



FINANCIAL ACTION TASK FORCE

Mutual Evaluation Fourth Follow-Up Report

Anti-Money Laundering and Combating the
Financing of Terrorism

NORWAY

26 February 2009

Following the adoption of its third Mutual Evaluation (MER) in June 2005, in accordance with the normal FATF follow-up procedures, Norway was required to provide information on the measures it has taken to address the deficiencies identified in the MER. Since June 2005, Norway has been taking action to enhance its AML/CFT regime in line with the recommendations in the MER. The FATF recognizes that Norway has made significant progress and that Norway should henceforward report on a biennial basis on the actions it will take in the AML/CFT area.

© 2009 FATF/OECD. All rights reserved.

No reproduction or translation of this publication may be made without prior written permission. Requests for permission to further disseminate, reproduce or translate all or part of this publication should be obtained from the FATF Secretariat, 2 rue André Pascal 75775 Paris Cedex 16, France (fax +33 1 44 30 61 37 or e-mail: Contact@fatf-gafi.org).

NORWAY: APPLICATION TO MOVE FROM REGULAR FOLLOW-UP TO BIENNIAL UPDATES

Note by the Secretariat

Key decision:

Decide whether Norway has taken sufficient action to be moved from regular follow-up to biennial updates, and should be directed to provide a biennial update to the Plenary in two years time (June 2011)?

I. Introduction

1. The purpose of this paper is to introduce Norway's fourth report back to the Plenary concerning the progress that it has made to remedy the deficiencies that were identified in its third mutual evaluation report (MER), and to consider Norway's application to move from regular follow up to biennial updates.

2. The MER of Norway was adopted by the Plenary on 10 June 2005. Norway was rated partially compliant on Recommendation 5 (customer due diligence) which is a core Recommendation and, as a result, Norway was placed on the regular follow-up process. While subject to regular follow up, Norway reported back to the Plenary in June 2007, June 2008 and February 2009¹. At the February 2009 Plenary meeting, Norway indicated that sufficient action for removal from the follow-up process would be taken by the Plenary meeting in June 2009, and the Plenary decided that Norway could apply for removal from the regular follow-up process at that time.

3. This paper is based on the updated procedure for removal from the regular follow-up process, as agreed by the FATF Plenary in October 2008 and February 2009². The procedure requires a country to take sufficient actions to be considered for removal from the process. To have taken sufficient action in the opinion of the Plenary, it is necessary that the country has an effective anti-money laundering (AML)/counter-terrorist financing (CFT) system in force, under which the country has implemented the following (Special) Recommendations at a level essentially equivalent to compliant (C) or largely compliant (LC), taking into consideration that there would be no re-rating: R. 1, 3-5, 10, 13, 23, 26, 35-36 and 40, and SR.I-V (core and key Recommendations). As indicated in the chart below, Norway was rated partially compliant (PC) or non-compliant (NC) on the following Recommendations:

Core Recommendations ³ rated NC or PC
R. 5 (PC)
Key Recommendations ⁴ rated NC or PC
R. 26 (PC), SR. I (PC), SR. III (PC)

¹ The first follow-up report is FATF/PLEN(2007)16, the second follow-up report is FATF/PLEN(2008)22, and the third follow-up report is FATF/PLEN(2009)8.

² Third Round of AML/CFT Evaluation Process and Procedures, paragraphs 39 (c), 40 and 41.

³ The core Recommendations are R. 1, R. 5, R. 10, R. 13, SR II and SR IV.

⁴ The key Recommendations are R. 3, R. 4, R. 23, R. 26, R. 35, R. 36, R. 40, SR I, SR III, and SR V.

Other Recommendations rated PC
R. 12, R. 18, R. 25, R. 30, R. 32, R. 38, SR. VI, SR. IX
Other Recommendations rated NC
R. 6, R. 7, SR. VII, SR. VIII

4. As prescribed by the mutual evaluation procedures, Norway provided the Secretariat with a full report on its progress, including supporting material (laws and data to assess effectiveness to a certain extent) (see Annexes 1 and 2). The Secretariat has drafted a detailed analysis of the progress made for R. 5, 26, SR. I and SR. III (core and key Recommendations), as well as an analysis of all other Recommendations rated PC or NC. This draft analysis was provided to Norway (with a list of additional questions) for its review, and comments were received. During the process, Norway has provided the Secretariat with all information requested.

5. As a general note on all applications for removal from regular follow-up, the procedure is described as a *paper-based desk review*, and, by its nature, it is less detailed than a mutual evaluation report. The analysis focuses on the (Special) Recommendations that were rated PC/NC, which means that only a part of the AML/CFT system is reviewed. Such analysis essentially consists of looking into the main laws, regulations and other material to verify the technical compliance of domestic legislation with the FATF standard. In assessing whether sufficient progress had been made, effectiveness is taken into account to the extent possible in a paper-based desk review, primarily through a consideration of data and statistics provided by the country. It is also important to note that these conclusions do not prejudice the results of future assessments, as they are based on information which was not verified through an on-site process and was not, in every case, as comprehensive as would exist during a mutual evaluation.

II. Main conclusion and recommendations to the Plenary

6. **Core Recommendations:** For R. 5, most of the deficiencies identified in the MER relating to the customer due diligence (CDD) framework have been addressed by enacting new legislation. Although a few shortcomings remain, Norway has taken sufficient action to bring its compliance to a level essentially equivalent to LC.

7. **Key Recommendations:** For R. 26 (financial intelligence unit (FIU)), Norway has made real progress, particularly to address the deficiencies relating to effectiveness. Although some concerns remain, overall, sufficient action has been taken to bring the compliance to a level essentially equivalent to LC. Norway has also partially addressed the deficiencies in relation to SR III (freezing of terrorist assets) and SR I (ratification and implementation of UN instruments), but not to a satisfactory level.

8. **Other Recommendations:** As for the overall set of other Recommendations that were rated PC/NC, Norway has made important progress. Leaving aside effectiveness, Norway has taken sufficient action to have achieved a level of compliance that is essentially equivalent to at least an LC on R. 6, 7, 12, 18, 25, 30, 32, SR VI, VII and SR IX. Norway has also taken steps to improve its compliance with R. 38 and SR VIII, albeit not yet to a satisfactory level.

9. **Conclusion:** Overall, Norway has reached a satisfactory level of compliance with all core Recommendations and eight of the key Recommendations, but has not reached a satisfactory level of compliance with two of the key Recommendations – SR III and SR I. It is, however, somewhat mitigating that the main concerns relating to SR I are with regard to the insufficient implementation of SR III, and so the underlying issues are the same.

10. The mutual evaluation follow-up procedures indicate that, for a country to have taken sufficient action to be considered for removal from the process, it must have an effective AML/CFT system in force, under which it has implemented all core and key Recommendations at a level essentially equivalent to C or LC, taking into account that there would be no re-rating. The Plenary does, however, retain some limited flexibility with regard to the key Recommendations if substantial progress has also been made on the overall set of Recommendations that have been rated PC or NC.

11. Norway has made substantial progress on the overall set of 16 Recommendations that were rated PC or NC. In particular, Norway has taken sufficient action to bring its compliance to a level essentially equivalent to at least an LC in relation to 12 of the Recommendations that were rated PC/NC (two out of the four core and key Recommendations (R. 5 and 26), and 10 out of the 12 other Recommendations). For the remaining two other Recommendations that were rated PC/NC, some positive steps have been taken to address the deficiencies, albeit not to a satisfactory level. Overall, however, Norway has made considerable efforts to strengthen its AML/CFT regime since 2005, including by making legislative amendments, allocating additional budgetary resources, and strengthening supervisory routines and practices. Consequently, it is recommended that this would be an appropriate circumstance for the Plenary to exercise its flexibility and remove Norway from the regular follow up process, with a view to having it present its first biennial update in June 2011.

III. Overview of Norway's progress

A. Overview of the main changes since the adoption of the MER

12. Norway's AML/CFT regime has been significantly reformed, with a view to addressing the deficiencies identified in the June 2005 MER. The most important measure taken in the reform process is the adoption of the new Money Laundering Act (MLA) and related regulations (MLR), both of which entered into force on 15 April 2009, and replace the 2003 Money Laundering Act and related 2004 regulations. The new MLA and MLR essentially enhance preventative measures in the financial and DNFBP sectors. Some significant features of the new MLA and MLR are as follows:

- CDD obligations are significantly enhanced in both the financial and DNFBP sectors through the introduction of obligations to identify beneficial owners, inquire about the purpose and nature of the intended business relationship, monitor customer relationships on an ongoing basis, and conduct enhanced due diligence for some categories of high risk customer, including politically exposed persons (PEPs) and correspondent banking relationships (R. 5, 6, 7 and 12).
- The application of the FATF Recommendations to money or value transfer service (MVTS) providers, and the related supervisory framework, are improved (SR VI).
- Additional measures have been introduced in relation to shell banks (R. 18).
- Specific requirements to ensure that full originator information accompanies cross-border wire transfers were introduced (SR VII).

13. Other legislative action has been taken to address the deficiencies identified in relation to SR IX (cash couriers) and SR VIII (non-profit organisations (NPOs)). In particular, the Customs Act was amended to extend the declaration obligation to bearer negotiable instruments (BNI) and improve implementation of SR IX, and a new law was passed to establish a voluntary registration regime for NPOs.

14. Norway has also strengthened its FIU, the Money Laundering Unit (MLU), by introducing a new database system, increasing the number of staff and technical resources, and enhancing training programs.

15. Norway has also taken some steps to improve its measures to freeze terrorist assets (SR III), although some concerns remain with regards to the implementation of S/RES/1373(2001) and monitoring mechanisms. These same concerns continue to impact Norway's implementation of SR I (ratification and implementation of United Nations instruments).

16. Overall, Norway has allocated significantly more resources to AML/CFT in several areas (R. 30) and has generally improved its mechanisms for collecting statistics (R. 32).

B. The legal and regulatory framework

17. Norway's legislative and regulatory scheme consists primarily of: the new MLA (law); the new MLR (regulations); and the Financial Supervisory Authority (FSA) Guidance Notes 2004. Norway reports that the FSA intends to issue additional guidance notes in the second quarter of 2009 to further elaborate the AML/CFT requirements.

18. The new MLA and MLR were developed with a view to improving Norway's compliance with the FATF Recommendations, and implementing the European Union (EU) Directive 2005/60/EC (3rd EU AML/CFT Directive) and EU Regulation (EC) No 1781/2006 on wire transfers.

19. Although it is not a member of the EU, as a participant of the EU common market and a signatory of the European Economic Area Agreement (EEA Agreement), Norway implements relevant EU legislation. The EEA Agreement is an agreement between the EU Member States and the European Community (EC) on the one hand, and the three European Free Trade Association (EFTA) States (Iceland, Liechtenstein and Norway) on the other hand. The EEA Agreement extends the EC internal market to the three EFTA States. It was signed on 2 May 1992 and entered into force on 1 January 1994.

20. The main provisions of the EEA Agreement reproduce, by and large, the relevant provisions of the EC Treaty as it stood at the time of the signature, and incorporate (in annexes) secondary EC legislation in the form of regulations, directives, etc. within its scope.⁵ This arrangement implies that EC provisions on the free movement of goods, services, persons, capital, and establishment, as well as the rules on competition and state aid are incorporated in the EEA Agreement. EC provisions concerning financial services, including rules related to AML/CFT, thus form a part of the EEA Agreement. New rules developed by the EC and falling within the scope of the EEA Agreement are regularly incorporated by decisions of a Joint Committee made up by the Contracting Parties.

21. For surveillance purposes and judicial review, the EFTA States have established a structure parallel to that of the EC. By a separate agreement, an EFTA Surveillance Authority (ESA) and an EFTA Court are set up. To ensure that the EFTA States fulfil their obligations under the EEA Agreement and to monitor the applications of the rules, the ESA is vested with competence similar to that of the European Commission. The EFTA Court has jurisprudence in actions brought before it by ESA or in actions against decisions by ESA. To ensure uniform surveillance throughout the EEA, ESA and the Commission cooperate closely, and both ESA and the EFTA Court shall pay due account to rulings by the European Court of Justice.

22. It is in this context that Norway domestically implemented the 3rd EU AML/CFT Directive by transposing it to the new MLA and MLR, and is applying EU Regulation (EC) No 1781/2006 on wire transfers through a provision in the MLR.

⁵ EC rules on trade in agricultural and fishery products are outside the scope of the EEA Agreement, which neither provides for a customs union as the case is in the EC.

IV. Review of the measures taken in relation to the Core Recommendations

Recommendation 5 – rating PC

R. 5 (Deficiency 1): Although Norway has implemented customer identification obligations, it has not implemented full customer due diligence (CDD) requirements.

23. Norway has addressed this deficiency by introducing and implementing more extensive CDD requirements (the specifics of which are described in more detail below) in relation to the particular deficiencies identified in the MER. The new legal requirements adequately address this deficiency.

R. 5 (Deficiency 2): 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 Financial Institution (FI) to verify that the individual is duly authorised to act for the legal person. (MER par. 213)

24. Norway has addressed this deficiency introducing a legal requirement that financial institutions (FIs) obtain documentation certifying that the natural person has the right to represent the customer externally (MLA s. 7). Such certification may be in the form of a certificate of company registration, memorandum of association, written power of attorney or the like. Financial institutions are also now required to identify the person acting on behalf of the customer on the basis of a valid proof of identity using a document, issued by an authorised body, that contains the representative's full name, signature, photograph and personal ID number. The new legal requirements adequately address the deficiency.

