities used in, or instrumentalities intended for use in the commission of any ML, FT or other predicate offence, or to property of a corresponding value. However, Norway can only recognise a foreign confiscation order; it cannot give effect to it without starting its own proceedings. Likewise, Norway must initiate its own proceedings to enforce a foreign freezing order. Although to date this has not been an issue (since, to the best of its recollection, Norway has not received a request that was not related to a Nordic country or the Vienna/Strasbourg Conventions), Norway recognises that this issue will have to be addressed as it goes forward and as requests for international co-operation increase.

[112] Regulation of Act No. 67 on transfer of convicted persons dated 20 July 1991 ss.1-9.

428. No special permanent arrangement for co-ordinating seizure and confiscation actions with other countries exist. However, co-ordination may (and does) take place on a case-to-case basis. No asset forfeiture fund exists. Norway reports that it did consider creating an asset forfeiture fund and, indeed, the proposal was set out in earlier drafts of the Action Plan 2004. However, the idea was eventually dropped. In 2004, Norway considered authorising the sharing of confiscated assets with other countries. As a result of these consideration, the Norwegian government proposed amendments to Penal Code section 37d (Ot.prp. nr. 90 (2003-2004)). The proposed amendment (which has been presented to Parliament) would allow the Ministry to decide that the confiscated assets shall be shared between Norway and one or more other countries. When making such a determination, the Ministry would, among other things, take into account the expenses incurred by the countries involved, the detrimental impact of the criminal act in the countries involved and the amount of the proceeds. Sharing would not take place if it would reduce the compensation to the victim of the crime. In other words, sharing would not be mandatory. Other issues may also be taken into consideration. It will be up to the judgment of the Ministry to decide whether sharing should take place.

429. ***Recommendation 32 (Statistics relating to mutual legal assistance):*** Norway collects statistics on the number of requests for mutual legal assistance, including requests related to freezing, seizing and confiscation. However, Norway does not collect statistics concerning the nature of the request, whether the request was granted or refused, what crime the request was related to or how much time was required to respond.

6.3.2 Recommendations and Comments

430. Overall, Norway has a very effective system for responding to mutual legal assistance requests from Nordic countries. Requests from both Nordic and Schengen countries can be handled expeditiously as they are channelled directly between judicial authorities. At present, Norway has to rely on section 24 of the Extradition Act as the main provision under which it provides mutual legal assistance. This creates one difficulty, however, with regards to the application of dual criminality to mutual legal assistance requests relating to ML/FT activities that have not been properly criminalised in Norway. One way to address this would be to enact separate and comprehensive mutual legal assistance legislation. This would not only allow Norway to remedy the deficiencies, but this will also improve the efficiency of the system. Norway could consider applying less restrictive requirements to mutual legal assistance requests. To resolve this issue, Norway should properly criminalise the following types of ML/FT activities: (i) self-laundering; (ii) a conspiracy between two people to commit ML; and (iii) obtaining or collecting funds/asset where the funds/assets are collected to be used by a terrorist organisation or individual terrorist where the use/intended use cannot be connected with a terrorist act and where those funds have not yet been provided to the terrorist organisation/terrorist. Norway should keep a fuller set of statistics, thus enabling it to better track the mutual legal assistance requests it receives and makes, and ensuring they are handled in a timely way.

431. Norway should enact legislation that would allow it to give effect to such orders in appropriate circumstances. Norway should consider enacting legislation that would clearly allow for confiscation in situations other than those covered by the Vienna and Strasbourg Conventions. A procedure that requires a case to be made out before a local (Norwegian) court on the basis of foreign evidence is inherently less effective than one where the Norwegian court satisfies itself that a foreign court has made a charging/seizing/confiscation order, and then simply gives effect to that order. As well, Norway should keep statistics concerning: (i) the nature of mutual legal assistance requests; (ii) whether the mutual legal assistance request was granted or refused; (iii) what crime the request was related to; and (iv) how much time was required to respond to the request.

6.3.3 Compliance with Recommendations 32, 36 to 38, and Special Recommendation V

	Rating	Summary of factors relevant to s.6.3 underlying overall rating

R.32	PC[113]	• Norway does not collect statistics concerning the nature of the mutual legal assistance request, whether the request was granted or refused, what crime the request was related to or how much time was required to respond.
R.36	LC	• In all cases involving mutual legal assistance requests from non-Nordic countries (where coercive measures are being sought), dual criminality applies. Additionally, for non-Schengen countries some of the requirements that apply to extradition requests also apply. This creates one difficulty, however, with regards to the application of dual criminality to mutual legal assistance requests relating to the following ML/FT activities that have not been properly criminalised in Norway: self-laundering; conspiracy between 2 people to commit ML; and collecting funds for a terrorist organisation/terrorist.
R.37	LC[114]	• The application of dual criminality may create an obstacle to mutual legal assistance in cases involving ML/FT activities that have not been properly criminalised in Norway.
R.38	PC	• Norway must start its own domestic proceedings to allow for confiscation in situations other than those covered by the Vienna and Strasbourg Conventions. A procedure that requires a case to be made out before a local (Norwegian) court on the basis of foreign evidence is inherently less effective than one where the Norwegian court satisfies itself that a foreign court has made a charging/seizing/confiscation order, and then simply gives effect to that order. .
SR.V	LC[115]	• In all cases involving mutual legal assistance requests from non-Nordic countries (where coercive measures are being sought), dual criminality applies. Additionally, for non-Schengen countries some of the other requirements that apply to extradition requests also apply. This creates one difficulty, however, with regards to the application of dual criminality to mutual legal assistance requests relating to the following FT activity that has not been properly criminalised in Norway: collecting funds for a terrorist organisation/terrorist. • Norway must start its own domestic proceedings to allow for confiscation in situations other than those covered by the Vienna and Strasbourg Conventions. A procedure that requires a case to be made out before a local (Norwegian) court on the basis of foreign evidence is inherently less effective than one where the Norwegian court satisfies itself that a foreign court has made a charging/seizing/confiscation order, and then simply gives effect to that order.

6.4 Extradition (R.32, 37 & 39, & SR.V)

6.4.1 Description and Analysis

432. ***Recommendation 37, 39 and Special Recommendation V:*** Both ML/FT are extraditable offences. Requests for extradition are treated as a matter of urgency within the Ministry of Justice &Police, the Prosecution authority and in the courts. However, no information concerning how long it takes to process an extradition request is available.

433. *Extradition requests from Nordic countries:* Norway has implemented an effective and streamlined system for handling extradition requests from Nordic countries. Extradition requests from Nordic countries (Denmark, Finland, Iceland and Sweden) are regulated by the NEA. Dual criminality does not apply (except in the case of extradition requests relating to political offences) (NEA s.4). Norway will extradite its own nationals to Nordic countries if the offence for which extradition is sought is punishable under Norwegian law with imprisonment for more than four years, or the person has been residing in the requesting state for the last two years (NEA s.2 para.1). Pursuant to the NEA, requests for extradition may be forwarded directly between the prosecuting authorities. However, persons cannot be extradited only on warrants of arrests of judgments. A chart

[113] This is an overall rating for compliance with Recommendation 32, based on the assessments in sections 2.5, 2.6, 3.13, 6.3, 6.4 and 6.5 of this report.

[114] This is an overall rating for compliance with Recommendation 37, based on the assessments in sections 6.3 and 6.4 of this report.

[115] This is an overall rating for compliance with Special Recommendation V, based on the assessments in sections 6.3, 6.4 and 6.5 of this report.

showing the difference between extraditions pursuant to the NEA and those pursuant to the EA are attached in Annex 15 to this report.

434. *Extradition requests from non-Nordic countries (including Schengen countries):* Extradition requests from non-Nordic countries are regulated by the EA. Norway has also ratified the European Convention on Extradition of 13 December 1957. Extradition may take place irrespective of the existence of an extradition treaty between the parties, provided that the conditions of the EA are met. There is a requirement of dual criminality for extradition. Extradition may only take place if the offence (or a corresponding offence) is punishable under Norwegian law with imprisonment for more than one year (EA s.3). As a general rule, extradition is possible in relation to all criminal acts provided that the other conditions pursuant to the EA are met. However, extradition may have to be refused if the request relates to one of the following ML/FT activities that have not been properly criminalised in Norway: (i) self-laundering; (ii) conspiring to commit ML outside of the context of an organised criminal group; and (iii) obtaining or collecting of funds/asset where the funds/assets are collected to be used by a terrorist organisation or individual terrorist where the use/intended use cannot be connected with a terrorist act and the funds have not yet been provided to the terrorist organisation/terrorist. If extradition is being sought in relation to a person who has already been convicted in the requesting state, the conviction must involve deprivation of liberty or committal to an institution for a period of at least 4 months (EA s.3). Extradition must not take place if it must be assumed that there is a grave danger that the person concerned, for reasons of race, religion, nationality, political convictions or other political circumstances, will be exposed to persecution directed against his life or liberty or that the said persecution is otherwise of a serious nature (EA s.6). Moreover, extradition may not take place if it would conflict with fundamental humanitarian considerations (EA s.7). Other than the exception for Nordic countries set out above, Norwegian nationals may not be extradited (EA s.2 and Norway's declaration to article 6 in the European Convention on Extradition). When extradition is refused because the person in question is a Norwegian national, the case will (upon request) be forwarded to the Prosecution Authority. If considered appropriate, proceedings may take place, including transmission of information relating to the offence. Pursuant to the EA section 19, the execution of the extradition has to be completed as soon as possible and latest within 4 weeks from the final decision has been made. A continued imprisonment beyond the 4 weeks can only be granted when particular causes apply.