R. 5 (Deficiency 3): 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). (MER par. 214)

R. 5 (Deficiency 5): 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.

25. Norway has addressed these deficiencies by requiring financial institutions to verify the identity of beneficial owners on the basis of reasonable measures (MLA s. 7, para. 1 No. 3). The MLA defines "beneficial owners" generally as the "natural persons who ultimately own or control the customer and/or on whose behalf a transaction or activity is being carried out" (MLA s. 2, para. 1 No. 3). This general definition is consistent with the FATF standards and is based on Directive 2005/60/EC. The definition is then further elaborated to describe five situations where a person "in all cases" is to be regarded as a beneficial owner. These five categories (listed below) are intended to cover the same situations as are listed in Directive 2005/60/EC article 3 No. 6 letters a) and b):

- (a) a natural person who directly or indirectly owns or controls more than 25% of the shares or voting rights of the company (with the exception of an entity that has financial instruments listed on a regulated market in an EEA state or is subject to disclosure requirements consistent with those that apply to listing on a regulated market in an EEA state);
- (b) a natural person who exercises control over the management of a legal entity;

- (c) a natural person who is the beneficiary of 25% or more of the assets of a foundation, trust or corresponding legal arrangement or entity;
- (d) a natural person who has the main interest in the establishment or operation of a foundation, trust or corresponding legal arrangement or entity; or
- (e) a natural person who exercises control over more than 25% of the assets of a foundation, trust or corresponding legal arrangement or entity.

26. The first category (a natural person who directly or indirectly owns or controls more than 25% of the shares or voting rights of the company) contains two exceptions (see para. 24(a) above). The first exception (for entities that have financial instruments listed on a regulated market in an EEA area) is based on Directive 2005/60/EC art 3 No. 6 letter a). The Norwegian authorities explain that the rationale behind this exception is that a company that has financial instruments listed on a “regulated market” (as defined in article 4 of EU Directive 2004/39/EC) in the EEA area will be subject to: EEA regulations and disclosure requirements pursuant to Directive 2004/109/EC on the harmonisation of transparency requirements in relation to information about issuers whose securities are admitted to trading on a regulated market and EU Directive 2003/6/EC on insider dealing and market manipulation (market abuse). The second exception (for entities that are subject to disclosure requirements consistent with those that apply to listing on a regulated market in an EEA state) is meant to cover a company that has financial instruments that are listed on a regulated market outside the EEA, but is subject to equivalent disclosure requirements as companies listed within the EEA.

27. In relation to the fourth category (a natural person who has the main interest in the establishment or operation of a foundation, trust or corresponding legal arrangement or entity) (see para. 23(d) above), an illustrative example is provided in the Report from the Government appointed Legislative Committee which, in addition to the Proposal to Parliament, is a tool for interpretation of the law. The example relates to those foundations for which the degree of certainty as to who will be the beneficial owner of the foundation’s assets depends on the formulation and detail of its articles of association. In such cases, a natural person or a class of persons that has the “main interest” in the establishment or operation of the foundation shall, if they can be identified, be regarded as beneficial owners.

28. The MLA provides that the verification of the identity of beneficial owners should be conducted on the basis of “reasonable measures”. Norway explains that this means the identification of beneficial owners is to be conducted on a risk sensitive basis (MLA s. 5), and that when the customer is a legal person, FIs will consult public registers or obtain relevant data from the customer. The Proposal to Parliament (Proposition No. 3 (2008-2009) to the Odelsting), which is a tool for the interpretation of a law, offers the following example: a bank opening an account for a limited company must verify the identity of the shareholders who control the company. This example is somewhat confusing since it suggests that if the shareholders who control the limited company are legal persons themselves, no further steps are needed – although the law itself would suggest that the requirement is to drill down and identify the natural persons who ultimately control the limited company. Norway confirms, however, that this example is meant to be the first step, and that the intention is that financial institutions drill down and identify the natural person who ultimately owns/controls the company, as is required by the law. This is an area that would greatly benefit from further guidance from the FSA, particularly with regards to what constitutes “reasonable measures”. What steps FIs will take in practice (*i.e.* what steps they will consider to be “reasonable measures”) is an issue of effectiveness and implementation that cannot be assessed in a paper-based desk review such as this. However, the law itself is consistent with the requirement to identify beneficial owners, as set out in Recommendation 5, and therefore adequately addresses the technical aspects of this deficiency.

R. 5 (Deficiency 4): 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). (MER par. 214)

29. The new MLA requires FIs to verify the identity of a person (other than the customer) who “has been granted a right of disposal over an account or a deposit, or...the right to carry out the transaction” (s. 7, para. 3). This is a significant improvement over the previous legislation which only required identification of the “customer” (*i.e.* the person attending at the FI), and did not require the identification of a person who is acting on behalf of another. Although the new MLA does not expressly obligate an FI to proactively inquire if the customer is acting on behalf of another person, the FI would be in breach of section 7 if it did not identify both the customer and the person acting on his/her behalf. The Norwegian authorities further explain that the Proposal to Parliament (Proposition No. 3 (2008-2009) to the Odelsting), which is a tool for the interpretation of a law, clarifies that, even if there are no clear indications that one person is “fronting” for another person, FIs should, for control purposes, explicitly ask customers whether they are “fronting” for someone else. These provisions adequately address the deficiency.

R. 5 (Deficiency 6): 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. (MER par. 214)

30. Norway has addressed this deficiency by requiring FIs to gather information concerning the purpose and intended nature of the customer relationship when applying CDD measures (MLA s. 7). Additionally, FIs are now required to conduct ongoing monitoring of existing customer relationships and ensure that transactions are consistent with their knowledge of the customer and its activities (MLA s. 14). These provisions fully address the deficiency.

R. 5 (Deficiency 7): There is no enhanced CDD legislation for higher risk categories of customers. Nor does Norwegian legislation provide for any simplified or reduced CDD measures. (MER par. 215)

Enhanced CDD

31. Norway has responded to this deficiency by requiring financial institutions to apply “other customer due diligence measures”, in addition to the basic CDD measures stipulated in MLA, to: situations that, by their nature involve a “high risk of transactions associated with proceeds of crime” or certain designated offences listed in the Criminal Code (including terrorist financing and terrorism offences); business relationships and transactions with PEPs; and correspondent banking relationships (ss. 15-16). Although these new provisions introduce the concept of enhanced CDD into Norway’s AML/CFT regime, there is concern that their application is overly narrow, as the concept of “higher risk categories” in R. 5 is broader and could include, for example, transactions with non-residents, companies with nominee shareholders or bearer shares, or private banking. A further concern is that the scope of the “other CDD measures” to be taken in such circumstances is not defined (other than with regard to PEPs and correspondent banking, in which cases, very specific enhanced CDD measures are specified). Norway indicates that these points are to be elaborated in FSA’s guidelines⁶, but on the legal basis currently in place, the deficiency is only partially addressed.

⁶ The Norwegian authorities advise that the FSA will include the following (not exhaustive) examples of “high risk” transactions and situations in the forthcoming Guidelines to the AML/CFT legislation: transactions involving transfers to/from a customer in a country or area lacking satisfactory AML/CFT measures (particularly those with strict secrecy laws that offer high returns and tax exemptions); and foreign exchange operations and payment transfers to foreign countries. The Guidelines will also include

Simplified CDD

32. Norway has also introduced simplified CDD procedures (MLA s.13). If a customer or transaction falls into the following cases, simplified CDD will apply (MLR s. 10):

- financial undertakings listed in section 10 of the MLR;
- a financial institution in the EU and EEA area, and their correspondent FIs which are compliant with the relevant FATF Recommendations;
- an FI listed or regulated in an EEA state or an FI subject to disclosure requirements consistent with those that apply to listing on a regulated market in an EEA state;
- a Norwegian state or municipal administrative body;
- beneficial owners of accounts with funds from several persons held by lawyers or other independent legal professional from EEA member states; and
- beneficial owners of accounts with funds from several persons held by lawyers or other independent legal professionals from third states provided that they are subject to AML/CFT requirements, are subject to effective systems for monitoring, and information concerning the identity of beneficial owners is available upon request to credit institutions holding the accounts concerned.

33. FIs are required to obtain sufficient information to make sure that the circumstances are covered by these exceptions before applying simplified CDD measures (MLA s.13). However, there is some concern about how simplified CDD is applied in cases where the customer is an FI, lawyer or other legal professional in the EU/EEA area since there is no limitation to countries that are in compliance with and have effectively implemented the FATF Recommendations, as required by R. 5. Norway explains that the reason for this exception is that EU/EEA countries are legally obliged to implement the 3rd AML/CFT Directive (article 11 of Directive 2005/60/EC, in this case), and failure to implement the Directive can be sanctioned by the EU Court of Justice or the EFTA Court (for further details, see section III(B) above). Nevertheless, in this regard, the deficiency has not been removed.

34. It should be noted, however, that this issue is somewhat mitigated by the following clarification provided by the authorities. Financial institutions may only apply simplified CDD on the basis of a risk assessment (MLA s. 5). When assessing risk, FIs will have to take into consideration whether an EEA-state in fact has implemented the 3rd AML/CFT Directive and whether a country has effectively implemented the FATF Recommendations. This interpretation of the requirement is not, however, clear on the face of the legislation. The authorities indicate that the FSA will be issuing further guidance on this point in the future.⁷

the list of examples of higher risk categories from the FATF methodology (which are derived from the Basel CDD Paper) (i.e. non-resident customers; private banking; legal persons or arrangements such as trusts that are personal assets holding vehicles; and companies that have nominee shareholders or shares in bearer form.

⁷ The Norwegian authorities indicate that the FSA will include the following extract concerning simplified CDD in the forthcoming guidelines: “Risk-based customer-due-diligence related to financial institutions may comprise to what extent a country has effectively transposed EU Directive 2005/60/EC and FATF Rec. 5 (Source: www.fatf.gafi.org – “Mutual evaluation reports”). Based on information in this respect FIs should assess whether a simplified CDD would be justifiable.”

R. 5 (Deficiency 8): 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. (MER par. 220)

35. Norway has responded to this deficiency by prohibiting FIs from establishing customer relationships or carrying out transactions, when CDD cannot be applied (s. 10 MLA). FIs are also now required to terminate the customer relationship when they consider that its continuation could entail a risk of transactions associated with ML/FT (MLA s. 10). Since the MLA cannot be given retroactive effect, the obligation to terminate an existing customer relationship only applies to customer relationships established after the MLA entered into force (15 April 2009) (MLA s. 34). Only one aspect of this deficiency remains unaddressed. FIs are not obliged to consider filing an STR where they are unable to adequately complete CDD measures. The Norwegian authorities are of the view that this aspect is already covered under the general suspicious transaction reporting (STR) reporting obligation (*i.e.* to file an STR where there is a suspicion of ML/FT) and the FSA intends to issue further guidance clarifying this point. However, the general STR reporting obligation does not cover all of the situations contemplated by R.5 (*e.g.* where there is no immediate/clear indication of ML/FT, but CDD cannot be completed, and upon consideration of all the circumstances, the FI determines that it is nevertheless appropriate to file an STR). This deficiency is partially addressed.

R. 5 (Deficiency 9): 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). (MER par. 221)

36. Norway has responded to this deficiency by adding two provisions to the MLA. The first provision requires FIs to conduct ongoing monitoring of existing customer relationships, ensure that transactions are consistent with their knowledge of the customer and its activities, and update customer documentation and information (MLA s. 14). The second provision requires FIs to apply CDD whenever there is doubt as to whether the customer information they have is correct or sufficient (s. 6 MLA). Norway is of the view that these provisions fully address the concerns identified in the MER.

37. Although these provisions go quite some way to correcting this deficiency, they are still not fully in line with the concept of applying CDD to existing customers on the basis of materiality and risk at appropriate times. In particular, the timing of the obligation to update customer information is not specified; it could theoretically be applied on a regular timeframe (*e.g.* every 2-3 years), rather than at appropriate times, on the basis of materiality and risk (*e.g.* when an unusual transaction of significance takes place or there are material changes in the way that the account is operated). The authorities report that the FSA intends to issue guidance in the future which would further clarify these requirements. However, in the meantime, the obligation to update customer documentation and information is a general one, and the law is silent as to when such updating must take place. Consequently, this particular aspect of the deficiency is only partially addressed.

Recommendation 5, Overall conclusion

38. Norway has made significant progress in improving compliance with R. 5. The new MLA and MLR impose requirements that adequately address the concerns raised in the MER about: the identification of beneficial owners (using language which is consistent with the FATF standards); the need to inquire about the purpose and nature of the intended business relationship and conduct ongoing monitoring of customer relationships; identify persons acting on behalf of another; and determine whether a customer is

acting on behalf of someone else. Enhanced CDD measures have also been imposed in relation to certain high risk transactions, although there remains a concern that the scope of these provisions is too narrow. Simplified CDD measures have also been introduced and seem to be satisfactory with one exception.

39. Substantial progress has also been made to introduce measures prohibiting FIs from establishing customer relationships or carrying out transactions when CDD cannot be applied, and to consider terminating the relationship in such circumstances. However, there is no corresponding requirement to consider filing an STR in such circumstances. Provisions have been introduced to apply CDD to existing customers; however, there remains a concern that the timing of these measures is not properly focused on the basis of materiality and risk.

40. As the MLA and MLR were only recently enacted, the effectiveness of their implementation cannot be assessed and are not taken into account for the purposes of this follow-up report. Overall, Norway has addressed the major concerns that were identified in relation to R.5, and taken substantial progress in addressing the remaining deficiencies. Norway has significantly enhanced its legal framework of CDD measures to a level that is essentially equivalent to an LC.