435. *Additional measures applicable to extradition requests from Schengen countries:* Simplified procedures of extradition are in place by allowing direct transmission of extradition requests between the appropriate ministries of the member states of Schengen. Pursuant to the Schengen Convention, consenting persons who waive formal extradition proceedings can be extradited by a simplified procedure.

436. The following chart sets out the total number of requests for extradition in criminal cases, sent from and received by Norway via the Ministry of Justice & Police.

NUMBER OF EXTRADITION REQUESTS TO/FROM NORWAY				
Extradition	2000	2001	2002	2003
To Norway	-	No available numbers	No available numbers	16
From Norway	-	11	11	19
Total	-	-	-	35

437. *Other international co-operation in the absence of extradition:* Norway has ratified the European Convention on transfer of proceedings in criminal matters dated 15 May 1972. Transfer of proceedings may also take place in the absence of an international convention, as mentioned above. On the request of a foreign state, the documents of the case will be forwarded to the Prosecution Authority which then will consider whether the proceedings may be transferred. When it comes to

international cooperation on procedural and evidentiary matters, Norway is part of the Nordic Agreement on Police Co-operation, which lays down procedures for direct and efficient transmitting of documentary evidence between police authorities in the Nordic countries. Norway has just recently concluded an agreement of cooperation with EU on participation in the Eurojust system, strengthening the efficiency of European prosecutorial cooperation such as smoothening procedural and evidentiary processes. Norway has ratified the European Convention on Extradition (1957), the European Convention on Mutual legal assistance in criminal matters (1959), and the European Convention on transfer of proceedings in criminal matters. With regard to efficiency and co-operation, reference is made to the procedures laid out in these conventions. In general, these procedures will also apply for co-operation when no convention is applicable. Between the Schengen countries and the Nordic countries, special conventions also apply, authorising requests for mutual legal assistance to be sent directly between the judicial authorities, as mentioned above.

438. ***Recommendation 32 (Statistics relating to extradition):*** Norway collects statistics on the number of requests for extradition. However, Norway does not collect statistics concerning the nature of the request, whether the request was granted or refused, what crime the request was related to or how much time was required to respond. The statistics related to extradition only include persons being extradited to or from Norway in 2003. Statistics for 2004 are unavailable due to a reorganisation of Norway's file system. Requests for extradition between the Nordic countries may, pursuant to the Act for extradition within the Nordic countries dated 03 March 1961, be sent directly between the prosecuting authorities. There are no statistics available concerning these requests.

6.4.2 Recommendations and Comments

439. Norway should also ensure that the application of dual criminality does not impede extradition when the case involves ML/FT activities that are not properly criminalised in Norway. In that regard, Norway should properly criminalise: (i) self-laundering; (ii) conspiring to commit ML outside of the context of an organised criminal group; and (iii) obtaining or collecting of funds/asset where the funds/assets are collected to be used by a terrorist organisation or individual terrorist where the use/intended use cannot be connected with a terrorist act and the funds have not yet been provided to the terrorist organisation/terrorist. Norway should also collect and maintain statistics on: (i) the number of requests for extradition; (ii) the nature of the request; (iii) whether the request was granted or refused; (iv) what crime the request was related to; or (v) how much time was required to respond. Statistics concerning requests for extradition between the Nordic countries that are sent directly to the prosecuting authorities should also be collected and maintained.

6.4.3 Compliance with Recommendations 32, 37 & 39, and Special Recommendation V

	Rating	Summary of factors relevant to s.6.4 underlying overall rating
R.32	PC[116]	• Norway does not collect statistics concerning the nature of the request, whether the request was granted or refused, what crime the request was related to or how much time was required to respond. • The statistics related to extradition only include persons being extradited to or from Norway in 2003. Statistics for 2004 are unavailable due to a reorganisation of Norway's file system. • Requests for extradition between the Nordic countries may, pursuant to the Act for extradition within the Nordic countries dated 03 March 1961, be sent directly between the prosecuting authorities. There are no statistics available concerning these requests.
R.37	LC[117]	• The application of dual criminality may create an obstacle to extradition in cases involving ML/FT activities that have not been properly criminalised in Norway.

[116] This is an overall rating for compliance with Recommendation 32, based on the assessments in sections 2.5, 2.6, 3.13, 6.3, 6.4 and 6.5 of this report.

[117] This is an overall rating for compliance with Recommendation 37, based on the assessments in sections 6.3 and 6.4 of this report.

R.39	LC	• Overall, there is concern that (except in the case of extradition requests from Nordic countries where dual criminality does not apply), extradition may be impeded when the case involves the following ML/FT activities that are not properly criminalised in Norway: (i) self-laundering; (ii) conspiring to commit ML outside of the context of an organised criminal group; and (iii) obtaining or collecting of funds/asset where the funds/assets are collected to be used by a terrorist organisation or individual terrorist where the use/intended use cannot be connected with a terrorist act and the funds have not yet been provided to the terrorist organisation/terrorist.
SR.V	LC[118]	• The application of dual criminality may create an obstacle to extradition in cases involving ML/FT activities that have not been properly criminalised in Norway. • Overall, there is concern that (except in the case of extradition requests from Nordic countries where dual criminality does not apply), extradition may be impeded when the case involves the following FT activities that are not properly criminalised in Norway: obtaining or collecting of funds/asset where the funds/assets are collected to be used by a terrorist organisation or individual terrorist where the use/intended use cannot be connected with a terrorist act and the funds have not yet been provided to the terrorist organisation/terrorist.

6.5 Other Forms of International Co-operation (R.32 & 40, & SR.V)

6.5.1 Description and Analysis

440. ***Recommendation 40 and Special Recommendation V:*** As a matter of general policy, the competent authorities in Norway for international co-operation in the combat of crime, whether on an operational or ministerial level, give a clear priority to exchanging information with international counterparts as promptly and effectively as possible. Norwegian legislation allows for a wide range of passing information to authorities in other countries relevant for preventing and detecting criminal acts. Norwegian law enforcement authorities have well functioning systems of electronically stored information, easy to find and easy to be forwarded to other countries. It is a general attitude in Norwegian law enforcement to give rapid response to requests from cooperating agencies abroad. However, last year, due to a systems crash, the MLU was unable to respond to co-operation requests from it foreign counterparts. Since then, the systems crash has been resolved and the MLU has designated staff to deal with such requests. It is too early to assess how effective these new measures will be**.**

441. When information is exchanged with foreign counterparts, it is on the condition that information can only be used for professional purposes (i.e. it must be kept within the conduct of criminal investigations and not given to unauthorised personnel). Norwegian law strictly limits the use of exchanged information by authorised personnel and in a professional manner to protect privacy. Norway does not have special control or safeguard systems to ensure that this condition is met. Norwegian law does not provide for the speciality principle (i.e. to confine the use of information shared with other foreign authorities to that purpose for which the request was originally made). Norway does not refuse requests for co-operation solely on the ground that the request is considered to involve fiscal matters. Nor does it refuse requests for co-operation on the grounds of secrecy laws or confidentiality requirements (other than those held in circumstances where legal professional privilege applies). In general, exchanges of information are not made subject to disproportionate or unduly restrictive conditions. The ability to co-operate both domestically and internationally has been improved by repealing the strict confidentiality provision that existed in the previous legislation (FS Act, s.2-17) through the adoption of the MLA (in force from 1 January 2004). Information can be exchanged with foreign FIUs, both spontaneously and upon request, regardless of whether the FIU is organised within the police or prosecution authority or within the administration. Norway has received several requests from foreign FIUs to enter into MOU. However no MOUs have yet been agreed upon.

[118] This is an overall rating for compliance with Special Recommendation V, based on the assessments in sections 6.3, 6.4 and 6.5 of this report.

442. *Law enforcement authorities* Norwegian law enforcement authorities are authorised to conduct investigations on behalf of foreign counterparts on the conditions that formal procedures laid down in legal instruments are applied.

443. *Financial intelligence unit:* It is possible in Norway to exchange information both spontaneously and upon request in relation to money laundering and underlying predicate offences. For instance, the MLU is able to co-operate with other FIUs both spontaneously and upon request; an MOU is not required. It may co-operate with both police/prosecution based FIUs and administrative FIUs. The MLU can make inquiries for foreign FIUs in its own database. The database contains information from STRs and inquiries that have been conducted by the unit, for example inquiries in registers etcetera. Consequently, where the MLU receives a request from a foreign FIU it may also make new inquiries in other databases, including law enforcement and public databases etcetera, that it has access to. In 2004, due to some technical failures with respect to connectivity with the Egmont Secure Web System, the MLU had to replace some computer hardware. This led to a loss of data relating to requests from foreign FIUs, including its statistics relating to formal requests for assistance made or received by the MLU, and spontaneous referrals made by the MLU to foreign authorities. As a result, the system for connecting to the Egmont Secure Web System was itself was down for some 3 months, thus impeding the MLU's ability to provide international co-operation during this period. The MLU estimates that approximately 25 foreign requests were affected by this problem. However, the problem has been subsequently rectified and the MLU has reorganised itself, dedicating two people to managing requests from foreign FIUs.