V. Review of the measures taken in relation to the Key Recommendations

Recommendation 26 – rating PC

R. 26 (Deficiency 1): 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. (MER par. 170)

R. 26 (Deficiency 2): 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. (MER par. 152)

R. 26 (Deficiency 3): 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. (MER par. 153)

41. Norway has allocated additional resources to the FIU, with a view to enhancing its overall effectiveness. To enhance the FIU’s technical resources. Norway has introduced a new database system (called “Ask”) in 2008, which has analytical and data processing functions. Norway initiated the project to develop the MLU’s data processing system at the end of 2004, and “Ask” came into full-fledged operation at the end of September 2008. “Ask” uses software with the functions of receiving, processing, analysing, searching and sorting out data. It also contains methods for developing and displaying statistics. The system is directly linked to relevant public and police sources, and all requests and messages from other FIUs and police units are registered in it. “Ask” has made it possible for the MLU to: *i*) create an overall picture of the persons or transactions reported via STRs; *ii*) process and pass more data to the law enforcement authorities; *iii*) increase the capacity for keeping the data; and *iv*) produce statistics for analysis and sharing with foreign counterparts. “Ask” is also used to facilitate the processing of requests from Norway’s foreign counterparts. In order to maximize its analytical function, the MLU has trained all the staff focusing on the methodologies of analysis and the application of various tools. This system has facilitated the electronic filing system of STRs, and currently, over 90% of STRs are received electronically. Norway reports that the “Ask” system has reduced the time that MLU staff expend for retrieving the data into another analytical tool, and presumably it also helps the MLU staff spend more time for analysing the

data in more efficient way. This significantly improves the MLU's ability to analyse STRs (at the time of the on-site visit, STRs had to be manually selected, extracted by the MLU staff and input to another system before they could be analysed).

42. To enhance the FIU's human and budgetary resources, Norway has allocated additional budget, and increased the number of staff. The number of the MLU staff has increased from 11½ to 16 in the last four years. Among the 16 staff members, 14 are in charge of analysing the STRs and are full time analysts. All the MLU staff members have been trained to use the new "Ask" system. The numbers of STRs that have been used in intelligence reports or criminal charges in the last three years has been steadily increasing (378 STRs in 2006, 681 in 2007 and 550 in 2008) which is some indication that the level of analysis is improved. Additionally, training programs for staff have been strengthened.

43. While a paper-based desk review is limited in its ability to assess effectiveness, especially with regards to the new database system, these deficiencies appear to be substantially addressed.

R. 26 (Deficiency 4): 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. (MER par. 155, 171)

44. No legislative change has been made with regards to the role of the Control Committee; the new MLA maintains the same provisions on the Control Committee as were in the MLA 2003. While the translated English name has changed to the "Supervisory Board," the original Norwegian term is the same. At the time of the on-site visit, the Control Committee was comprised of representatives from the Norwegian Financial Services Association, the Employers Association of the Norwegian Finance Sector and the Norwegian Bar Association. The Control Committee had an authority to access all the data and information of the MLU except for the information relating to an on-going investigation. The concern expressed in the MER was that, 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 although, in practice, this does not seem to have occurred. The MLU and the Control Committee meet only two to three times a year, and Norway asserts that the Control Committee helps the MLU be on alert for data management. It is encouraging that Norway reports no interference with the MLU's daily work by the Control Committee in practice. However, although, to date, the Control Committee has not interfered with the MLU's independence, the current legislative framework retains that possibility. This aspect of the deficiency has not been addressed.

45. The MER expressed further concern that the Control Committee's intervention expended the limited resources of the MLU in considering whether old STR files should be deleted or retained, thereby undermined the MLU's overall effectiveness. However, the Norwegian authorities report that this last issue has been largely dealt with through the introduction of the "Ask" system. For its meetings with the Control Committee, the MLU submits an update of the status of STRs, but using the "Ask" system, fewer MLU resources need to be allocated to this task. This aspect of the deficiency has been adequately addressed.

R. 26 (Deficiency 5): 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. (MER par. 159)

46. During the on-site visit, the assessment team found that the MLU had not been able to properly respond to requests for assistance from foreign FIUs for a three-month period because its computer system had failed and the requests from foreign FIUs were lost. This problem has now been resolved. Norway receives and responds to requests from Egmont Group members by exchanging through the Egmont Secure Web system. All of this data and related information is fed into and processed by the new database system "Ask". The MLU has assigned three analysts and one secretary to handle the communications with the Egmont Group members. This deficiency has been adequately addressed.

R. 26 (Deficiency 6): 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 (MER par. 171)

47. When the MER was adopted, the STR information received by the MLU was to be deleted no later than five years from the time the information was recorded, unless new related information had been recorded or an investigation/legal proceeding started. While the MER acknowledged Norway's desire for the protection of privacy, it expressed concern that the lapse-of-time system could deprive the MLU of a potential source of information, and inhibited the effectiveness of the MLU's function.

48. Norway has maintained the same clause on the automatic deletion of the STR information in the new MLA. However, Norway reports that, with the introduction of the "Ask", it has revised its procedure for the deletion and retention of STR information as follows. "Ask" sorts out STR information that expired (*i.e.* more than five years old), and automatically cross-checks it with other relevant information. If the process shows any relevance to other information, it notifies the matching, the data is not deleted, and another five-year period starts from this point. Even if no relevance is shown, the data is not automatically deleted, and will be further processed manually by an analyst before he/she makes the final decision to delete or retain. Norway explains that this manual process complements the computer system, especially the areas where the computer is hard to detect, such as, similar names, and to double-check to avoid technical errors. (In fact, a similar type of manual process existed at the time of the on-site visit.) However, this is an improvement over the previous situation in which manual checks were done of the information but the MLU had only limited ability at the time to data mine information. In 2008, the MLU received 9 026 STRs and deleted 1 118 STRs. Nevertheless, the concerns remain, as expressed in the MER at paragraph 171 (*i.e.* that automatic deletion impedes the MLU's ability to detect patterns over the long term and may be counter-productive to the AML effort since an astute criminal might simply choose to launder money through transactions spaced five years apart).

Recommendation 26, Overall conclusion

49. A desk-based review of this nature has limitations in its ability to assess the FIU's effectiveness. That said, the increased level of human and technical resources, and Norway's reported experience to date is promising, and preliminary results suggest that the FIU's effectiveness has increased. The only effectiveness concern that remains is in relation to the deletion of STRs after five years in cases where no new related information has been received; however, it is difficult to assess how much this impacts the FIU's effectiveness. In terms of technical deficiencies, the only remaining issue is the role of the Control Committee and the possibility of it interfering with the FIU's independence. However, it is encouraging that, to date (and after many years of operation), no instances of actual interference in the FIU's operation have been identified. On this basis, Norway has addressed the majority of the deficiencies, and overall compliance can be assessed at a level essentially equivalent to LC.

Special Recommendation III – rating PC

SR.III (Deficiency 1): 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)). (MER par. 138)

50. The new MLA requires reporting entities (FIs and DNFBPs) to establish electronic surveillance systems for the purpose of identifying transactions that may be associated with ML/FT (MLA s. 24). Norway reports that this system is also used to implement asset freezing measures. As Norway implements S/RES/1267(1999) using administrative procedures set out in the Act of 7 June 1968, it is the FSA which is responsible for ensuring compliance with this requirement. The FSA regularly conducts thematic AML/CFT on-site inspections of reporting entities on a risk based approach. As part of this process, the FSA monitors and examines whether reporting entities have properly established and maintained such surveillance systems. Norway reports that, as part of this exercise, the FSA explicitly asks whether the 1267 list has been introduced and implemented in the electronic surveillance systems, and how many hits on the list have been detected. On the basis of the current information, it appears that this deficiency has been adequately addressed in relation to S/RES/1267(1999).

51. Freezing under S/RES/1373(2001) is implemented through the Criminal Procedure Act. As the FSA is not directly involved in criminal proceedings, it is the responsibility of the Police and/or Public Prosecution Authorities to ensure that such freezing is effectuated (e.g. through monitoring). To date, Norway has tested this procedure once (see paragraph 59 for more details). However, this case does not clarify how Norway's mechanisms for implementing SR/RES/1373(2001) could work effectively in practice in relation to reporting entities that come into possession of terrorist-related assets after the criminal proceedings and related designation process have taken place, given that neither the Police nor Public Prosecution Authorities have any general supervisory powers with respect to reporting entities. Given these practical concerns, it cannot be said that this deficiency has been adequately addressed in relation to S/RES/1373(2001).

SR. III (Deficiency 2): 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. (MER par. 129)

52. Following the adoption by the UN Security Council of S/RES/1730(2006) on 19 December 2006, Norway issued a regulation entitled "Regulations relating Sanctions against Usama Bin Laden, Al-Qaida and the Taliban," which provides for delisting procedures pursuant to S/RES/1267(1999) and its successor resolutions. Norway has fully addressed this deficiency.

SR. III (Deficiency 3): 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 be meeting their obligations concerning freezing orders issued pursuant to S/RES/1267(1999).

SR. III (Deficiency 7): 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) (MER par. 130)

53. In 2008, the FSA published "Guidelines concerning the Obligations to Freeze Assets related to Terrorism." These guidelines focus primarily on freezing actions taken pursuant to S/RES/1267(1999) (although they also make passing reference to freezing actions pursuant to S/RES/1373(2001) and other

obligations to freeze assets). In relation to S/RES/1267(1999), the guidelines: explain the purpose of asset freezing; elaborate where updated information on the designees is available; when such assets should be frozen (real-time freezing); what assets are exempted from the freezing measures; and who entities should notify in the event of a freezing. As of this follow-up report, assets equivalent to approximately USD 1 000 have been frozen pursuant to S/RES/1267(1999) (as was the case at the time of the on-site visit). The guidelines clearly define the purpose of S/RES/1267(1999), the responsibility of entities, and specific procedures of freezing and notification. Norway has adequately addressed this deficiency in relation to guidance on implementing S/RES/1267(1999).

54. In contrast, the guidance contains very little elaboration on freezing measures pursuant to S/RES/1373(2001). The guidance states that: S/RES/1373(2001) relates to freezing terrorist assets in general (not linked to al-Qaida and the Taliban); in Norway, such asset freezing does not follow from a list, but from a special decision made on a case-by-case basis, pursuant to section 202d of the Criminal Procedures Act (CPA); and the freezing obligations are implemented by chapter 15b of CPA. While this accurately refers to the applicable legal framework, no further guidance is provided concerning how, in practice, these mechanisms work in practice. For instance, the guidelines do not: explain what concrete steps entities reporting entities should take when the Police and/or Public Prosecution Authorities decide to freeze such assets; identify relevant points of contact within these authorities; or explain what specific issues may arise where a reporting entity, who was not a party to the original case initiating the freezing action, subsequently comes into possession of such assets. In these circumstances, it cannot be said that Norway has taken adequate steps to address this deficiency in relation to S/RES/1373(2001).

SR. III (Deficiency 4): It is unclear how humanitarian exemptions would apply to property frozen pursuant to S/RES/1373(2001). (MER par. 131)

55. Norway explains that the CPA has a provision that assets, which are necessary for the maintenance of the designated person, his/her household, or any person whom he/she maintains, may not be frozen (s.202d). This means that a person whose assets have been frozen pursuant to S/RES/1373(2001) may apply for the release of assets for humanitarian purposes. In such cases, the Police and/or Public Prosecution Authorities will examine the request, and if appropriate, will decide to release the freezing assets to the extent necessary for the particular purposes. This clarification addresses the deficiency.

SR. III (Deficiency 5): 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. (MER par. 133)

56. The specific concern identified in the MER was that 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 (as opposed to being used to commit a terrorist act) by a terrorist organisation or individual terrorist. This is because such activity is not criminalised (see section 2.2 of the MER). Although Norway considers the existing legislation to satisfy the requirements of S/RES/1373(2001), it has submitted a bill to clarify this issue (Governments Proposition No. 8 to Parliament). In particular, the preparatory works to the new section 135 of the Penal Code will clarify that the penal provisions are to be interpreted in a manner that is compliant with SR II. The Norwegian Parliament adopted the revision, and the revised Penal Code is expected to come into force in autumn 2009 (although this timetable may change). However, until that provision comes into force, the deficiency has not yet been addressed.

SR. III (Deficiency 6): 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. (MER par. 130)

57. In relation to S/RES/1267(1999), Norway has addressed the deficiency by providing the latest information on designations through the FSA's website, along with the guidelines (described above) which specifically explain how reporting FIs respond to the foreign lists. This enhances communication of S/RES/1267(1999) and adequately addresses this aspect of the deficiency.

58. However, it is unclear whether this mechanism could be effectively applied to freezing actions taken pursuant to S/RES/1373(2001) since those are taken through criminal procedures. For instance, it is unclear how a reporting entity, who was not a party to the original case initiating the freezing action, but subsequently comes into possession of such assets, would become aware of the freezing obligation since, ordinarily, in criminal matters, notice is only given to parties involved in the case. The Norwegian authorities explain that, in the event that terrorist assets came into the possession of someone after a freezing order is put in motion, a new case and a new freezing order would be effectuated. However, it is unclear how the authorities would even become aware that the reporting entity had come into possession of such assets (thereby triggering the need to initiate a new case), since neither the Police nor the Public Prosecution Authorities have any general supervisory authority over the financial/DNFBP sectors, and there do not seem to be adequate communication mechanisms to ensure that the reporting entities themselves (other than those who were party to the original case) have notice of S/RES/1373(2001) designations. The deficiency remains unaddressed in relation to S/RES/1373(2001).

59. Norway has also provided some relevant information concerning its implementation of S/RES/1373(2001). Norway reports that there has been one case where assets were frozen pursuant to S/RES/1373(2001) on the basis of the section 202d procedure. Approximately NOK 220 000 worth of assets belonging to a person who was a member of organisation suspected of terrorist financing were frozen by a decision taken on 3 April 2008. This case was initiated by the Police Security Service. Assets were frozen immediately and the decision was upheld by a court of first instance. However, some five months later, the freezing was lifted by the court of appeal because it could not be established that the person concerned was the owner of the assets. This case demonstrates how section 202d implements S/RES/1373(2001) in practice. However, it does not clarify how a reporting entity, who was not a party to the original case initiating the freezing action, but subsequently comes into possession of such assets, would become aware of the freezing obligation or how compliance by such an entity could be monitored (see the above discussion of deficiencies 1 and 6).

SR. III: Overall conclusion

60. Norway has made some progress in improving its implementation of SR III, particularly in relation to its implementation of S/RES/1267(1999). The key improvements in this area are improved communication mechanisms for S/RES/1267(1999) and the issuance of relevant guidelines. Norway has also clarified the application of humanitarian exemptions to freezing in relation to S/RES/1373(2001). However, a number of important deficiencies remain, particularly in relation to S/RES/1373(2001). There are still no clear communication mechanisms or comprehensive guidance on how, in practice, to implement these obligations, and the inability to freeze terrorist related assets pursuant to S/RES/1373(2001) where they are unrelated to a terrorist act remains unaddressed. Moreover, the monitoring mechanisms for both S/RES/1267(1999) and S/RES/1373(2001) are inadequate. In these circumstances, Norway has not taken sufficient action to have implemented SR III at a level essentially equivalent to C or LC.

Special Recommendation I – rating PC

SR. I (Deficiency 1): 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. (MER par. 408)

61. As noted above, Norway has substantially strengthened its CDD measures in relation to the identification of beneficial owners (see R. 5). This deficiency is fully addressed.

SR. I (Deficiency 2): 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). (MER par. 410)

62. As noted above, Norway has implemented measures for monitoring and supervising compliance with S/RES/1267(1999) (see SR III). This deficiency is adequately addressed.

SR. I (Deficiency 3): 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). (MER par. 411)

63. As noted above, concerns remain about the sufficiency of communication mechanisms, and the procedures for monitoring and supervising compliance with S/RES/1373(2001) (see SR III). This deficiency has not been addressed.

SR. I: Overall conclusion

64. Norway has made some progress in improving its implementation of SR I. In particular, Norway has fully addressed the deficiencies identified in relation to its implementation of the Terrorist Financing Convention and S/RES/1267(1999). However, the same concerns that are described above in relation to SR III apply in relation to its implementation of S/RES/1373. In these circumstances, Norway has not taken sufficient action to have implemented SR I at a level essentially equivalent to C or LC.

VI. Review of the measures taken in relation to other Recommendations rated NC or PC

Recommendation 6 – Rating NC

R. 6 (Deficiency 1): Norway has not implemented any AML/CFT measures concerning the establishment of customer relationships with politically exposed persons (PEPs). (MER par. 224)

65. The new MLA establishes measures concerning the establishment of customer relationships with PEPs. Under the MLA, the PEP is defined as a natural person: *i)* who holds or held during the last year a high public office or post in a state other than Norway; *ii)* who is an immediate family member of a person referred to in *i)*; and *iii)* who is known to be a close associate of a person referred to in *i)* (MLA s.15; MLR s.11). As for “a close associate,” the MLR further defines as a person: *i)* who is known as a beneficial owner in a legal arrangement or entity jointly with a PEP; or *ii)* who has close business connections with a PEP. The term “close business connections” is a bit vague, but the FSA intends to issue further guidance clarifying this issue. Nevertheless, this definition is substantially consistent with the FATF definition.

66. Reporting entities are required to conduct “appropriate CDD measures” to verify whether the customers are PEPs. Such measures include: *i)* obtaining approval from senior management before establishing a customer relationship; *ii)* taking appropriate measures to ascertain the origin of the customer’s assets and of capital involved in the customer relationship or the transaction; and *iii)* carrying

out enhanced ongoing monitoring of the relationship. There remains a deficiency in that there is no specific requirement for reporting entities to verify whether potential customers and beneficial owners are PEPs.

67. As the MLA and MLR were only recently enacted, the effectiveness of their implementation cannot be assessed and are not taken into account for the purposes of this follow-up report. Norway has taken sufficient action to have reached a level of compliance with R.6 that is essentially equivalent to LC.

Recommendation 7 – rating NC

R. 7 (Deficiency 1): Norway has not implemented any AML/CFT measures concerning establishment of cross-border correspondent banking relationships. (MER par. 225)

68. The new MLA introduced specific requirements in relation to correspondent banking relationships. When establishing cross-border correspondent banking relationships with institutions outside the EEA area, credit institutions are required to: *i*) gather sufficient information concerning the correspondent institution to understand fully the nature of its activities and, on the basis of publicly available information, to determine the reputation of the institution and the quality of supervision; *ii*) assess the institution's control measures for AML/CFT; *iii*) ensure that the decision maker obtains approval from senior management before establishing new correspondent relationship; *iv*) document the respective responsibilities; and *v*) ascertain that the correspondent institution conducts ongoing monitoring of customers (MLA s.16). While the language of these provisions is identical to R. 7, there remains a deficiency in that these provisions do not apply to correspondent relationships with credit institutions within the EEA countries. Norway explains that the reason for this exception is that EU/EEA countries are legally obliged to implement the 3rd AML/CFT Directive (article 11 of Directive 2005/60/EC, in this case), and failure to implement the Directive can be sanctioned by the EU Court of Justice or the EFTA Court (see section III. B of this report for further details).

69. As the MLA and MLR were only recently enacted, the effectiveness of their implementation cannot be assessed and are not taken into account for the purposes of this follow-up report. Norway has taken sufficient action to have reached a level of compliance with R. 7 that is essentially equivalent to LC.

Recommendation 12 – rating PC

R. 12 (Deficiency 1): 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). (MER par. 338)

70. Norway has fully addressed this deficiency by extending AML/CFT obligations to trust and company service providers (MLA ss. 2-3).

R. 12 (Deficiency 2): 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. (MER par. 339)

71. The CDD obligations described above in relation to R. 5 apply equally to financial institutions and DNFBP. Norway has largely addressed this deficiency.

R. 12 (Deficiency 3): Norway has not implemented any AML/CFT measures concerning Recommendations 6 that are applicable to Reporting BPs. (MER par. 343)

72. The AML/CFT obligations described above in relation to R.6 apply equally to financial institutions and DNFBP. Norway has largely addressed this deficiency.

73. As the MLA and MLR were only recently enacted, the effectiveness of their implementation cannot be assessed and are not taken into account for the purposes of this follow-up report. Norway has taken sufficient action to have reached a level of compliance with R. 12 that is essentially equivalent to LC.

Recommendation 18 – rating PC

R. 18 (Deficiency 1): There is no prohibition on financial institutions entering into or continuing correspondent banking relationships with shell banks. (MER par. 306)

74. The new MLA prohibits credit institutions from entering into or from continuing correspondent banking relationships with shell banks (s. 16). This deficiency is fully addressed.

R. 18 (Deficiency 2): 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. (MER par. 306)

75. The new MLA also obliges credit institutions to take appropriate measures to ensure that they do not engage in or continue correspondent banking relationships with credit institutions that allow their accounts to be used by shell banks. This deficiency is fully addressed.

76. As the MLA and MLR were only recently enacted, the effectiveness of their implementation cannot be assessed and are not taken into account for the purposes of this follow-up report. Norway has taken sufficient action to have reached a level of compliance with R.18 that is essentially equivalent to at least an LC.

Recommendation 25 rating PC

R. 25 (Deficiency 1): Almost every reporting entity that the assessors met with asked for more specific and tailored guidance concerning AML/CFT obligations. (MER para. 284)

77. In response to this deficiency, the FSA issued AML/CFT guidelines to auditors and external accountants in 2006. The guidelines explain the purpose of the MLA, and the CDD and STR requirements. In addition, the FIU and FSA launched a website in 2007 concerning AML/CFT, which includes relevant laws and regulations, announcements from the public sector, court decisions, typologies, trends, and relevant news from the FATF, EU, and others. However, specific guidelines have not been issued to any other category of DNFBP, and the website (although it contains information relevant to all reporting entities) is not focused on the challenges in particular sectors. This deficiency is not adequately addressed.

R. 25 (Deficiency 2): 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. (MER para. 280)

78. The Norwegian authorities also report that they have conducted outreach to FIs, during which it was emphasised that citizenship is merely one of several indicators when identifying transactions that might qualify for STRs. As well, the MLA requires reporting entities to establish electronic surveillance systems to identify transactions that may be associated with ML/FT. Norway reports that these monitoring systems have increased focus on the nature of the transactions, and enhanced the quality of STRs overall. Of the STRs filed in 2006/2007, 72% related to Norwegians and 28% (down from 70% at the time of the

on-site visit) to non-Norwegians (although it should be noted that this statistics does not include STRs related to currency exchange and money transfer, and the aggregate figures are not available). Unfortunately, a full set of data could not be obtained; however, on the basis of the information available, it appears that this aspect of the deficiency has been adequately addressed.

R. 25 (Deficiency 3): 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. (MER para. 325)

79. As noted above (see deficiency 1), AML/CFT guidance was issued to auditors and external accountants in 2006. This deficiency has been partially addressed.

R. 25 (Deficiency 4): 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.

R. 25 (Deficiency 5): 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". (MER par. 281)

80. The new database system of the MLU provides an automatic response to entities upon receipt of STRs. Norway reports that feedback is now being provided regularly through various channels (e.g. on an individual basis, through regular meetings with reporting entities and interested organizations, and through training and seminars). The MLU also publishes relevant information and trends in financial crime on its website and in its annual reports. These deficiencies have been adequately addressed.

81. Norway has taken sufficient action to have reached a level of compliance with R. 25 that is essentially equivalent to LC.

Recommendation 30 – rating PC

R.30 (Deficiency 1): 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.

82. The number of staff of the MLU has increased to 16, of which 14 staff members are responsible for the analysis of STRs. The MLU is now able to accept and process STRs electronically through its new database systems. This deficiency has been fully addressed.

R. 30 (Deficiency 2): 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.

R. 30 (Deficiency 3): 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.

83. With the introduction of the new computer system in the MLU, more STRs are being processed electronically and the FIU's analytical functions have been strengthened. These deficiencies have been fully addressed.

R. 30 (Deficiency 4): The management and resources of the MLU currently are not ring-fenced.

84. The significant additional allocation of budgetary resources affirms ØKOKRIM's current objective to strengthening the work of the MLU on a permanent basis and demonstrates that the MLU's current budgetary system is not an obstacle at this time. However, even though it is not an immediate issue, the concern remains that in future, should the ØKOKRIM's priorities change, the MLU could suffer as its management and resources are not ring-fenced. This deficiency has not been adequately addressed.

R. 30 (Deficiency 5): High staff turnover at the MLU has caused some difficulties in maintaining effective relationships with reporting entities.

85. Norway reports that the staffing of the MLU has been relatively stable over recent years and staff turnover is not more frequent than that of other units, and that this stability has a positive impact on the FIU's ability to maintain effective relationships with reporting entities. This deficiency is fully addressed.

R. 30 (Deficiency 6): Only two of the MLU's staff is trained in the use of Analysts Notebook.

86. Additional training has been provided to staff. Norway reports that all investigators/analysts at the MLU have received training in the use of Analysts Notebook, and almost all have received additional analytical training at the National Criminal Intelligence Service or at the Norwegian Police Security Service. The MLU has also introduced a training program to improve the competence of those staff who have not yet taken an operative intelligence course within one year following their appointment. This deficiency is fully addressed.

R. 30 (Deficiency 7): 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. (MER par. 162, 166, 172)

87. Concerns that the MLU's resources were inadequate overall have been addressed. The Ministry of Justice (which is responsible for the MLU's operation and budget) has significantly increased the MLU's budget (by approximately EUR 4 million) which has allowed the MLU to increase its staff and enhance its technical resources.

R. 30 (Deficiency 8): 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.

88. Norway has responded to this deficiency by including financial and economic investigation in the basic training for police officers and in several post-graduate programmes. The course runs over a period of one year, and is taken by approximately 30 persons annually. Post-graduate training and master studies programs in organized crime now include components on ML, and financial investigation and intelligence. Other relevant training is now being offered by ØKOKRIM (for investigators, prosecutors and auditors) and the Oslo Police District which is offering trainee programs in confiscation. This deficiency has been fully addressed.

R. 30 (Deficiency 9): There is concern that ØKOKRIM attracts too many of the most highly trained economic crime investigators – to the detriment of the police districts.

R. 30 (Deficiency 10): 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. (MER par. 191, 201)

89. Norway reports that, although ØKOKRIM continues to recruit some personnel from the economic crime teams, this is no longer reported to be a problem for the police districts as resource allocations to the police districts in AML have been strengthened and the Police Directorate generally has had an increasingly strong focus on economic and financial investigation over the last few years. These deficiencies have been fully addressed.

R. 30 (Deficiency 11): Considering the number of entities that the FSA is responsible for supervising, its number of staff seems inadequate. (MER par. 313)

90. The Ministry of Finance has significantly increased the FSA’s resources in order to strengthen its AML/CFT functions. The FSA now has 245 staff positions (up from 183 in 2003) – a 34% increase overall. The average number of the staff designated to on-site inspections within the banking sector has increased from 19 (in 2007) to 23. Norway reports that the FSA has been allocating its resources with a high priority on AML/CFT supervision. For instance, in 2005/2006, the FSA conducted thematic AML/CFT inspections on all MVTs providers. This deficiency is fully addressed.

91. Norway has taken sufficient action to have reached a level of compliance with R.30 that is essentially equivalent to LC.

Recommendation 32 – rating PC

R. 32 (Deficiency 1): 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. (MER par. 169)

92. Norway reports that the new database system (“Ask”) has improved communication with foreign FIUs through the Egmont Group Website system, and the MLU allocated four staff especially for this task. No serious technical failures in relation to connectivity with the Egmont Secure Web System have since been reported. This deficiency is fully addressed.

R. 32 (Deficiency 2): 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. (MER par. 200)

93. Norway provided statistics from the police districts on reported offences, prosecutorial decisions and the number of acquittals in relation to “ordinary offences” (punishable by up to three years imprisonment), aggravated offences (up to 6 years imprisonment), self-laundering, drug felony related offences (up to 21 years imprisonment) and negligent offences (up to two years imprisonment). However, the statistics do not specify the type of criminal sanctions being imposed in these cases. This deficiency has been partially addressed.

R. 32 (Deficiency 3): Norway does not maintain statistics concerning sanctions imposed for failing to comply with AML/CFT obligations. (MER par. 332)

94. Norway has provided statistics on the administrative sanctions imposed by the FSA for non-compliance with the AML/CFT obligations. In 2008, the FSA imposed 59 administrative sanctions on seven banks, 35 auditors and accountants, and 17 real estate agents. This deficiency is fully addressed.