444. MOUs with foreign FIUs: The MLU does not need to have an MOU in order to be able to exchange information with foreign counterparts. ØKOKRIM signed an MOU with the C.T.I.F.-C.F.I. of Belgium in 1995. However, after the new MLA was adopted, the legislative situation in Norway changed concerning entering into MOUs with foreign FIUs. It is now clear that the MLU may enter into MOUs with foreign FIUs regardless of the way that they are organised. The following foreign FIUs have requested an MOU with Norway: Albania, Poland, Russia, Singapore, Thailand, The Netherlands Antilles and Ukraine. Norway may enter into MOUs with foreign FIUs (including administrative ones). However, despite these requests, no additional MOUs have been entered into. This creates a negative impact on effectiveness, particularly in situations where the foreign FIU requires an MOU in order to be able to co-operate. On a policy level, The Ministry of Justice & Police is of the view that MOUs represent an important tool and must be used adequately. In co-operation with The Police Directorate and ØKOKRIM, the Ministry of Justice & Police will assess and respond to the requests to enter MOUs that have already been received. A procedure for handling these requests is about to be established.

445. *Supervisory authorities:* The Financial Supervision Act does not contain any explicit provision concerning mutual assistance between regulators in supervisory matters. Nevertheless, in general, Norwegian authorities may execute requests for assistance (even in the absence of any applicable agreement or statutory provision) provided that the execution of the request is not contrary to Norwegian law. Consequently, the FSA may assist foreign supervisory authorities that make inquiries related to the ordinary discharge of their supervisory functions and powers. However, the FSA has not yet received any formal requests for assistance from other supervisors. The FSA can co-operate spontaneously with other foreign supervisory authorities. Norway reports that such co-operation has been carried out in relation with on-site inspections in Nordic banking groups.

446. The EEA agreement: Norway is a party to the EEA Agreement and is therefore committed to transpose and implement all so-called "EEA-relevant" acts adopted by the EU. The EEA Agreement is a dynamic treaty whereby each new act needs to be evaluated for its "EEA-relevance" before being incorporated into the EEA Agreement (with or without particular adaptations). Acts related to financial services are listed in the Annex IX to the EEA Agreement (see http://secretariat.efta.int/Web/EuropeanEconomicArea/EEAAgreement/annexes/annex10.pdf). Norway participates as an observer in all working groups or expert groups under the European Commission, and

in the regulatory and supervisory committees established within the EU. In addition, it is granted specific participation in the Contact Committee on Money Laundering (Protocol 37 to the EEA Agreement).

447. Multilateral MoUs: On the EU/EEA level all insurance supervisory authorities have jointly developed and agreed on multilateral collaboration agreements. The so-called "Siena Protocol" pertains to exchange of information and cooperation related to insurance supervision according to the insurance directives. The "Helsinki Protocol" details the co-operation with regard to supervision of insurance groups with activities across borders. The occupational pensions supervisors are currently drafting a corresponding multilateral MoU with regard to supervision of occupational pensions providers (EU Directive 2003/41/EC of 3 June 2003 on the activities and supervision of institutions for occupational retirement provision (IORP). Norway also signed a multilateral MoU with other securities supervisors in the EEA regarding cooperation with regard to supervision of the securities market as a member of FESCO (now CESR). The FSA has also signed a bilateral MoU with the United States' Securities and Exchange Commission (SEC) and has annual meetings with representatives of the Federal Reserve Bank, where issues pertaining to measures against money laundering are on the agenda. As a member of IOSCO, IAIS, and the newly formed International Pension Supervisors Group (IOPS), the FSA co-operates and exchanges information with other supervisors who are members of these organisations.[119]

448. Bilateral MoUs: Within the banking sector, there is no multilateral MoU in Europe; hence Norway has negotiated MoUs with relevant supervisory authorities (i.e. the home supervisor of credit institutions established in Norway, or host supervisor in countries where Norwegian credit institutions are established). The FSA has signed bilateral co-operation agreements (MoUs) with the banking and investment firms supervisors in: France, Germany, Luxembourg, the Netherlands and the United Kingdom (FS Act). The FSA meets on a regular basis with representatives from these supervisory authorities.

449. Nordic MoUs: The Nordic supervisory authorities used to have bilateral MoUs but decided to merge these into one common Nordic MoU for all financial supervisors in Denmark, Finland, Iceland, Norway and Sweden, applying to banking, insurance and securities market supervision in the Nordic countries. The Nordic supervisors meet on an annual basis at high level, and have regular sector-specific meetings and expert meetings. Additionally, the Nordic supervisory authorities felt the need to draw up more detailed MoUs regarding the supervisory cooperation pertaining to the supervision of particular financial groups. Hence there is a MoU between the supervisory authorities in Finland, Sweden and Norway with regard to the supervision of a large financial group which includes an insurance company and between the authorities in Denmark, Finland, Norway and Sweden with regard to supervision of another financial group.

450. *Customs authorities:* In principle, the Norwegian custom authorities do not need an MOU as a legal basis to co-operate with their respective foreign counterparts. They are allowed to share information with other countries' customs and excise administrations according to article 4 of the Norwegian Customs Act. This is, however, only possible if such information can be shared on a mutual basis, and the recipient stores and protects the information according to the Norwegian Personal Protective Act, or according to such principles as safe haven. On the other hand, as a general rule, the Customs Directorate uses MOUs with other countries that authorise the custom authorities to collect and share information related to custom offences. The reason for this is that the legal basis for co-operation and information sharing is then thoroughly considered, and the authorities do not lose time in the process of considering the legal terms on a case-by-case basis.

451. ***Recommendation 32 (Statistics related to other forms of international co-operation):*** Norway does not maintain statistics concerning the number of sanctions applied or the number of formal requests for assistance made and received by supervisors relating to or including AML/CFT.

[119] The FSA will apply to enter the IOSCO multilateral MOU during the summer of 2005.

However, Norway does maintain statistics concerning the number of formal requests for assistance made to or received by the FIU from foreign counterparts. The figures are uncertain because the registration routines are not quite clear, especially as regards the requests made to foreign counterparts.

6.5.2 Recommendations and Comments

452. Norway should ensure that the MLU's new systems for facilitating co-operation with foreign counterparts are working effectively. As well, Norway should collect and maintain statistics concerning the number of sanctions applied, and the number of formal requests for assistance made and received by supervisors relating to or including AML/CFT. Norway should also improve the certainty of its statistics concerning the number of formal requests for assistance made to or received by the MLU from foreign counterparts.

6.5.3 Compliance with Recommendations 32 & 40, and Special Recommendation V

	Rating	Summary of factors relevant to s.6.5 underlying overall rating
R.32	PC[120]	• Norway does maintain statistics concerning the number of formal requests for assistance made to or received by the FIU from foreign counterparts. • The figures are uncertain because the registration routines are not quite clear, especially as regards the requests made to foreign counterparts.
R.40	C	• Recommendation 40 is fully observed.
SR.V	LC[121]	• It is a general attitude in Norwegian law enforcement to give rapid response to requests from cooperating agencies abroad. However, last year, due to a systems crash, the MLU was unable to respond to co-operation requests from it foreign counterparts. Since then, the systems crash has been resolved and the MLU has designated staff to deal with such requests. It is too early to assess how effective these new measures will be.

7 OTHER ISSUES

7.1 Other relevant AML/CFT measures or issues

453. ***AML measures implemented by the Tax authorities:*** In principle, money laundering is not directly within the tax authorities administrative responsibilities. However, in the letter of instruction (*disponeringsbrevet*) from the Tax Directorate to the county revenue offices, the Tax Directorate has directed the tax authorities to focus on revealing ML conducting their tax audits, and to inform the police if signs of ML or other serious crimes are detected. AML is now supposed to be part of every tax audit. However, at the moment, tax auditors do not receive any specific training in ML issues. They have had some training in tax crime cases and there are some similarities; however, they still need training on how to distinguish between tax crimes and money laundering activity.

454. Although the tax authorities are bound by a duty of confidentiality, the statutory tax secrecy rules allow information to be given to the police and the public prosecutor for use in a criminal investigation relating to tax evasion. If the case concerns offences outside the tax authorities' administrative area (i.e. money laundering or drug-related crimes), information can be given to the police and public prosecutor if there are adequate grounds to suspect a criminal offence punishable with a minimum sentence of 6 months imprisonment. When there is a suspicion of ML, the tax authorities are obligated to report to the police and Prosecution Authority; however, there is no legal duty for the tax authorities to report suspicious transactions to the MLU. To date, the tax authorities have not made any reports to the

[120] This is an overall rating for compliance with Recommendation 32, based on the assessments in sections 2.5, 2.6, 3.13, 6.3, 6.4 and 6.5 of this report.

[121] This is an overall rating for compliance with Special Recommendation V, based on the assessments in sections 6.3, 6.4 and 6.5 of this report.

police or Prosecution Authority so it is not clear whether the police would send a copy of such a report to the MLU. The Directorate of Taxes has elaborated guidelines establishing criteria for reporting to the law enforcement authorities, when reasonable grounds of suspicion of a serious criminal offence (beyond the fiscal area) has occurred (Tax Directorate Bulletin of 5 November 2003 (the Tax Bulletin)). Local tax inspectors must obtain prior approval of the Country Revenue Office before conveying information to law enforcement agencies. A similar system regulates disclosure by the customs service under the Customs Act. The Tax Bulletin specifically provides that making such reports in good faith is not a breach of the duty of secrecy set out in the Assessment Act. If a tax auditor develops a suspicion that a crime has been committed, he/she must discuss it with a superior colleague. If both agree, the case must be sent to the Country Revenue Office, which decides if the case shall be reported to the police.

455. All financial institutions in Norway are obliged to disclose to the tax authorities by the end of the year information about the balance on the bank accounts, the share dividend, etcetera. The tax authorities systematically co-operate with the police, prosecution authority or specialised structures such as ØKOKRIM in the course of financial investigations in order to identify and generate effectively relevant data regarding income and asset declarations, life style, etcetera. For instance, the Tax Directorate participates on a working group with the FSA, ØKOKRIM and Norges Bank to deal with AML issues. They have one meeting per year to deal with these issues. Until recently, the Tax Directorate did not deal with AML issues. The tax authorities do not have intelligence units specifically devoted to AML. They do, on the other hand, have intelligence units for general tax control, which also look for suspicions of ML. The lists of persons and entities designated under United Nations S/RES/1267(1999) are not distributed specifically to the tax authorities and do not play a role. Although the tax authorities have just started to focus on money laundering, they should be complimented for their efforts to do so.

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). These ratings are based only on the essential criteria, and defined as follows:

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[122]
Legal systems		
1.ML offence	LC	Self-laundering is not a criminal offence and there is no fundamental principle of domestic law that would preclude self-laundering from being an offence. The conspiracy offence would not extend to a conspiracy involving only two people, and the requirement for an "organised criminal group" with a particular purpose would only apply to certain ML scenarios and there is no fundamental principle of domestic law that would preclude such conduct being criminalised.
2.ML offence – mental element and corporate liability	C	Recommendation 2 is fully observed.
3.Confiscation and provisional measures	C	Recommendation 3 is fully observed.
Preventive measures		
4.Secrecy laws consistent with the Recommendations	C	Recommendation 4 is fully observed.
5.Customer due diligence	PC	Although Norway has implemented customer identification obligations, it has not implemented full customer due diligence (CDD) requirements. There are extensive rules on the identification of a customer who is a legal person and also of an individual acting for that legal person. However, there is presently no legal requirement under the MLA or MLR for a Reporting FI to verify that the individual is duly authorised to act for the legal person. If a Reporting FI knows or has reason to believe that a customer is acting as a (legal) representative of another, on behalf of another, or that another person owns the asset that is the subject of a transaction, the FI is required to identify that other person (MLA s.6). Other than this, there is no other requirement to identify a beneficial

[122] These factors are only required to be set out when the rating is less than Compliant.

		owner within the meaning of the FATF Recommendations (i.e. the natural person(s) who ultimately owns or controls a customer and/or the person on whose behalf a transaction is being conducted, and incorporating those persons who exercise ultimate effective control over a legal person or arrangement). Reporting FIs are not legally required to actively inquire if the customer is "fronting" for any other person in respect of an account or a transaction (for instance, by asking as a routine part of the account opening procedure whether the account holder is acting on behalf of another person). Reporting FIs are also required to obtain information relating to the shareholding or any corporate group behind a customer who is a legal person. There is no obligation on the Reporting FI to inquire about the purpose and nature of the business relationship vis-à-vis the Reporting FI itself, or to conduct ongoing due diligence on the business relationship in that regard. There is no enhanced CDD legislation for higher risk categories of customers. Nor does Norwegian legislation provide for any simplified or reduced CDD measures. There is no obligation not to open an account, not establish a business relationship, consider making an STR or (in the case of existing customers) terminate the business relationship in instances where the beneficial owner cannot be identified or information concerning the purpose and intended nature of the business relationship cannot be obtained. This is because there is no obligation to collect this information in the first place. There are no legal or regulatory measures in place as to how Reporting FIs should apply CDD measures to their existing pool of customers. There is no legal requirement for a customer's identity to be re-verified upon a subsequent enlargement of the customer relationship in the same institution (i.e. the opening of a new account, writing a new insurance policy, etc). The requirements regarding customer identification are primarily focused on the banking sector. However, this one-size-fits-all approach may, in some cases, not take into account the normal conduct of business in non-bank sectors.
6.Politically exposed persons	NC	Norway has not implemented any AML/CFT measures concerning the establishment of customer relationships with politically exposed persons (PEPs).
7.Correspondent banking	NC	Norway has not implemented any AML/CFT measures concerning establishment of cross-border correspondent banking relationships.
8.New technologies & non face-to-face business	C	Recommendation 8 is fully observed.
9.Third parties and introducers	NA	Recommendation 9 does not apply in the Norwegian context.
10.Record keeping	C	Recommendation 10 is fully observed.
11.Unusual transactions	C	Recommendation 11 is fully observed.
12.DNFBP – R.5, 6, 8-11, 17	PC	Overall, the ratings for Recommendation 12 have been lowered due to concerns about the scope of application of AML/CFT obligations (in relation to company service providers). The same serious deficiencies in the implementation of Recommendation 5 apply equally to Reporting FIs and Reporting BPs. In other words, customer identification requirements have been implemented, but full CDD requirements have not. Norway has not implemented any AML/CFT measures concerning Recommendations 6 that are applicable to Reporting BPs. Considering the calls for more guidance as voiced by these sectors (particularly dealers in precious metals/stones) during the on-site visit, there are preliminary concerns about the effectiveness of implementation for Recommendation 11. However, it should be noted that reporting is occurring in all DNFBP sectors—except dealers in precious metals/stones (which are also not supervised for compliance with AML/CFT obligations). Dealers in precious metals and stones are not monitored or supervised for compliance with AML/CFT obligations and are not subject to administrative sanctions.
13.Suspicious transaction reporting	LC	In general, there are some concerns about the effectiveness of the reporting system. For instance, (except for MVTS providers), the number of STRs being reported by non-bank financial institutions is very small and the number of STRs being reported by banks themselves is also decreasing. Additionally, there were some indications during the on-site visit that, in the past year, a MVTS provider had not been complying with its

		reporting obligations. The FSA has since taken action to correct this problem. Another effectiveness concern relates to the fact that, in general, banks seem to focus on transactions performed by foreigners as being suspicious, rather than focusing on the nature and characteristics of the transactions themselves. There also appears to have been defensive reporting of STRs by the old MVTS provider (i.e. reporting of STRs without giving proper consideration to whether or not they are really suspicious). It is not clear that the reporting obligations under Recommendation 13 and Special Recommendation IV apply to transactions that may be related to the mere collection of funds for a terrorist/terrorist organisation.
14.Protection & no tipping-off	C	Recommendation 14 is fully observed.
15.Internal controls, compliance & audit	LC	There is no legal obligation on Reporting FIs to establish screening procedures to ensure high standards when hiring employees. There are some preliminary concerns about how effectively internal controls have been implemented. The internal controls themselves suffer from the same deficiencies as the legal requirements. For instance, because full CDD is not a legal requirement in Norway, there is no legal obligation to implement internal controls to ensure that full CDD is performed, and it did not appear that institutions had voluntarily implemented the much higher standards that are required.
16.DNFBP – R.13-15, 17 & 21	LC	Overall, the ratings for Recommendation 16 have been lowered due to concerns about the scope of application of AML/CFT obligations (in relation to company service providers).
17.Sanctions	LC	Where a Reporting FI has not complied with its AML/CFT obligations, the wording of the MLA does not make it clear whether sanctions can be applied to the directors and senior management of the FI that was responsible for the violation by the FI. In relation to criminal penalties, the assessors feel that the legal provisions cited by Norway are unclear, but Norway is of the firm view that criminal penalties can be applied to the directors and senior management of Reporting FIs in respect of a breach by the Reporting FI. In relation to civil penalties, the Financial Supervision Act provide a means for the FSA to take a form of civil enforcement action but it would be applicable on a forward looking basis.
18.Shell banks	PC	There is no prohibition on financial institutions entering into or continuing correspondent banking relationships with shell banks. There is no obligation on financial institutions to satisfy themselves that a respondent financing institution in a foreign country is not permitting its accounts to be used by shell banks.
19.Other forms of reporting	C	Recommendation 19 is fully observed.
20.Other NFBP & secure transaction techniques	C	Recommendation 20 is fully observed.
21.Special attention for higher risk countries	C	Recommendation 21 is fully observed.
22.Foreign branches & subsidiaries	LC	There is no requirement for a financial institution to inform the FSA if its foreign branch or subsidiary is unable to observe appropriate AML/CFT measures because this is prohibited by the laws or regulations of the host country.
23.Regulation, supervision and monitoring	LC	There is some concern about how effectively the MVTS sector is being supervised given that the assessors have been made aware of some problems concerning how the reporting obligation is being complied with. Norway has reported that inquiries are in progress on this case and appropriate action will be taken. There is no obligation on the financial institution to notify the FSA of changes in management. The FSA may assess whether managers, directors or controlling owners are fit and proper, but only in the context of granting licences for the first time and applications to acquire qualifying holdings in financial institutions.