R. 32 (Deficiency 4): 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. (MER par. 429)

95. Norway does not keep these statistics and explains that the majority of requests for mutual legal assistance are between Norway and EU countries, and are communicated directly between the competent judicial authorities. This deficiency has not been addressed.

R. 32 (Deficiency 5): 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. (MER par. 438)

96. Norway has improved the management of its extradition statistics and is now able to provide statistics beyond 2003. Norway provided the following statistics regarding extradition from/to Norway: extradition requests from Norway – 26 (2005), 24 (2006) and 25 (2007); and extradition requests to Norway – 42 (2005), 29 (2006) and 25 (2007). This deficiency is fully addressed.

R. 32 (Deficiency 6): 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. (MER par.438)

97. Norway reports that statistics regarding extradition between the Nordic countries is not centrally controlled as the competent judicial authorities communicate directly with each other. This arrangement is laid down in the Act for extradition within the Nordic countries dated 3 March 1961. Norway indicates that this system facilitates a rapid feedback without any red tape, but means that such statistics are not centrally maintained. This deficiency has not been addressed.

R. 32 (Deficiency 7): 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. (MER par. 451)

98. Norway reports that its mechanisms for keeping such statistics have been improved by the FIU's new database system, which handles these requests through the Egmont Secure Web system. Norway provided recent statistics regarding the formal requests for assistance from foreign FIUs: 34 in 2007, 65 in 2008, and 33 in 2009 (as of May). This deficiency is fully addressed.

99. Norway has taken sufficient action to have reached a level of compliance with R.32 that is essentially equivalent to LC.

Recommendation 38 – rating PC

R. 38 (Deficiency 1): 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. (MER par. 431)

100. Norway reported that it has responded to this deficiency by revising a regulation so that the *UN Convention Against Corruption* is added to the Vienna and Strasbourg Conventions. With this amendment, competent authorities are mandated to give effect to confiscation orders issued by the courts of other parties to the Convention. Although this does enhance the system, the revised regulation only relates to the *UN Convention Against Corruption* and the confiscation of property acquired through or involved in the commission of corruption. This deficiency is only partially addressed.

101. Norway has not yet taken sufficient steps to achieve a satisfactory level of compliance with R. 38.

Special Recommendation VI – rating PC

SR.VI (Deficiency 1): 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. (MER par. 334)

102. As described elsewhere in this report, the new MLA has significantly strengthened CDD requirements (R. 5) and established AML/CFT measures in relation to R. 6, 7 and SR VII that achieve a satisfactory level of compliance, although a few deficiencies remain as noted elsewhere in this report (see R. 5, 6, 7 and SR VII). Supervision of MVTS operators has been substantially strengthened in relation to the implementation of all applicable FATF Recommendations, including R. 15 and 22. Norway has implemented a licensing regime for MVTS providers, and the FSA is monitoring the sector. This deficiency is adequately addressed.

SR. VI (Deficiency 2): 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, the Recommendation 13 has not been implemented effectively in this sector. (MER par. 334-335)

103. Currently, there are three MVTS providers licensed in Norway, and all of them have submitted the STRs. The statistics provided by Norway show a significant increase in the level of STR reporting in

this sector during the last four years (512 STRs in 2005, 3 941 in 2006, 3 385 in 2007, and 6 680 in 2008), suggesting that implementation of R.13 has improved. This deficiency is adequately addressed.

SR. VI (Deficiency 3): 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. (MER par. 334-335)

104. The FSA took steps to address the issues raised with regards to the successor MVTs provider's reporting of STRs by conducting an inspection and holding meetings jointly with the FIU, FSA and the MVTs provider. Thereafter, the MVTs provider submitted STRs constantly every year. The FSA has strengthened its supervision of the sector generally, and now conducts on-site inspections of all MVTs providers. This deficiency is adequately addressed.

105. As the MLA and MLR were only recently enacted, the effectiveness of their implementation cannot be assessed and are not taken into account for the purposes of this follow-up report. Norway has taken sufficient action to have reached a level of compliance with SR VI that is essentially equivalent to LC.

Special Recommendation VII – rating NC

SR. VII (Deficiency 1): 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. (MER par. 256)

106. Norway has addressed this issue in the new MLR which provides that the “Regulation (EC) No. 1781/2006 of the European Parliament and the Council of 15 November 2006 on information on the payer accompanying transfers” is applied to Norway as regulations (MLR s. 20). Although not an EU member, Norway implements relevant EU legislation in its capacity as a participant in the EU common market and signatory of the EEA Agreement (see section III.B above). The EU Regulation applies to wire transfers sent or received by a MVTs providers established in the European Community (Article 3(1)). It requires FIs to obtain, verify and maintain full originator information (name, address and account number) on all wire transfers exceeding EUR 1 000 (Articles 3(3), 4(1) and 5(5)). The address may be substituted with the originator's date and place of birth (Article 4(2)). Where the originator does not have an account number, a unique identifier which allows the transaction to be traced back to the originator shall be substituted (Article 4(3)). Originator information must be verified on the basis of date or information obtained from a reliable and independent source (Article 5(2)). This deficiency is fully addressed.

SR. VII (Deficiency 2): 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. (MER par.255)

107. The EU Regulation requires full originator information to be included in the message or payment form that accompanies a cross-border transfer (Article 5(1)). This deficiency is fully addressed.

SR. VII (Deficiency 3): 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. (MER par. 259)

108. For domestic transfers, full originator information may be substituted by a unique identifier which allows the transaction to be traced back to the originator, provided that full originator information may be made available within three working days of receiving the request (Article 6). Wire transfers occurring within the EEA and EU countries are considered to be domestic. This is consistent with recent amendments to the Interpretative Note of SR VII. This deficiency is fully addressed.

SR. VII (Deficiency 4): 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. (MER par .260)

109. This deficiency is not relevant in relation to the current FATF standard on wire transfers, following amendments to SRVII that were adopted after Norway's MER. The current standard requires ordering FIs to include the originator's account number or unique identifier on each individual cross-border wire transfer, provided that the batch file (in which the individual transfers are batched) contains full originator information that is fully traceable within the recipient country. Article 7 of the EU Regulation meets these requirements and is, therefore, consistent with the current FATF standard.

SR.VII (Deficiency 5): 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. (MER par.260)

110. The EU requires intermediary FIs in the payment chain to maintain all of the required originator information with the accompanying wire transfer (Article 12). Where technical limitations prevent originator information from accompanying the transfer of funds, the intermediary FI must keep the records for five years. This deficiency is fully addressed.

SR. VII (Deficiency 6): 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. (MER par. 260)

111. The EU Regulation (requires beneficiary FIs to adopt risk-based procedures for identifying and handling wire transfer that are not accompanied by complete originator information which are largely consistent with SR VII (Articles 8-10). This deficiency is fully addressed.

SR. VII (Deficiency 7): There are no sanctions for breaching many of the obligations under SR VII because many of the obligations themselves have not been implemented. (MER par .260)

112. Article 15 of the EU Regulation requires Member States to set penalties applicable to infringements of the regulation, and to take all measures necessary to ensure that they are implemented. Norway reports that the FSA now supervises FIs for compliance with these requirements in accordance with the Financial Supervisory Act. Breaches may be punished through coercive measures and/or criminal sanction. Administrative sanctions for breaches of this requirement are authorised in section 27 of the MLA. These obligations only entered into force on 15 April 2009. The FSA reports that, to date, no breaches of the above requirements have been detected. This deficiency is fully addressed.

113. As section 20 of the MLR (which applies the EU Regulation) was only recently enacted, the effectiveness of its implementation cannot be assessed and is not taken into account for the purposes of this follow-up report. Norway has taken sufficient action to have reached a level of compliance with SR VII that is essentially equivalent to at least a C.

Special Recommendation VIII – rating NC

SR. VIII (Deficiency 1): 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. (MER par. 399)

114. In 2007, Norway conducted a survey of its NPO sector, and a review of the applicable laws and regulations. The results indicate that, although NPOs are not subject to a specific law or supervisory body, a number are subject to registration, and regulations regarding accounting and auditing. The survey concluded that the sector's level of vulnerability to abuse by terrorists or terrorist organizations is not considered to be alarming, and that close supervision and monitoring of the financial sector contributes to reducing the overall risk. Norway reports that, even though existing laws and regulations do specifically contain AML/CFT aspects, they are nevertheless functioning as a protection from terrorist financing or other misuse. This deficiency has been adequately addressed.

SR. VIII (Deficiency 2): 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. (MER par. 399)

115. In 2008, Norway introduced a new law that gives NPOs the option to register in the Registry of Voluntary Organisations, provided that they meet the registration criteria. NPOs that wish to receive government support will often choose to register since it is often a condition of receiving the support. Similarly, banks often require NPOs to register as a condition for opening an account. More than 10 000 NPOs have chosen to be registered. Although the implementation of the registration system is a positive step, Norway has not yet implemented the full range of measures now required by SR VIII. Norway's MER was adopted before the FATF issued the Interpretative Note to SR VIII (INSR VIII) which requires countries to implement a full range of measures including: outreach; supervision and monitoring of those NPOs which account for a significant portion of the financial resources under control of the sector and a substantial share of the sector's international activities; measures to ensure that countries can effectively investigate and gather information on NPOs; and measures to ensure that they can respond to international requests for information about NPOs of concern. This deficiency is only partially addressed.

SR. VIII (Deficiency 3): The system is further weakened by the fact that Recommendation 5 has not been implemented with regards to beneficial ownership. (MER par. 399)

116. As noted above, Norway has taken steps to strengthen its implementation of R. 5 with regards to beneficial ownership. This deficiency has been adequately addressed.

117. Norway has not yet taken sufficient steps to achieve a satisfactory level of compliance with SR VIII. It should be noted that Norway has taken action to address all three deficiencies identified in the MER – two have been addressed adequately and one partially. Nevertheless, Norway needs to continue working to reach a satisfactory level of compliance in relation to the current FATF standard on SR VIII.

Special Recommendation IX – rating PC

SR. IX (Deficiency 1): 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 be retained). (MER par. 287)

118. In 2008, Norway issued a regulation to the Customs Act that extends the declaration obligation to bearer negotiable instruments (BNI) above NOK 2 000 (EUR 2 800). Persons who breach this requirement or make a false declaration are subject to fines or imprisonment. The deficiency is fully addressed.

SR. IX (Deficiency 2): The police and Prosecution Authority (including ØKOKRIM and the MLU) can only access the Currency Transaction Register after an investigation is started. (MER par. 292)

119. Norway amended the Currency Transaction Register Act to allow the police and prosecution authority full access to the Currency Transaction Register at any time. The amendment came into effect in December 2006. The deficiency is fully addressed.

SR. IX (Deficiency 3): 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. (MER par. 296)

120. Norway reports that, when notified by foreign jurisdictions about terrorist designations, the MOFA distributes these lists to the relevant Norwegian authorities, including the Customs authorities. The Norwegian authorities also confirm that when the Police and/or Public Prosecution Authorities decide to freeze assets pursuant to S/RES/1373(2001) they inform other relevant authorities, including Customs. This deficiency has been adequately addressed.

121. Norway has also provided updated statistics showing the amounts of currency that were confiscated in the period from 2004 to 2008.

2004	2005	2006	2007	2008
NOK 10 589 227	NOK 11 752 975	NOK 11 311 177	NOK 12 279 249	NOK19 189 438

122. In relation to these deficiencies and on the basis of the information available, Norway has taken sufficient action to have reached a level of compliance with SR IX that is essentially equivalent to LC.

VII. Review of the other significant changes to the AML/CFT regime

Recommendation 9 – rating NA

R. 9 (Deficiency 1): Recommendation 9 does not apply in the Norwegian context (MER par. 236-241)

123. When the MER was adopted, R.9 did not apply in the Norwegian context because FIs and other reporting entities were prohibited from relying on third parties to perform CDD. The new MLA introduced provisions that allow reporting entities to rely on third parties to perform CDD measures, including verification of the identifies of customers and beneficial owners, and gathering of information concerning the purpose and nature of the customer relationship (s. 11). Third parties that may be relied upon are listed in the MLA and include FIs, investment firms, insurance companies, securities fund managers, accountants, lawyers, real estate agents. Third parties in other countries may be relied upon if they are subject to supervision and requirements relating to registration, CDD and recordkeeping pursuant to the MLA. However, in determining where such third parties may be based, the competent authorities are not required to take into account whether those countries adequately apply the FATF Recommendations, as is required by R. 9. Third parties are obliged to make the data on the customers available, and to forward it immediately to the reporting entity upon request. However, there is no corresponding requirement for the

reporting entity to take adequate steps to satisfy itself that the third party will be able to fulfil this requirement. Ultimate responsibility for CDD remains with the reporting entity.