24.DNFBP - regulation, supervision and monitoring	LC	Dealers in precious metals and stones are not monitored or supervised for compliance with AML/CFT obligations and are not subject to administrative sanctions, and there is no indication that Norway has considered this issue following a risk-based approach. By designating the FSA responsible for monitoring real estate agents, accountants and auditors for compliance with AML/CFT obligations, Norway has included these DNFBP sectors under the same supervisory regime that applies to the financial institutions sectors. Although this is commendable, it creates concerns about the sufficiency of the FSA's resources to supervise all of these entities.
25.Guidelines & Feedback	PC	Supervisory authorities: Almost every reporting entity that the assessors met with asked for more specific and tailored guidance concerning AML/CFT obligations. The FSA has issued detailed guidance to Reporting FIs concerning how to comply with the reporting obligations. Despite the guidance given, 70% of all STRs are based on transactions made by non-Norwegians. It seems that the only real indicator or typology that has made any impact within the reporting community is the fact that a non-Norwegian is performing a transaction. It does not seem that those STRs should not have been made, which leads however to the conclusion that there is a potential for other types of STRs to be reported if only the employees of reporting institutions had been guided to focus not only on the customer, but also the nature of the transactions. The Supervisory Council has not issued AML/CFT guidance to the Reporting BPs it supervises. The Supervisory Council does participate, however, in a working group that has as a mandate to propose guidelines to the lawyers. Likewise, the NARF and NIPA (which are industry associations, not supervisors) participate in a working group that has a mandate to propose guidelines to auditors and external accountants. Financial intelligence unit: Upon receipt of the STR, the MLU sends a computer printout with information about the reference number to the financial institution. After making its inquiries, the MLU normally informs the Reporting FI of the decision that was taken, and (if applicable) of the police district or foreign unit investigating the case. However, this has not been a consistent practice in the last years. The Reporting FI should also receive transcripts of legal decisions; however, this has not been followed up lately. Previously, Reporting FIs received a report every six months about the current status of all the STRs that the Reporting FI had reported; however, this is no longer the practice. Until 2004, the MLU sent quarterly reports to reporting entities; however, this practice was stopped due to a lack of resources. Norway reports, however, that the practice of sending quarterly reports recommenced as of 1 January 2005. The MLU also had a tradition of giving feedback to Reporting FIs/BPs through a Contact Forum (biannual meetings with representatives from these entities). The Contact Forum discussed issues such as feedback, suspicious transactions, money laundering methods and other similar topics; however, this Forum has been abolished due to its unmanageable size after the adoption of the new Money Laundering Act. Instead, the MLU has been giving information and feedback through its quarterly newspaper "Money Laundering News".
Institutional and other measures		
26.The FIU	PC	Although, on paper, the MLU generally meets the requirements of Recommendation 26, its lack of effectiveness causes concerns and impedes the overall effectiveness of Norway's AML/CFT system. Technical limitations prevent the MLU staff to apply analytical tools directly to all of the information in the database, forcing them to extract a selection of STRs to another system where the analytical tools can be applied. As a result any analysis of STR information which the MLU staff might do is restricted to the selected extract only and is done without the benefit of allowing the analytical tools to search through the entire STR database. Overall, the impression is that much of the information from the STRs is distributed to other law enforcement bodies without sufficient analysis. This is because the MLU has insufficient resources to handle the STRs that it receives. In theory, the Control Committee could interfere with the MLU's independence, particularly with regards to the exercise of its discretion on the decision to

		delete records pursuant to section 10 of the MLA; however, in practice, this does not seem to have occurred. At a minimum, the Control Committee's intervention has impacted on the overall effectiveness of the MLU in that a disproportionate amount of the MLU's very limited resources are now expended towards considering whether to delete or justify retaining old STR files. As an Egmont member, the MLU is aware of the Egmont Group Statement of Purpose and its Principles for Information Exchange Between Financial Intelligence Units for Money Laundering Cases (Egmont Principles for Information Exchange). However, in practice, the MLU does not follow all of these guidelines. While the desire to protect the privacy of information is understandable, to insist that such STR information be deleted may deprive the MLU of a potential source of information that may be exceedingly useful for its work, and inhibit the effectiveness of the MLU's work.
27.Law Enforcement Authorities	C	Recommendation 27 is fully observed.
28.Powers of competent authorities	C	Recommendation 28 is fully observed.
29.Supervisors	LC	FIs are obliged to produce self-assessment reports that are used by the FSA to determine which FIs will be visited on-site. However, these self-assessments are based on the prudential supervision and contain no AML/CFT questions. AML/CFT assessments of Reporting FIs by the FSA are an integral part of regular visits but seem to be too limited. For example, for a larger bank, the FSA indicated that the AML/CFT component of a regular examination took 2 days of off-site studies and 1 hour during the on-site. Moreover, for smaller FIs, the FSA indicated that AML/CFT assessments are not held annually, but only when there are indications that an assessment would be necessary. The assessors found that some institutions, that were deemed to be high risk, had just been assessed for the first time in 7 years. Not surprisingly, the assessment found some major shortcomings (like lack of a good AML/CFT compliance handbook within the institutions) that should normally not be found in countries that have implemented the FATF standard for some time.
30.Resources, integrity and training	PC	Financial Intelligence Unit: The number of staff is inadequate to deal with the volume of STRs that the MLU currently receives because much of the MLU's activities are based on inefficient manual processes. For instance, the MLU does not accept STRs electronically; most are submitted either by fax, post or in person (though some are provided on a computer disc), after which the MLU staff must manually input the STRs into their system—even though most representatives from the private sector that met with the assessors indicated a strong desire and the current technical capability to submit reports electronically. Much of the MLU's analytical processes are handled manually and, with its current systems, there is no possibility for the system to automatically draw connections between STRs. The MLU can only work on a few of the STRs that it receives; the rest are simply filed away for future reference. Manual analysis is done, but is often dependent upon the MLU staff remembering a person's name or a previous STR. This process is clearly very inefficient. The management and resources of the MLU currently are not ring-fenced. High staff turnover at the MLU has caused some difficulties in maintaining effective relationships with reporting entities. Only two of the MLU's staff are trained in the use of Analysts Notebook. The joint involvement of the Ministry of Finance (through the Control Committee) and the Ministry of Justice & Police (as the ministry directly responsible for the MLU's operation and budget) may result in an unfocused and fragmented approach to the MLU's development. There seems to be widespread recognition that the MLU's resources are inadequate. Although, additional budgetary resources have been dedicated to ØKOKRIM to address these issues, the assessment team remains of the view that these resources are still inadequate. Law enforcement and prosecutorial authorities: The Police College currently provides an annual advanced training course to police officers and lawyers on economic crime; however, Norway acknowledges that this is not sufficient to meet the need for competence in this area. Consequently, Norway is

		experiencing difficulty in recruiting lawyers and police officers with adequate professional competence in the area of economic crime. Moreover, there is concern that members of economic crime teams must wait too long to obtain advanced training in economic crime cases. There is concern that ØKOKRIM attracts too many of the most highly trained economic crime investigators—to the detriment of the police districts. There is also some concern that, in the last few years, the Police Directorate has not given sufficient priority to AML efforts with regards to the Police College's involvement, ØKOKRIM and others. Supervisory authorities: Considering the number of entities that the FSA is responsible for supervising, its number of staff seems inadequate.
31.National co-operation	LC	Although formal meetings do take place, solid outcomes do not always seem to result. There is still room for improvement in more effective interagency co-operation.
32.Statistics	PC	Not all of the statistics collected by the MLU are reliable. In 2004, due to some technical failures with respect to connectivity with the Egmont Secure Web System, the MLU had to replace some computer hardware. This led to a loss of data relating to requests from foreign FIUs, including its statistics relating to formal requests for assistance made or received by the MLU, and spontaneous referrals made by the MLU to foreign authorities. The inadequacy of the MLU's statistics collection mechanisms (i.e. its computer systems) has thus impeded its statistics collection capabilities. No statistical information is available concerning the criminal sanctions that were imposed on persons convicted of money laundering. Norwegian authorities report that it is difficult to know exactly how many money laundering cases really exist because it depends on how the judge characterises the case. Norway does not maintain statistics concerning sanctions imposed for failing to comply with AML/CFT obligations. Norway does not collect statistics concerning the nature of the mutual legal assistance request, whether the request was granted or refused, what crime the request was related to or how much time was required to respond. Norway does not collect statistics concerning the nature of the request, whether the request was granted or refused, what crime the request was related to or how much time was required to respond. The statistics related to extradition only include persons being extradited to or from Norway in 2003. Statistics for 2004 are unavailable due to a reorganisation of Norway's file system. Requests for extradition between the Nordic countries may, pursuant to the Act for extradition within the Nordic countries dated 03 March 1961, be sent directly between the prosecuting authorities. There are no statistics available concerning these requests. Norway does maintain statistics concerning the number of formal requests for assistance made to or received by the FIU from foreign counterparts. The figures are uncertain because the registration routines are not quite clear, especially as regards the requests made to foreign counterparts.
33.Legal persons – beneficial owners	LC	Norway could provide much more timely access to information concerning beneficial ownership.
34.Legal arrangements – beneficial owners	NA	Recommendation 34 is not applicable in the Norwegian context.
International Co-operation		
35.Conventions	LC	Implementation of the Palermo Convention: Article 6(2)(e) of the Convention obligates countries to make self-laundering an offence unless it is contrary to fundamental principles of domestic law. Self-laundering is not an offence in Norway, but this cannot be justified on the basis of its being contrary to a fundamental law. Implementation of the Terrorist Financing Convention: Article 18(1)(b) of the Convention requires countries to implement efficient measures to identify customers in whose interest accounts are opened is insufficiently implemented. Norway's implementation of Recommendation 5 does not include adequate measures to ascertain the identity of beneficial owners.