FATF Secretariat

24 June 2009

ANNEX 1

PART I

MEASURES TAKEN TO ADDRESS THE DEFICIENCIES IN RELATION TO THE CORE RECOMMENDATIONS

Recommendation 5 – rating PC

Summary of factors underlying rating	Description of measures	Secretariat's comments / confirmation
<ul style="list-style-type: none"> • Although Norway has implemented customer identification obligations, it has not implemented full customer due diligence (CDD) requirements. 	1. The new anti-money laundering legislation transposes the third EU AML Directive (2005/60/EC) and FATF recommendations, and implements CDD requirements in line with Rec. 5 and Directive 2005/60/EC.	
	2. Please refer to the Introduction to the report for more information on the background for the new AML legislation.	
<ul style="list-style-type: none"> • 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. 	1. According to the MLA Section 7 Paragraph 2 reporting entities have a legal requirement to verify the identity of the person acting on behalf of a legal person. Furthermore, there is an obligation to verify that the person concerned has the right to represent the customer externally.	
	2.	
<ul style="list-style-type: none"> • 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 	1. According to MLA Section 7 Paragraph 1 No 3 reporting entities are obliged to verify the identity of beneficial owners on the basis of reasonable measures. The term “beneficial owner” is defined in the MLA Section 2 Paragraph 1 No 3. Beneficial owners are defined as “the natural persons who ultimately own or control the customer and/or on whose behalf a transaction or activity is being carried out”. In addition to this the definition in MLA Section 2 Paragraph 1 No 3 defines situations where a natural person “in all cases”	

Summary of factors underlying rating	Description of measures	Secretariat's comments / confirmation
<p>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>i.e.</i> 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).</p>	<p>shall be regarded as a beneficial owner. Examples of such situations include; a person who directly or indirectly owns or controls more than 25 per cent of the shares or voting rights in a company, exercises control over the management of a legal entity, is the beneficiary of 25 per cent or more of the assets, or has the main interest in the establishment or operation of the customer. The definition is based on the definition in Directive 2005/60/EC article 3 No 6. According to the MLA Section 8 Paragraph 5 reporting entities shall also record data unequivocally identifying beneficial owners.</p> <p>2. The Ministry of Finance has, in <u>the proposal for a new MLA Act to the Parliament (Proposal 3 (2008-2009) to the Parliament)</u>, given some guidance on the requirement to verify the identity of beneficial owners. The requirements for verification of the identity of beneficial owners should be determined on a risk sensitive basis, cf. MLA Section 5. Primarily, reporting entities should seek to verify the identity of beneficial owners when in the process of establishing a customer relationship. This can either be done by consulting public registers of legal persons or obtaining the relevant data from the customer. The reporting entity has to assess whether the information obtained is adequate. Normally, the register of shareholders or a partnership agreement will give adequate information to verify the identity of a beneficial owner.</p>	<p>Secretariat's comments / confirmation</p> <p><i>Norway explains that according to the Norwegian legal tradition, the proposal to the Parliament has an important source when interpreting the MLA (p.2). Does the proposal have a function as a guideline?</i></p> <p>All official documents produced as part of the legislative proposal will in many respects function as guidance when interpreting the law. The preparatory documents (especially the proposal to Parliament and the report from the Government appointed Legislative Committee) will be especially important as guidance when the law is new. The documents give an explanation for the proposed legislation and guidance on how the provisions should be construed. Together with any further comments by the Parliamentary Committee preparing the case for adoption by Parliament these documents give guidance to courts, to regulatory authorities, and to the general public at large on how the law is to be understood. The level of specification and detail in these preparatory documents may, of course, differ from case to case.</p>
<ul style="list-style-type: none"> • 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 	<p>1. As referred to above, according to the MLA Section 7 Paragraph 1 No 3, reporting entities are obliged to verify the identity of beneficial owners on the basis of reasonable measures. In addition, if a person other than the customer have a right of disposal over an account or deposit, or is carrying</p>	<p><i>The new MLA has measures to identify beneficial owners, but how is the compliance with this provision monitored and ensured? In order to</i></p>

Summary of factors underlying rating	Description of measures	Secretariat's comments / confirmation
<p>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).</p>	<p>out a transaction on behalf of the customer, the identity of the persons concerned shall be verified on the basis of valid proof of identity, cf. MLA Section 7 Paragraph 3.</p>	<p>assess the effectiveness, it would be helpful if a supplementary description on the supervision is provided.</p> <p>The MLA and the associated Regulations entered into force on April 15 2009. The FSA is at present working on detailed guidelines to the Act and the Regulations, including the obligation to identify beneficial owners. The deadline for this work is second quarter 2009. The Guidelines will be issued in close cooperation with relevant industry organisations and will include the following topics:</p> <ul style="list-style-type: none"> • Explanation of the term “beneficial owner”, in particular in relation to corporate entities. • The requirement of identifying and verifying the identity of beneficial owners, as part of the customer due diligence, will be emphasised • Advice on how to obtain the required information • Comments are also made on certain practical issues, i.a. private banking, pooled accounts etc. • Recommendations as to what information should be registered about a beneficial owner. • Explanations related to the legal requirement “to inquire about the purpose and nature of the business relationship” for different customer/client categories. <p>How reporting entities are complying with the new rules and how they apply the Guidelines will be supervised through the regular surveillance and monitoring work</p>
	<p>2. The Ministry of Finance has, in the proposal for a new MLA Act (Proposal 3 (2008-2009) to the Parliament), given some guidance on the requirement to verify the identity of persons carrying out a transaction on behalf of a customer. It is recognised that it might be difficult to assess whether one customer is “fronting” for another person unless there are clear indications that this is the case. If such indications do not exist, reporting entities should, for control purposes, ask the customer whether he/she is “fronting” for someone else.</p>	

Summary of factors underlying rating	Description of measures	Secretariat's comments / confirmation
		conducted by the FSA. Supervisory resources are allocated on a risk sensitive basis.
<ul style="list-style-type: none"> 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. 	<p>1. As referred to above, according to MLA Section 7 Paragraph 1 No 3, reporting entities are obliged to verify the identity of beneficial owners on the basis of reasonable measures. The term "beneficial owner" is defined in the MLA Section 2 Paragraph 1 No 3, cf. above. The MLR Section 7 defines what is regarded as valid identity for legal persons. In cases where the customer is a legal person registered in a public register, a transcript from the relevant register will be valid proof of identity. Based on this information, information concerning the ownership and control can be obtained.</p> <p>2. As expressed in the Summary of Norway's 3rd MER Paragraph 28 and 29, Norway has several registries for legal persons. <u>All Norwegian legal persons, and Norwegian and foreign companies or other legal persons conducting business activities in Norway are obliged to register in one or more registers.</u> Registered information concerning a particular legal person can be retrieved through Norway's single number identification system. Additionally, Norway obliges 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 available to anyone who asks. These measures ensure that accurate, adequate and reasonably current information concerning the ownership and control of Norwegian legal persons is readily accessible.</p>	<p><i>The Section 7 of the MLR provides three cases of valid proof, and it includes a legal person not registered in a public register. In what case is a legal person not registered?</i></p> <p>Norway has a large number of registers. Examples relevant here include:</p> <ul style="list-style-type: none"> The Central Coordinating Register for Legal Entities which registers basic data about legal entities to coordinate information on business and industry that resides in various public registers: <ul style="list-style-type: none"> The Register of Business Enterprises which contains all Norwegian and foreign business enterprises in Norway. The Register of Employers – employers are obliged to contribute to the national social security system The Foundation Register The Register of Businesses and undertakings

Summary of factors underlying rating	Description of measures	Secretariat's comments / confirmation
		<p>established for statistical purposes</p> <ul style="list-style-type: none"> ○ The Business Tax Register ○ The VAT Register ○ The Bankruptcy register. <p>All these registers are attached to the Central Coordinating Register. If an entity is registered in one or more of the underlying registers it will automatically be registered in the Central Coordinating Register.</p> <p>In addition:</p> <ul style="list-style-type: none"> • The Register of Company Accounts collects annual accounts, including the auditor's report, from all private and public limited companies, savings banks, mutual insurance companies and petroleum enterprises. • The Voluntary Registry was created after an initiative from non-governmental organizations and NPOs. The register has improved and simplified the interaction between NGOs/NPOs and public authorities. Reference is also made to the response to SR VIII. <p>In all cases where an entity conducts business in Norway they are obliged to register in one or more registers. When an entity does not conduct any business, registration may be voluntary. In practice however, many entities choose to</p>

Summary of factors underlying rating	Description of measures	Secretariat's comments / confirmation
		<p>register.</p> <p>In the end there are of course entities, mostly NPOs, that are not registered, but if a legal person not registered anywhere wants to open a bank account, the normal CDD procedures apply.</p>
<ul style="list-style-type: none"> • 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. 	<ol style="list-style-type: none"> 1. According to the MLA Section 7 Paragraph 1 No 4, CDD shall include gathering information concerning the purpose and intended nature of the customer relationship. 2. The reporting entities are obliged to conduct ongoing monitoring of existing customer relationships, and ensure that transactions they become aware of are consistent with their knowledge of the customer and its activities, cf. MLA Section 14. Furthermore, reporting entities shall apply customer due diligence measures when in doubt as to whether previously obtained data concerning the customer are correct or sufficient, cf. MLA Section 6 Paragraph 1 No 4. In both cases, this includes conducting ongoing due diligence with regard to information about the purpose and nature of the business relationship. 	<p><i>In order to assess the effectiveness, it would be helpful if a supplementary description on the supervision is provided.</i></p> <p>As described above the MLA and associated Regulations entered into force on April 15 2009. Kredittilsynet will also issue guidelines concerning ongoing due-diligence. The reporting entities will be supervised pursuant to the legislation and these guidelines. Supervisory resources are allocated on a risk sensitive basis.</p>
<ul style="list-style-type: none"> • There is no enhanced CDD legislation for higher risk categories of customers. Nor does Norwegian legislation provide for any simplified or reduced CDD measures. 	<ol style="list-style-type: none"> 1. In situations that by their nature involve a high risk of ML or TF, reporting entities shall apply enhanced CDD, cf. MLA Section 15 Paragraph 1. The reporting entities are obliged to apply other CDD measures in addition to the measures applied in normal risk situations. This obligation implements directive 2005/60/EC article 13. 2. According to Section 13 of the MLA the Ministry of Finance may, in regulations, provide exceptions from the standard obligation to apply CDD measures as laid down in the MLA Section 6. Such exceptions (simplified CDD) are provided in the MLR Section 10 which is based on Directive 2005/60/EC article 11. Reporting entities shall, before applying simplified CDD, obtain sufficient information to establish that the circumstances are covered by the exception concerned. 	

Summary of factors underlying rating	Description of measures	Secretariat's comments / confirmation
<ul style="list-style-type: none"> 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. 	<p>1. According to the MLA Section 10, if CDD measures, including verification of the identity of beneficial owners and information concerning the purpose and intended nature of the customer relationship, cannot be applied, entities with a reporting obligation shall not establish a customer relationship or carry out the transaction. If the attempted transaction is regarded as suspicious, the reporting entity will have to consider making an STR, cf. MLA Section 17 and 18.</p>	
	<p>2. If CDD measures cannot be applied, an established customer relationship shall be terminated if continuation of the relationship entail a risk of ML or TF, cf. MLA Section 10. The obligation to terminate customer relationships pursuant to this Section only applies to customer relationship established after the MLA entered into force (15 April 2009), cf. MLA Section 34 Paragraph 2. An obligation to terminate customer relationships that were established before the MLA 2009 entered into force would give the MLA retroactive effect. However, if CDD measures cannot be applied, this has to be taken into consideration when assessing risk and applying ongoing monitoring, cf. MLA Section 5 and Section 14.</p>	
<ul style="list-style-type: none"> 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). 	<p>1. The MLA section 14 introduces an obligation to monitor existing customer relationship and ensure that transactions they become aware of are consistent with their knowledge of the customer and its activities (ongoing CDD).</p>	
	<p>2. If a reporting entity is in doubt as to whether previously obtained data concerning the customer are correct or sufficient (e.g. because of an enlargement of the customer relationship) the reporting entity is obliged to apply CDD measures, cf. MLA Section 6 Paragraph 1 No 4.</p>	
<ul style="list-style-type: none"> 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. 	<p>1. The requirements regarding "customer due diligence" apply to all entities with a reporting obligation, including financial institutions and non-bank institutions. Reference is made to the MLA section 4.</p>	
	<p>2. Section 2 of the MLR is tailored to non-bank sectors and takes into account the normal conduct of business for these entities. The section regulates when a customer relationship shall be deemed to be established. Section 3 and 4 of the MLR include tailored provisions concerning when CDD measures shall be applied by "dealers in objects" and "lawyers and other</p>	

Summary of factors underlying rating	Description of measures	Secretariat's comments / confirmation
	<p>persons who provide independent legal assistance on a professional or regular basis”, respectively. In June 2006 the FSA (Kredittilsynet) issued specific and tailored AML/CFT guidelines to auditors and external accountants in close cooperation with relevant industry organisations and the FIU. Reference is made to Circular 13/2006, see enclosure. Cf. also response to Rec. 25 below.</p>	

PART II

MEASURES TAKEN TO ADDRESS THE DEFICIENCIES IN RELATION TO THE KEY RECOMMENDATIONS

Recommendation 26 – rating PC

Summary of factors underlying rating	Description of measures	Secretariat's comments / confirmation
<ul style="list-style-type: none"> • 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. 	<p>1. As mentioned in the Introduction to this report, great efforts have been made since Norway's MER in 2005 to improve the effectiveness of the MLU. This includes increased resources, both increased staff and a new system for receiving, processing/analysing and publishing intelligence data and information on criminal cases on the basis of received STRs.</p> <p>The ELMO project (a pilot study) was initiated by the Money Laundering Unit (MLU) at the end of 2004. ELMO was designed to handle large quantities of suspicious transaction reports (STRs) and other trustworthy information in a considerably more efficient manner than previously possible. The project was based on the legal framework of the Money Laundering Act, legislative guidelines, the recommendations of the FATF, the practices of other organizations and the MLU's own requirements with regard to its work. Specifications for the project were submitted to the Police Directorate in October 2005.</p> <p>In June 2008, the ELMO project delivered a finished IT solution to the Financial Intelligence Unit (FIU) for testing. The name of the solution is "Ask" [English: Ash]. <i>(In Norse mythology, Yggdrasil, the World Tree, was an ash tree. The tree spread its branches over the whole world, and had its roots in Mimir's Well, the well of wisdom.)</i></p> <p>"Ask" was put into full production at the end of September 2008. "Ask" is an advanced, high-technology system for receiving, processing/analysing and publishing intelligence data and information on criminal cases on the basis of received STRs. The total costs of the system has over the last two years been more than EUR 4 million, and has in addition demanded considerable resources from the FIU in connection with design, development and testing.</p>	

Summary of factors underlying rating	Description of measures	Secretariat's comments / confirmation
	<p>The overall aim of "Ask" is to enable the FIU and the Norwegian police to increase their efficiency and effectiveness in using financial intelligence data, mainly received from reporting businesses, professions and industry, in day-to-day intelligence and investigation work. The new technological solution has significantly improved the quality and the effectiveness of the FIU:</p> <ul style="list-style-type: none"> • The FIU is becoming increasingly more efficient in receiving data and in processing and converting received data and other available data directly into the police's systems for intelligence and processing of criminal cases. • An increasing number of criminal cases are passed on to the police and control authorities. • The capacity for keeping statistics and conducting assessments of threats, trends and means of money laundering is, and will continue to be improved. • The FIU will be able to work more proactively, since criminal activity will be discovered earlier. • It will be possible to increase recovery of the proceeds of crime and to improve the assessment of defrauded tax, VAT and contributions to the national insurance. <p>At its most intensive stage, the project engaged 20 developers simultaneously from the Police data and material service. We believe that "Ask" is a rather sophisticated system.</p> <p>Over 90% of all STRs are currently received electronically from the reporting entities. In addition to electronic transaction monitoring systems, large reporting entities have their own systems for direct transfer of STRs to the FIU. Other entities send in reports using a web form available at www.altinn.no. (Altinn is an Internet-based reporting channel enabling business enterprises and private individuals to submit information to Norwegian public agencies). These measures result in freeing up of resources to support the reporting entities, and for analysis. <u>The FIU has sufficient staff to receive and process data.</u></p>	
	<p>2. "Ask" is a tool supporting the analysis that underlies work at the FIU, like partial automation for receipt and gathering of data, evaluation/validation, processing and integration of data. In addition, various methods are used by "Ask" for processing and interpretation of data, for testing of hypotheses and for proceeding in the analysis of cases. Examples are advanced searches in "Ask" itself and across sources, visualisation (networks,</p>	

Summary of factors underlying rating	Description of measures	Secretariat's comments / confirmation
	<p>timelines, geographical information systems (GIS)), evaluation of sources and data, control of links between reported persons, etc.</p> <p>“Ask” is directly linked to most relevant data sources, both public sources and the police’s own sources. In addition, all requests and messages from other FIUs, police units, etc. are registered in “Ask” to ensure a complete record of these requests/messages, and to be able to integrate these data with other data. On the basis of the information contained in received STRs, searches are made in all associated data sources in order to enrich the initial information. This makes it possible to create an overall picture of the persons/transactions reported via STRs. These searches are made continuously on the basis of pre-defined rules. “Ask” makes use of an advanced rule engine for automatic network building based on data from STRs, public sources and police sources. The same rule engine is used to compute the relevance of both personal and organisational information, and to establish “risk-scoring”/“relevance-scoring” related to persons registered in “Ask” on the basis of rules created by the staff of the FIU. The relevance/“risk-scoring” may be based on rule matches in “Ask” itself or across databases.</p> <p>“Ask” also contains advanced methods for developing and displaying statistics. In the new solution, these statistics are based on a new, better and larger data model than the one used in the previous solution and this will, over time, provide a far higher quality of statistics. This particularly applies to the receipt and transmission of data to foreign counterparts, since registration routines and metadata are of far higher quality than previously.</p>	
<ul style="list-style-type: none"> • 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. 	<p>With the help of the new technical solution (“Ask”), the staff of the FIU will be able to publish data directly to the national intelligence data solution for the police. The data can be published as searchable objects/items, either for automatic rule-based searches or for manual searches as events on the basis of analyses. All the information contained and sorted by “Ask” is now the basis for applying analytical tools, please also see description of the “Ask” system above. Improved handling of data concerning financing of terrorism has also been implemented in “Ask”. Examples are tagging of STRs by the reporting entities, automatic sorting of objects related to TF and automatic indexing and monitoring of the UN 1267 list. Integration/automatic monitoring of other lists is technically possible.</p> <p>2. The IT system “Ask” cannot function without organisational support processes. The FIU has therefore has functions for rule monitoring and maintenance, classification of cases, entity analysis and system maintenance. All employees are also trained in methodology of analysis</p>	

Summary of factors underlying rating	Description of measures	Secretariat's comments / confirmation
	<p>and in the application of various tools. Please also refer to description of the "Ask" system above.</p> <p>The FIU has requested the supplier and developer of the "Ask" system to provide resources for further development and operation of the system. The FIU has also envisaged further developments in cooperation with the supplier. Among other features, the FIU would like to see the implementation of self-educating technology and neural networks.</p>	
<ul style="list-style-type: none"> 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. 	<p>1. <u>Since 2005, ØKOKRIM has been assigned 11 new staff members</u> to work on money laundering related intelligence reports and cases (MLU and a new investigative team). This budgetary increase related to personnel is supported by necessary funding for developing a sophisticated system for the receiving and analysis of STRs ("Ask"), cf. above.</p> <p>2. As described above the new system "Ask" will greatly improve the effectiveness of the MLU's work. "Ask" will enable the staff at the MLU to focus more on analysis of cases.</p>	<p><i>The MER (para.162) says that the MLU has 11½ employees as of January 2005, and only 7 of which directly are involved in analysing STRs. As of today, how many staff members are working in the MLU, and how many of them are dealing with STRs?</i></p> <p>In the 2006 budget Økokrim was allocated additional funds for bolstering its efforts to combat money laundering. These funds were used in part to strengthen the MLU but also to establish a new team- the Stolen Goods and Money Laundering Team- which was especially mandated to investigate and bring to trial cases originating from STRs. As of today the Stolen Goods and Money Laundering Team consists of 7 staff members. The total number of employees at the MLU is 16. 14 of these are dealing directly with the STR's as analysts. Only the head of the MLU and one person designated to tasks concerning strategic analysis is not dealing directly with STRs.</p>

Summary of factors underlying rating	Description of measures	Secretariat's comments / confirmation
<ul style="list-style-type: none"> 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. 	<ol style="list-style-type: none"> <u>The MLU has not experienced that the Control Committee is interfering in its daily work. The MLU and the Control Committee meet 2-3 times a year.</u> As regards the deletion of old STR files, the "Ask" system facilitates for efficient routines and the resources allocated to deletion of old STRs is now very limited. "Ask" takes into account the statutory provisions (cf. MLA Section 29) concerning deletion of data on the basis of knowledge and automation. On the basis of rules, "Ask" automatically withdraws data that for one or more reasons is not relevant (according to the law). The indicated data is quality controlled, and is then deleted manually in order to ensure that no relevant data is deleted. 	<p>1. Is the "Supervisory Committee" is the correct name under the new MLA?</p> <p>The official name in Norwegian is "Kontrollutvalget for tiltak mot hvitvasking" or in short "Kontrollutvalget". This is the same as under the MLA 2003. The unofficial English translation of the name has unfortunately not been consistent. In the translated version of the new MLA the name is translated to the "Supervisory Board for Measures to Combat Money Laundering" (the Supervisory Board).</p> <p>2. The MER's concern was: i) the MLU is subject to oversight of the Control Committee, and ii) therefore, it could intervene the MLU's activities, which undermines its independence. Given that no actual interference is occurred, what are the role / responsibility of the Control Committee? What is the purpose of the meeting?</p> <p>The Supervisory Board's main responsibility is to ensure that rule of law and personal privacy issues are considered when the MLU handles information.</p> <p>In meetings with the MLU the Supervisory Board receives an update on the status of STRs in the money laundering database and receives information about other matters related to the MLU's ongoing operation. The Supervisory Board is also mandated to investigate complaints from individuals or organisations regarding the treatment of information sent to the MLU.</p> <p>The oversight from the Supervisory Board will naturally require some resources from the MLU, but this is very limited due to the new system, "Ask", which facilitates easier withdrawal of information on STRs.</p>

Summary of factors underlying rating	Description of measures	Secretariat's comments / confirmation															
		<p>Consequently, the MLU does not experience that the Supervisory Board interfere with their daily work. The existence of the Supervisory Board and its powers implies first and foremost that the MLU has to be alert and careful in its handling of data such that data protection rules are abided by and that any allegations to the contrary easily can be rejected.</p>															
<ul style="list-style-type: none"> 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. 	<ol style="list-style-type: none"> The MLU regards itself to be complying with the Egmont Group Statement of Purpose and Principles for Information Exchange. The MLU is not dependent on an MOU to exchange information. However the MLU has recently signed a number of MOUs (based on the Egmont Model MOU) with a number of jurisdictions. In addition to this, a number of MOUs are currently being negotiated. 	<p><i>The MER identified this deficiency based on an actual case that information exchange with foreign FIUs was not properly handled (para.159). A supplementary description is needed to explain how the MLU has addressed to prevent such case.</i></p> <p>The request from Egmont Group members and the answers to these are exchanged through the Egmont Secure Web system. All requests are also logged, filed and handled in the "Ask" system. The incident that took place in 2004 was due to a technical error of a limited impact and does not longer represent a problem. It should be underlined that this incident occurred before the introduction of the totally new, and much more sophisticated "Ask" system, which is now operational. Three analysts and one secretary are assigned with a special responsibility for the requests.</p>															
<ul style="list-style-type: none"> 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. 	<ol style="list-style-type: none"> STRs are not deleted if new information has been recorded or investigations or legal proceedings have been instituted against the registered person during the five year period the law sets out, cf. MLA Section 29 Paragraph 1. <u>Whether a STR should be deleted or not is considered based on the comprehensive amount of information contained in "Ask". This greatly limits the risk of deleting an STR that could have been a potential source of information. The deletion procedures are significantly more efficient with the new system "Ask" in place.</u> Please also refer to answer above concerning the Control Committee. 	<p><i>1. Please provide the update (2005-) of the table on para. 154 of the MER.</i></p> <table border="1" data-bbox="1532 1185 2011 1375"> <thead> <tr> <th colspan="5">Processing of STRs</th> </tr> <tr> <th></th> <th>2005</th> <th>2006</th> <th>2007</th> <th>2008</th> </tr> </thead> <tbody> <tr> <td>Numer of reports received</td> <td>4893</td> <td>7042</td> <td>7543</td> <td>9026</td> </tr> </tbody> </table>	Processing of STRs						2005	2006	2007	2008	Numer of reports received	4893	7042	7543	9026
Processing of STRs																	
	2005	2006	2007	2008													
Numer of reports received	4893	7042	7543	9026													

Summary of factors underlying rating	Description of measures	Secretariat's comments / confirmation				
		Number of deleted reports (Both Cases deleted – suspicion proven to be unfounded and deleted according to law)	38	20	30	1118
		Intelligence reports		254	334	243
		Criminal charges		44	52	27
		Number of STRs used in intelligence reports/ criminal charges		378	681	550
		<p>2. Is there any guidance which supports this description?</p> <p>The rules concerning deleting of information from STR's are the same now as they were in 2005. The practice has however changed with the introduction of "Ask". "Ask" ensures that <u>all</u> the information that is known to the MLU is thoroughly checked before a STR is deleted. This checking is done automatically and consists of a search/scanning of all the information in possession of the MLU. If this</p>				

Summary of factors underlying rating	Description of measures	Secretariat's comments / confirmation
		process shows that there is new information which has relevance to the STR, the STR will not be deleted. The STR's which have no new information of relevance, will be listed out in "Ask" and will be processed manually by an analyst before the final decision to delete or not to delete is made. This extra check is done to avoid that deletion by default eliminates information that should not be eliminated. The MLU has established internal practices for how this work should be carried out.
	2. The right for protection of individuals with regard to the processing of personal data has to be weighed against the aim of combating ML/TF. Based on this the MLA Section 29 decides that if no new information is obtain or no criminal proceedings have been instituted after five years from receipt of the STR, or it is found that no criminal act has been committed, the STR should be deleted. The deletion procedure will greatly limit the risk of losing valuable information.	

Special Recommendation I – rating PC

Summary of factors underlying rating	Description of measures	Secretariat's comments / confirmation
<p>• 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.</p>	<p>1. The new anti-money laundering legislation transposes the third EU AML Directive (2005/60/EC) and FATF recommendations. The transposition includes "Customer due diligence" measures in line with Rec. 5 and Directive 2005/60/EC. This includes a requirement to identify customers in whose interest accounts are opened. Cf. also response to Rec. 5</p> <p>2. The MLA comprises a duty to apply customer due diligence measures and to verify the identity of beneficial owners on the basis of appropriate measures. Cf. also response to Rec. 5</p>	
<p>• Implementation of S/RES/1267(1999): Although</p>	<p>1. Norwegian financial institutions are <u>obliged to establish electronic surveillance systems</u> (the obligation was introduced by the end of 2004) for the purpose of identifying transactions that may be associated with</p>	<p><i>In order to assess the effectiveness, please provide a supplementary description on how the competent authorities monitor the</i></p>

Summary of factors underlying rating	Description of measures	Secretariat's comments / confirmation
<p>Norway has implemented measures that penalise breaches of freezing orders issued pursuant to S/RES/1267(1999), <u>it does not monitor or supervise for compliance with this requirement</u> (as required by section 8 of the resolution).</p>	<p>proceeds of crime or offences subject to section 147a, 147b or 147c of the Penal code (these sections prohibit and penalize terrorism and terrorist financing). Reference is made to section 24 of the MLA and section 18 of the MLR. These monitoring systems are tailored pursuant to Norwegian legislation, including a module that comprises freezing obligations pursuant to UN Resolutions. During AML/CFT on-site inspections these systems are examined, including the surveillance and follow-up of freezing obligations.</p>	<p><i>compliance with this obligation and on the function of the system in individual FIs.</i></p> <p>First of all, it is straightforward to verify that the legal obligation to establish electronic surveillance systems as such is complied with. Secondly, the functioning of electronic surveillance systems have been examined during on-site inspections and on the basis of off-site reviews.</p> <p>Two examples of such supervisory measures:</p> <ul style="list-style-type: none"> • 2007 - a thematic AML/CFT on-site inspection was carried out at DnB NOR Bank (market share of the Norwegian banking market 39%, market share of the total Norwegian financial market 33%). The inspection comprised i.a. the bank's electronic surveillance system. • An off-site review of the electronic monitoring systems at all finance companies (30 companies) was carried out in 2008. <p>These supervisory measures comprised the electronic monitoring systems of both major suppliers of such systems to Norwegian financial institutions (EDB Business Partner and SAS Institute).</p>
<p>• 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</p>	<p>2.</p> <p>1. Actions taken under S/RES/1267 (1999) and <u>1373 (2001) are published on the FSA's (Kredittilsynet) website</u> under "Lister fra FN, FATF samt lignende kunngjøringer" (Lists from UN, FATF and similar announcements). The consolidated list from the UN's Sanctions Committee (1267) is included as a hyperlink in the web edition of the text of the Regulation on sanctions against Usama Bin Laden, Al-Qaida and the Taliban of 22 December 1999 No. 1374 on "Lovdata" (www.lovdata.no - http://websir.lovdata.no/cgi-lex/wiftzok?bas=sf+stv+del+ins+bv+fv+nb+jb+sj+mv+pv+ov&emne1=usama&button=S%F8k&sok=fast) and the Norwegian regulations will consequently always be updated. ("Lovdata" is a web registry containing all</p>	