36.Mutual legal assistance (MLA)	LC	In all cases involving mutual legal assistance requests from non-Nordic countries (where coercive measures are being sought), dual criminality applies. Additionally, for non-Schengen countries some of the other requirements that apply to extradition requests also apply. This creates one difficulty, however, with regards to the application of dual criminality to mutual legal assistance requests relating to the following ML/FT activities that have not been properly criminalised in Norway: Self-laundering; conspiracy between 2 people to commit ML; and collecting funds for a terrorist organisation/terrorist.
37.Dual criminality	LC	The application of dual criminality may create an obstacle to mutual legal assistance and extradition in cases involving ML/FT activities that have not been properly criminalized in Norway.
38.MLA on confiscation and freezing	PC	Norway must start its own confiscation in situations other than those covered by the Vienna and Strasbourg Conventions. A procedure that requires a case to be made out before a local (Norwegian) court on the basis of foreign evidence is inherently less effective than one where the Norwegian court satisfies itself that a foreign court has made a charging/seizing/confiscation order, and then simply gives effect to that order.
39.Extradition	LC	Overall, there is concern that (except in the case of extradition requests from Nordic countries where dual criminality does not apply), extradition may be impeded when the case involves the following ML/FT activities that are not properly criminalised in Norway: (i) self-laundering; (ii) conspiring to commit ML outside of the context of an organised criminal group; and (ii) obtaining or collecting of funds/asset where the funds/assets are collected to be used by a terrorist organisation or individual terrorist where the use/intended use cannot be connected with a terrorist act and the funds have not yet been provided to the terrorist organisation/terrorist.
40.Other forms of co-operation	C	Recommendation 40 is fully observed.
Nine Special Recommendations	Rating	Summary of factors underlying rating
SR.I Implement UN instruments	PC	Implementation of the Terrorist Financing Convention: Article 18(1)(b) of the Convention requires countries to implement efficient measures to identify customers in whose interest accounts are opened is insufficiently implemented. Norway's implementation of Recommendation 5 does not include adequate measures to ascertain the identity of beneficial owners. Implementation of S/RES/1267(1999): Although Norway has implemented measures that penalise breaches of freezing orders issued pursuant to S/RES/1267(1999), it does not monitor or supervise for compliance with this requirement (as required by section 8 of the resolution). Implementation of S/RES/1373(2001): Norway's implementation of S/RES/1373(2001) is not adequate enough. No effective mechanisms exist for communicating actions taken under S/RES/1373(2001) to the financial sector. Moreover, there are no specific measures in place to monitor compliance with the obligations pursuant to S/RES/1373(2001).
SR.II Criminalise terrorist financing	LC	In addition to criminalising the activities enumerated in the Terrorist Financing Convention, countries are also obligated to criminalise a third type of activity—collecting funds in the knowledge that they are to be used (for any purpose) by a terrorist organisation or an individual terrorist. Norway has not yet criminalised this type of activity.
SR.III Freeze and confiscate terrorist assets	PC	Norway has not implemented measures to monitor compliance with the 1968 Act and Regulations (S/RES/1267(1999) or freezing mechanisms issued pursuant to s.202d of the Penal Code (S/RES/1373(2001)). The freezing action pursuant to S/RES/1267(1999) can be legally challenged by the entity frozen; however, the Norwegian authorities could not point at clear gateways for such action. Rather it is assumed that the entity frozen will use the same legal mechanisms that any citizen has at its disposal to challenge governmental decisions. Norway has issued some

		guidance to financial institutions and other persons/entities that may be holding targeted funds/assets; however, this guidance focuses more on how the FSA processes such lists, rather than giving guidance to financial institutions as to how they should meeting their obligations concerning freezing orders issued pursuant to S/RES/1267(1999). It is unclear how humanitarian exemptions would apply to property frozen pursuant to S/RES/1373(2001). Because the scope of the terrorist financing offence is not quite broad enough, Norway would be unable to freeze the assets in Norway of a person who is considered (more than 50% likely) to have collected funds in the knowledge that they are to be used generally (for any purpose) by a terrorist organisation/individual terrorist. There are no other mechanisms to ensure that relevant information is guided through government authorities to the financial community, nor are there any communication channels for providing feedback between the government and the financial sector. Norway has not issued any guidance to financial institutions and other persons or entities that may be holding targeted funds or other assets concerning their obligations in taking action under freezing mechanisms issued pursuant to S/RES/1373(2001).
SR.IV Suspicious transaction reporting	LC	Unclear the reporting obligations extends to all transactions where there is any suspicion that there is a link to a terrorist organisation or terrorist financier. Concerns raised above in Recommendation 13 about the effectiveness of the reporting system apply equally to SR IV.
SR.V International co-operation	LC	In all cases involving mutual legal assistance requests from non-Nordic countries (where coercive measures are being sought), dual criminality applies. Additionally, for non-Schengen countries some of the other requirements that apply to extradition requests also apply. This creates one difficulty, however, with regards to the application of dual criminality to mutual legal assistance requests relating to the following FT activity that has not been properly criminalised in Norway: collecting funds for a terrorist organisation/terrorist. Norway must start its own domestic proceedings to allow for confiscation in situations other than those covered by the Vienna and Strasbourg Conventions. A procedure that requires a case to be made out before a local (Norwegian) court on the basis of foreign evidence is inherently less effective than one where the Norwegian court satisfies itself that a foreign court has made a charging/seizing/confiscation order, and then simply gives effect to that order. The application of dual criminality may create an obstacle to extradition in cases involving ML/FT activities that have not been properly criminalised in Norway. Overall there is concern that (except in the case of extradition requests from Nordic countries where dual criminality does not apply), extradition may be impeded when the case involves the following FT activity that is not properly criminalised in Norway: obtaining or collecting of funds/assets where the funds/assets are collected to be used by a terrorist organisation or individual terrorist where the use/intended use cannot be connected with a terrorist act and the funds have not yet been provided to the terrorist organisation/terrorist.
SR VI AML requirements for money/value transfer services	PC	As with all other Reporting FIs in Norway, overall implementation of Recommendations 5-7, 15 and 22, and SR VII is very inadequate. This negatively impacts on the effectiveness of AML/CFT measures in the MVTS and other financial institution sectors. There are specific problems in the MVTS sector relating to the effectiveness of the reporting system. Reporting in the sector has diminished recently in part, it seems, because of a breakdown of communication between the MLU and the MVTS provider. Whatever the reason, Recommendation 13 has not been implemented effectively in this sector. There are some concerns about the effectiveness of supervision and sanction in the MVTS sector. In 2003, the MLU received information on approximately 2 500 MVTS transactions, and in 2004 the number of transactions reported exceeded 5 000. These STRs were submitted by the old MVTS provider. The successor MVTS provider commenced operations in early 2004, but reports have only been filed once by it. Although this problem has been brought to the attention of the FSA, no corrective action had been taken at the time of the on-site visit. However, subsequently, the FSA has started action to remedy this deficiency.
SR VII Wire transfer	NC	The MLA does not contain any obligation to collect or maintain this information for an

rules		occasional customer who is ordering a wire transfer that is below the threshold of NOK 100 000 (EUR 12 100/USD 15 800) unless the reporting entity suspects that the transaction is associated with terrorism or ML/FT (in which case, the reporting entity must request proof of identity, regardless of whether the customer is an occasional or permanent one (MLA s.5 para.4)). This threshold is significantly higher than the USD 3 000 threshold currently permitted by SR VII. There is no legal obligation to include full originator information in the message or payment form that accompanies a cross-border or domestic wire transfer. For domestic wire transfers, there is no obligation to maintain full originator information in such a manner that: (i) it can be made available to the beneficiary financial institution and to competent authorities within three business days of receiving a request; and (ii) domestic law enforcement authorities can compel immediate production of it. There is no obligation on Reporting FIs to ensure that non-routine transactions are not batched where this would increase the risk of money laundering or terrorist financing. There are no obligations on intermediary Reporting FIs in the payment chain to maintain all of the required originator information with the accompanying wire transfer. There are no obligations on beneficiary Reporting FIs to adopt risk-based procedures for identifying and handling wire transfers that are not accompanied by complete originator information. There are no sanctions for breaching many of the obligations under SR VII because many of the obligations themselves have not been implemented.
SR.VIII Non-profit organisations	NC	Norway has not yet carried out a review of the laws and regulations that relate to non-profit organisations (NPOs) that may be abused for the financing of terrorism. Norway has not implemented measures to ensure that terrorist organisations cannot pose as legitimate NPOs, or to ensure that funds/assets collected by or transferred through NPOs are not diverted to support the activities of terrorists or terrorist organisations. The system is further weakened by the fact that Recommendation 5 has not been implemented with regards to beneficial ownership.
SR IX Cash couriers	PC	The declaration obligation does not apply to bearer negotiable instruments—although when foreign negotiable instruments are cashed in, at a Norwegian bank for instance, the bank involved will be obliged to report the transaction to the Currency Transaction Register. However, in such cases it is the cashing-in that is being detected and, therefore, required to be reported, not the cross-border transportation itself, because the cashing-in is when the transaction takes place. Moreover, this system will not capture cross-border transportations of bearer negotiable instruments in Norwegian currency, regardless of whether they are cashed in Norway or not. In relation to bearer negotiable instruments, there is no possibility to stop or restrain them to determine whether evidence of ML/FT may be found, there is no penalty for falsely declaring them (because there is no obligation to declare); identification of the bearer is not be retained, there is no penalties for making a false declaration; etcetera. The police and Prosecution Authority (including ØKOKRIM and the MLU) can only access the Currency Transaction Register after an investigation is started. Lists of designated persons and entities made pursuant to UN S/RES/1267(1999) are distributed to the customs authorities and are available to all customs posts electronically. However, lists of persons/entities designated pursuant to S/RES/1373(2001) are not.

Table 2: Recommended Action Plan to Improve the AML/CFT System

AML/CFT System	Recommended Action (listed in order of priority)
1. General	No text required
2. Legal System and Related Institutional Measures	
Criminalisation of Money Laundering (R.1 & 2)	• Criminalise conspiracy involving 2 people to commit ML. • Extend the ML offence to self-laundering. • Ascertain why the number of aggravated ML cases remains small (even though the threshold for the offence is very low). Depending on the underlying reasons, Norway should consider whether additional legislative or training measures need to be taken.
Criminalisation of Terrorist Financing (SR.II)	• Clarify the legislation to ensure that the offence covers collecting funds in the knowledge that they are to be used (for any purpose) by a terrorist organisation/individual terrorist.
Confiscation, freezing and seizing of proceeds of crime (R.3)	• Norway should continue its work in improving the awareness of police concerning the need to secure confiscation claims (either by charging or seizure) early on in the case. • Norway should consider implementing the following elements that, while not required by the FATF Recommendations, would further enhance an already effective confiscation regime: giving the authorities the power to seize/charge all of the defendant's property in appropriate cases (not just ensuring that the court can order a defendant to disclose all of his/her assets and allowing property to be seized/charged after a confiscation order has been issued. • Norway should examine whether better data could be collected to identify the reasons for failure to recover the some proceeds and whether it is changing over time.

Freezing of funds used for terrorist financing (SR.III)	• Amend the laws to fully implement S/RES/1373(2001) consistent with its aims and objectives, preferably in a similar way as S/RES/1267(1999) has been implemented. This would create one single system for designating, listing, freezing, de-listing and de-freezing of terrorist assets.
	• Enact measures that would allow for the possibility of freezing funds or other assets where the suspect belongs to a terrorist organisation or is known to finance such organisations or terrorists in general (even if the financing cannot be connected to an act of terrorism.
	• In relation to S/RES/1373(2001): (i) implement effective systems for ensuring that relevant information is guided through government authorities to the financial community; (ii) improve implementation of S/RES/1373(2001).
	• Give clear practical guidance to financial institutions concerning how to implement freezing actions under S/RES/1267(1999) or S/RES/1373(2001) and develop policy and procedures to handle freezing cases.
	• Have measures in place to monitor compliance with both S/RES/1267(1999) and S/RES/1373(2001).
	• In relation to S/RES/1267:
	  • Establish an effective system for communication among governmental institutions and with the private sector (and the like) to facilitate every aspect of the freezing/unfreezing regime within Norway;
	  • Provide clear guidance (more than the bare reporting obligation in the MLA) to financial institutions that may hold terrorist funds concerning their responsibilities under the freezing regime;

	• Create a procedure for considering de-listing requests and for unfreezing the funds or other assets of de-listed persons. • Create a procedure for unfreezing, in a timely manner, the funds/assets of persons inadvertently affected by the freezing mechanism upon verification that the person is not a designated person. • Clarify the procedure for authorising access to funds/assets that are frozen and that are determined to be necessary on humanitarian grounds in a manner consistent with S/RES/1452(2002); • Create an appropriate procedure for a judicial review of freezing actions.
The Financial Intelligence Unit and its functions (R.26, 30 & 32)	• It is recommended that Norway allocate more staff and technological resources to the MLU as soon as possible. In particular, the MLU needs better technology. Although the staff are very professional and highly trained, all staff need to be trained in the use of analytical tools such as Analysts Notebook. In addition to a system for electronic reporting, the MLU urgently needs tools to conduct electronic analysis as soon as possible. • The management and resources of the MLU currently are not ring-fenced. It is recommended that Norway ring-fence the responsibility and resources of the MLU. • It is recommended that Norway should reconsider the twin rules of deleting STR information not acted on within 5 years and STR information where the suspicion has been rebutted. • Norway should improve the MLU's statistics collection capabilities by providing it with better technological tools. • The Police Directorate is planning for a new national intelligence system which makes it possible to search for information in all the police databases from one platform to gather all information in one database in order to co-ordinate and facilitate searches for information. There is now a discussion at the Police Directorate to link and match this register with the information from STRs. Norway should ensure that this initiative does not negatively impact the MLU's ability to securely protect and disseminate STR information only in accordance with the law.
Law enforcement, prosecution and other competent authorities (R.27, 28, 30 & 32)	• Norway should ensure that sufficient priority is given to AML efforts with regards to the Police College's involvement, ØKOKRIM and others. • Likewise, even though the Action Plan 2004 recognises that more resources need to be allocated towards training, and the Police College had hired a staff member specifically for that purpose, the hire was cancelled just prior to the on-site visit. Norway should ensure that this hiring is carried out as soon as possible. • Norway should ensure that additional resources are allocated to AML/CFT training for police and prosecutors. • Norway should collect statistics concerning the types of criminal sanctions imposed for ML.
3. Preventive Measures – Financial Institutions	
Risk of money laundering or terrorist financing	
Customer due diligence, including enhanced or reduced measures (R.5 to 8)	• Norway should implement the following missing elements of Recommendation 5 as a matter of priority: • There should not be an exemption from customer due diligence if the reporting FI has actual suspicion that a transaction is connected with ML/TF (i.e. there should not be an exemption from MLA section 5 para.3).

	• There is no requirement for a Reporting FI to re-perform customer identification when it has doubts about previously obtained identification data. Presently the obligation is only to verify data if the information contained in the presented documents is on its face incorrect (MLR s. 8). • Although there are extensive requirements for identification of a customer that is a legal person, there is no requirement for a Reporting FI to verify that an individual purporting to act on behalf of that legal person is in fact so authorised. • There is no definitive duty imposed on a Reporting FI to check if the customer is acting on behalf of another person. Currently the duty is a contingent one (i.e. to check only if it has reasons to suspect this to be the case). • There is also no duty imposed to check the corporate or ownership structure behind a customer who is a legal person, by identifying, for example, the controlling shareholder or operating mind behind the customer • There is no duty imposed to inquire as to the purpose and intended nature of the business relationship vis-à-vis the Reporting FI itself. • Reporting FIs are not required by law to conduct ongoing due diligence on their business relationships. • There are also no rules governing the CDD treatment of existing customers. • Norway should implement both Recommendations 6 and 7 as a matter of priority. • Norway is recommended to reassess the existing identification requirements and procedures and consider developing measures that are more tailored to the business practices of the non-bank financial sectors.
Third parties and introduced business (R.9)	• No recommendations.
Financial institution secrecy or confidentiality (R.4)	• Allowing a confidentiality override so that banks can exchange information in the course of investigating suspicious transactions is sensible, but Norway should consider extending this to other types of Reporting FIs. This recommendation does however not affect the rating
Record keeping and wire transfer rules (R.10 & SR.VII)	• SR VII has not been implemented in most respects. Norway should implement the provisions of SR VII as soon as possible.
Monitoring of transactions and relationships (R.11 & 21)	• No recommendations.
Suspicious transaction reports and other reporting (R.13-14, 25 & SR.IV)	• The FSA should ensure that non-bank financial institutions, including MVTS providers, comply with their reporting obligations. Steps should also be taken to refocus reporting in general to concentrate more on the nature of the transaction. • The guidance given by the FSA should be deepened, broadened and based on the different typologies, trends and techniques that focus more attention on the nature of transactions themselves. Additional guidelines that are more tailored to particular types of financial institutions should be issued. • More outreach to the DNFBP sectors should be undertaken to ensure that sector participants understand the rationale for the reporting obligation and how to comply with it. • The MLU should deliver more specific feedback to reporting entities, particularly concerning the status of STRs and the outcome of specific cases.
Other types of reporting (R.19 and SR IX)	• Overall, Norway's declaration system is insufficient in scope, and should be extended to include incoming and outgoing cross-border transportations of bearer negotiable instruments.

	• At a minimum, the MLU, and possibly also the police/ØKOKRIM should have electronic access to the Currency Transaction Register even where no investigation has formally commenced. The MLU should be able to conduct a check against this register in the same way as it conducts checks against many other registers when it receives an STR. • In addition to distributing the lists of persons designated under S/RES/1267(1999) to the customs authorities, lists of persons designated under S/RES/1373(2001) should also be distributed.
Internal controls, compliance, audit and foreign branches (R.15 & 22)	• Reporting Fis should be obligated to establish screening procedures to ensure high standards when hiring employees. • Norway should implement a requirement that a financial institution inform the FSA if its foreign branch or subsidiary is unable to observe appropriate AML/CFT measures because this is prohibited by the laws or regulations of the host country. • Once Norway has corrected the legal requirements in the other areas of its AML/CFT regime (particularly with regards to customer identification measures), Reporting FIs should be obligated to implement satisfactory internal controls in that regard.
Shell banks (R.18)	• Norway should implement provisions that: (i) prohibit financial institutions from entering into or continuing correspondent banking relationships with shell banks; and (ii) obligate financial institutions to satisfy themselves that the respondent financial institution in a foreign country does not permit its accounts to be used by shell banks.
The supervisory and oversight system - competent authorities and SROs (R. 17, 23, 29 & 30).	• Although the FSA can sanction the officers/employees of the entities it supervises for failing to comply with the MLA through its powers under the Financial Supervision Act, Norway should clarify the MLA in this regard. • The FSA should be given additional resources to be allocated for AML/CFT supervision. • The FSA should consider creating a well staffed stand alone AML/CFT unit or at least a team of examiners specialising in AML/CFT measures that check FIs compliance with AML/CFT on an ongoing basis for all supervised entities.
Financial institutions - market entry and ownership/control (R.23)	• Financial institutions should be obligated to notify the FSA of changes in management.
AML/CFT Guidelines (R.25)	• The FSA should respond to the requests of Reporting FIs/BPs for additional and more specific AML/CFT guidelines on a more regular basis. Just as was done in the banking, insurance and securities sectors, such guidance should be more tailored to the different types of FIs and DNFBPs. • The group that was established by the Ministry of Justice & Police to propose AML/CFT guidance for lawyers is encouraged to complete the final stages of its work as soon as possible. • The NIPA, the NARF and ØKOKRIM should finish developing guidance for accountants and auditors concerning compliance with AML/CFT obligations.
Ongoing supervision and monitoring (R.23, 29 & 32)	• The self-assessment reports used to identify priority FIs for inspection visits should be revised to include questions relating to AML/CFT • Norway should ensure that AML/CFT assessments of Reporting FIs occur more regularly, particularly in high risk institutions. • Norway should collect and maintain statistics concerning the number and type of sanctions applied.
Money value transfer services (SR.VI)	• The FSA should take immediate steps (including the application of sanctions, if necessary) to correct the problems with reporting in this sector. • The FSA should improve the effectiveness of its monitoring and supervision of this sector. • Norway should take steps to properly implement Recommendations 5-7, 15 and 22, and SR VII. These measures should apply to all Reporting FIs, including MVTS operators

4. Preventive Measures –Non-Financial Businesses and Professions	
Customer due diligence and record-keeping (R.12)	• Norway should implement Recommendations 5 and 6 fully and make these measures applicable to both Reporting FIs/BPs. • Overall, it should be made clear that any person who provides company services is subject to the MLA. Clarifying the rules could include codifying the current practice by amending the law to restrict the provision of company services to only certain groups (e.g. accountants and lawyers) to reflect the current practice.
Monitoring of transactions and relationships (R.12 & 16)	• It would be preferable that lawyers be appropriately restricted or guided concerning what to advise a potential client when refusing to establish a customer relationship because it would imply an obligation to file a report to the MLU. In such circumstances, it should be sufficient to advise the potential client that the case cannot be accepted because of it would place the lawyer in a conflict of interest, rather than specifying that it would be the obligation to report to the FIU. However, this recommendation does not affect the rating.
Suspicious transaction reporting (R.16)	• See fourth bullet point of recommended action for R.17, 24-25 below.
Internal controls, compliance & audit (R.16)	• See second bullet point of recommended action for R.12 above.
Regulation, supervision and monitoring (R.17, 24-25)	• An authority should be designated to monitor and supervise dealers in precious metals/stones for compliance with AML/CFT obligations. • Norway should be aware of issues relating to the illicit operation of internet casinos in Norway, and should be prepared to address these problems. • See also second bullet point of recommended action for R.17, 23, 29 & 30 above. • The FSA should issue more tailored and sector-specific guidance to DNFBPs concerning how to properly implement their AML/CFT obligations, including what sorts of transactions could be considered unusual and related to ML/FT.
Other designated non-financial businesses and professions (R.20)	• Norway should continue to take measures to encourage the development and use of modern and secure techniques for conducting financial transactions that are less vulnerable to money laundering.
5. Legal Persons and Arrangements & Non-Profit Organisations	
Legal Persons – Access to beneficial ownership and control information (R.33)	• Norway should take additional measures to ensure that information concerning beneficial ownership is available on a more timely basis.
Legal Arrangements – Access to beneficial ownership and control information (R.34)	• No recommendations.
Non-profit organisations (SR.VIII)	• Norway should conduct a review of the adequacy of its laws and regulations relating to non-profit organisations that can be abused for the financing of terrorism. • Norway should implement measures to ensure that terrorist organisations cannot pose as legitimate non-profit organisations. • Norway should implement measures to ensure that funds or other assets collected by or transferred through non-profit organisations are not diverted to support the activities of terrorists or terrorist organisations.
6. National and International Co-operation	
National co-operation and coordination (R.31)	• Norway should take steps to improve co-ordination, particularly at the operational level. • See also second bullet point of recommended action for R.26, 30 & 32 above. • Norway should ensure that sufficient resources are allocated to implement the recommendations in the Action Plan 2004.
The Conventions and UN Special	• Norway should fully implement: article 6(2)(e) of the Palermo Convention by

Resolutions (R.35 & SR.I)	making self-laundering a criminal offence; article 18(1)(b) of the Terrorist Financing Convention by implementing effective measures to identify beneficial owners; article 18(1)(b) of the Terrorist Financing Convention by implementing effective measures to identify beneficial owners; section 8 of S/RES/1267(1999) by implementing measures to supervise and monitor reporting entities for compliance with freezing orders issued pursuant to this resolution; and S/RES/1373(2001).
Mutual Legal Assistance (R.32, 36-38, SR.V)	• At present, Norway has to rely on section 24 of the Extradition Act as the main provision under which it provides mutual legal assistance. Norway should take measures to address the difficulties that this creates (particularly with regards to the application of dual criminality to mutual legal assistance requests from Nordic countries relating to ML/FT activities that have not been properly criminalized in Norway). One way to do this would be to enact separate and comprehensive mutual legal assistance legislation. • Norway should consider applying even less restrictive requirements to mutual legal assistance requests, particularly with regards to its application of dual criminality. In particular, Norway should take measures to address the potential obstacles that dual criminality presents in mutual legal assistance cases where the ML/FT activity has not been properly criminalised in Norway. In particular, Norway should properly criminalise the following types of ML/FT activities: (i) self-laundering; (ii) a conspiracy between 2 people to commit ML; and (ii) obtaining or collecting funds/asset where the funds/assets are collected to be used by a terrorist organisation or individual terrorist (for any purpose) - without, however, being made available to the organisation or terrorist in question. • Norway should keep a fuller set of statistics, thus enabling it to better track the mutual legal assistance requests it receives and makes, and ensuring they are handled in a timely way. • Norway should consider enacting legislation that would clearly allow for confiscation in situations other than those covered by the Vienna and Strasbourg Conventions. Norway should also consider enacting measures that would allow it to give effect to a foreign freezing, seizing or confiscation order, again in situations other than those covered by the Vienna and Strasbourg Conventions, without the necessity of starting its own domestic proceedings. • Norway should keep statistics concerning: (i) the nature of mutual legal assistance requests; (ii) whether the mutual legal assistance request was granted or refused; (iii) what crime the request was related to; and (iv) how much time was required to respond to the request.
Extradition (R.32, 37 & 39, & SR.V)	• Norway should also ensure that the application of dual criminality does not impede extradition when the case involves ML/FT activities that are not properly criminalised in Norway. See also second bullet in recommended action for R.32, 36-38 & SR.V above. • Norway should also collect and maintain statistics on: (i) the number of requests for extradition; (ii) the nature of the request; (iii) whether the request was granted or refused; (iv) what crime the request was related to; or (v) how much time was required to respond. Statistics concerning requests for extradition between the Nordic countries that are sent directly to the prosecuting authorities should also be collected and maintained.
Other Forms of Co-operation (R.32 & 40, & SR.V)	• Norway should ensure that the MLU's new systems for facilitating co-operation with foreign counterparts are working effectively. As well, Norway should collect and maintain statistics concerning the number of sanctions applied, and the number of formal requests for assistance made and received by supervisors relating to or including AML/CFT. Norway should also improve the certainty of its statistics concerning the number of formal requests for assistance made to or received by the MLU from foreign counterparts.
7. Other Issues	

Other relevant AML/CFT measures or issues	• No recommendations.
General framework – structural issues	• No recommendations.

Table 3: Authorities' Response to the Evaluation (if necessary)

Relevant sections and paragraphs	Country Comments