Summary of factors underlying rating	Description of measures	Secretariat's comments / confirmation
pursuant to S/RES/1373(2001).	<p>Norwegian legislation. The database is continuously updated). Cf. also response to implementation of S/RES/1267(1999) above.</p> <p>2. S/RES/1373 is implemented through The Criminal Procedure Act section 202d and 202e. These provisions mandate the freezing of funds in cases where it is just cause to suspect that an act of terrorism financing has been committed. Reporting entities are obliged to file STRs if there are transactions that give rise to suspicions that a link to terrorism or financing of terrorism exists, cf. MLA section 18. The threshold for reporting – as regards the level of suspicion – is low. Supervision for compliance with reporting obligations under the Money Laundering Act is carried out by the FSA (Kredittilsynet).</p> <p>The MLU has formalized cooperation with the Police Security Service. Two meetings are taking place on a regular and frequent basis to mutually inform each other, discuss and clarify relevant issues.</p>	<p>1) In case a person is designated under the S/RES/1737, how are the FIs informed about the information of the designee – by a notification from police/prosecutor and/or the FSA's website?</p> <p>The relevant information will be published right away on the webpage of the FSA and the financial industry associations will be informed immediately.</p> <p>2) In order to assess the effectiveness, please provide a supplementary description on how the competent authorities (please identify which authorities are in charge) monitor the compliance with this obligation and on the function of the system in individual FIs.</p> <p>Reference is made to the reply above. As a part of it's regular surveillance of the FIs, the FSA monitors how freezing of funds actually and practically are carried out by the FIs.</p>

Special Recommendation III – rating PC

Summary of factors underlying rating	Description of measures	Secretariat's comments / confirmation
<ul style="list-style-type: none"> 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)). 	<p>1. Decisions to freeze based on Section 202d of the Criminal Procedure Act are subject to prosecutorial control as well as control by the courts. Cf. also response under SR I above bullet point 1 and 2.</p> <p>1. The decision to freeze assets pursuant to the Norwegian Regulation on sanctions against Usama Bin Laden, Al-Qaida and the Taliban of 22 December 1999 No. 1374, implementing S/RES/1267(1999) may be appealed, by a party or another person having a legal interest in appealing the case, <u>to the immediate superior of the administrative agency that made the decision. The final decision may eventually be challenged within the Norwegian courts.</u></p>	<p><i>Please describe how the appeal is to be handled under the Norwegian legal system (other than notifying to the UNSC). (It is assumed that a procedure in accordance with an act on administrative appeal / litigation is in place.)</i></p> <p>Administrative appeals against freezing decisions are governed by the Act of 10 February 1967 relating to procedure in cases concerning the public administration. Enclosed you will find an English translation of Chapter VI of the Act.</p> <p>According to Section 32 letter a, an appeal against an administrative decision shall be lodged with the administrative agency that made the decision. This agency shall carry out such investigations as are warranted by the appeal. It may rescind or alter the decision if it considers the appeal justified, cf. Section 33 second paragraph. Should no such decision be made, the documents in the case shall be sent to the appellate instance as soon as the case has been properly prepared, cf. section 33 fourth paragraph. The appellate instance may try all aspects of the case and thereunder take new circumstances into account. It shall consider the views presented by the appellant, and may also take into consideration matters not addressed by him, cf. Section 34 second paragraph. The appellate instance may itself make a new administrative decision in the case or rescind the previous administrative decision and return the case to the subordinate instance for a new hearing of the whole or part of it, cf. Section 34</p>

Summary of factors underlying rating	Description of measures	Secretariat's comments / confirmation
		fourth paragraph. The appellate instance's final decision may be challenged within the Norwegian courts. Legal proceedings are governed by the Dispute Act of 17 June 2005.
<ul style="list-style-type: none"> 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 	<p>2. Further to that, the Regulation implementing S/RES/1267(1999) has been amended and the provisions on freezing of assets now informs listed entities/persons about the possibility to request de-listing through the focal point established by S/RES/1730/2006. The regulation also outlines the de-listing procedures.</p> <p>1. In 2008 the FSA published "Guidelines concerning the obligations to freeze assets related to terrorism" on its website (www.kredittilsynet.no) and on the website www.hvitvasking.no. Guidelines are enclosed. (See also response to Rec. 25 Supervisory authorities).</p>	
<ul style="list-style-type: none"> 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). 	<p>2. These guidelines comprise the freezing obligations pursuant to S/RES/1267 (1999) and S/RES 1373 (2001).</p> <p>1. S/RES/1373(2001) is implemented in Norwegian law through the Criminal Procedure Act section 202d. Section 202d, second paragraph decides that: "Assets that are necessary for the maintenance of the person to whom the decision is directed, his household or any person whom he maintains, may not be frozen."</p>	
<ul style="list-style-type: none"> It is unclear how humanitarian exemptions would apply to property frozen pursuant to S/RES/1373(2001). 	<p>1. The Parliament has adopted a new Penal Code terrorist financing provision. The new provision is not in force. The deliberations in the preparatory works conclude that the present provision (penal code section 147 b) is in full compliance with FATF-standards. Although not deemed to be strictly necessary, a significant reason for amending the provision is to clarify that Norway meets the international standards in this area. (An English translation of the relevant part of the Proposition to the Parliament expressing compliance with the FATF-standards, is enclosed, Proposition No. 8 (2007-2008) to the Odelsting (Parliament)). The new provision is planned to come into force in the autumn of 2009 as part of a major overhaul of the entire part II (Felonies) of the Penal code.</p>	

Summary of factors underlying rating	Description of measures	Secretariat's comments / confirmation
<ul style="list-style-type: none"> 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. 	<p>2. The new penal provision against the financing of terrorism in the Penal Code of 2005 (which is planned to come into force <u>in the autumn of 2009</u>) is worded as follows:</p> <p><i>“Section 135 The financing of terrorism</i></p> <p><i>Any person who unlawfully provides, receives, sends, obtains or collects money or other assets with the intention or knowledge that these resources shall wholly or partly be used</i></p> <p><i>a) to perform an act as referred to in section 131, section 134 or sections 137 to 144,</i></p> <p><i>b) by a person or group that intends to commit acts as referred to in section 131, section 134 or sections 137 to 144 when such a person or group has taken steps to realise the purpose by illegal means,</i></p> <p><i>c) by an undertaking owned or controlled by a person as referred to in (b) or</i></p> <p><i>d) by an undertaking or a person who acts on behalf of or on the instructions of a person as referred to in (b).</i></p> <p><i>shall be liable to imprisonment for a term not exceeding 10 years.</i></p> <p><i>The same penalty shall be imposed on any person who makes bank services or other financial services available to persons or undertakings as referred to in the first paragraph (b), (c) or (d).”</i></p> <p>Section 135 is placed in chapter 18 of the Penal Code of 2005 – “Acts of Terrorism and terror related acts”. The other provisions in this chapter covers <i>i.e.</i> acts of:</p> <ul style="list-style-type: none"> Hijacking of ships, platforms or aircraft. Disturbance of the secure operation of means of transport, etc. Discharge, etc. of hazardous substances from ships. Complicity in evasion of punishment. Unlawful dealings with dangerous material, etc. Terrorist bombing. Attacks on an internationally protected person. 	<p>Specifically when?</p> <p>No specific date is set for when the Penal Code of 2005 will enter into force. This will not affect whether or not Norway comply with the FATF standards on this point. Section 147 b in the present Penal Code is in line with the FATF-standard on this point. This is specifically stated in the preparatory works (Proposal No. 8 (2007-2008)) to the new Penal Code. The amendments in the Penal Code are done merely to <i>clarify</i> that Norway meets international standards.</p>

Summary of factors underlying rating	Description of measures	Secretariat's comments / confirmation
	<ul style="list-style-type: none"> • Taking of hostages. • Threatening acts of terrorism, etc. • Terror conspiracy. • Incitement, enlistment and recruitment to acts of terrorism, etc. <p>Gross acts of terrorism will in the Penal Code of 2005 (which is planned to come into force in the autumn of 2009) be punishable with up to 30 years imprisonment. Today, 21 years imprisonment is maximum penalty in the Penal Code.</p> <p>A decision to freeze can be taken by the head and deputy head of the police security service as well as by any public prosecutor. A decision to freeze can be executed immediately and without any court hearing or approval if the requirements of the law are met. This also applies for foreign requests for assistance as regards freezing, cf. section 202d, first paragraph. The decision to freeze must within seven days bring the case before the District Court for affirmation.</p>	
	<p>1. As mentioned above, actions taken under S/RES/1267 (1999) and 1373 (2001) are published on the FSA's website under "Lister fra FN, FATF samt lignende kunngjøringer" (Lists from UN, FATF and similar announcements). The consolidated list from the UN's Sanctions Committee (1267) is included as a hyperlink in the web edition of the text of the Regulations on sanctions against Usama Bin Laden, Al-Qaida and the Taliban of 22 December 1999 No. 1374 on Lovdata (www.lovdata.no) and the Norwegian regulations will consequently always be updated. ("Lovdata" is a web registry containing all Norwegian legislation. The database is continuously updated)</p>	
<ul style="list-style-type: none"> • 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. 	<p>2. The Secretariat of the 1267 Committee with respect to Al-Qaida, Usama bin Laden, and the Taliban and other individuals, groups, undertakings and entities associated with them visited Norway in 2008 and was informed about the Norwegian freezing mechanisms pursuant to the S/RES/ 1267 (1999). No written report or conclusions were issued. Norwegian authorities were informed that no major deficiencies were identified and that the mechanisms are well functioning.</p>	
	<p>1. As mentioned above, the FSA (Kredittilsynet) published "Guidelines concerning the obligations to freeze assets related to terrorism" on its website (www.kredittilsynet.no) and on the website www.hvitvasking.no in 2008. Guidelines are enclosed. (See also response to Rec. 25 Supervisory authorities).</p>	

Summary of factors underlying rating	Description of measures	Secretariat's comments / confirmation
<ul style="list-style-type: none"> 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). 	2. The guidelines comprise the freezing obligations pursuant to S/RES/1267 (1999) and S/RES 1373 (2001).	

PART III

MEASURES TAKEN TO ADDRESS THE DEFICIENCIES IN RELATION TO OTHER RECOMMENDATIONS RATED PC OR NC

Forty Recommendations	Rating	Summary of factors underlying rating	Description of measures	Secretariat's comments / confirmation
Legal systems				
6. Politically exposed persons	NC	1. Norway has not implemented any AML/CFT measures concerning the establishment of customer relationships with politically exposed persons (PEPs).	1. Norway has implemented enhanced CDD measures, cf. MLA section 15. The MLA Section 15 Paragraph 2 sets out the requirements imposed on reporting entities when establishing a customer relationship with or carrying out transactions on behalf of PEPs. The reporting entities are obliged to have at their disposal appropriate due diligence measures to establish whether the customer is a PEP. The MLR Section 11 defines who is regarded as a PEP. The definition is based on the definition in EC Directive 2006/70/EC Article 2.	
7. Correspondent banking	NC	1. Norway has not implemented any AML/CFT measures concerning establishment of cross-border correspondent banking relationships.	1. Section 16 of the MLA implements AML/CFT measures concerning establishment of cross border correspondent banking relationships with institutions outside the EEA area. Certain safe-guards are mandatory when using a correspondent bank or <u>credit institution</u> outside the EEA. The obligation is limited to cross-boarder relationships with institutions outside the EEA because all EEA countries are legally obliged to	<p>1. What is the definition of the “credit institution”? Is there any provision which defines the “credit institution”?</p> <p>The MLA Section 16 implements EC Directive 2005/60/EC article 13 No. 3. “Credit institution” is defined in the Directive article 3 No. 1 as “a credit institution as defined in the first subparagraph of Article 1 (1) of Directive 2000/12/EC of the European Parliament and the Council of 20 March 2000 relating to the taking up and pursuit of the business of credit institutions, including branches within the meaning of Article 1 (3) of that Directive located in the</p>

Forty Recommendations	Rating	Summary of factors underlying rating	Description of measures	Secretariat's comments / confirmation
			implement EC Directive 2005/60/EC. Failure to implement the directive can be sanctioned by the EU Court of Justice or the EFTA Court of Justice	<p><i>Community of credit institutions having their head offices inside or outside the Community</i>". The definition of "credit institution" in Directive 2000/12/EC is implemented into Norwegian law in the Act on financing activity and financial institutions Section 1-5 No. 3. An English translation of the Act is enclosed.</p> <p>2. What is the sanction against the breach of the obligation under Section 16 of the MLA? And where is it provided?</p> <p>According to the MLA Section 27 Supervisory bodies may order an entity with a reporting obligation to put an end to matters that contravene the MLA or provisions laid down pursuant thereto. If the reporting entity fails to comply with orders from the supervisory bodies, they may impose a coercive fine.</p>
12. DNFBP – R.5, 6, 8-11, 17	PC	<p>1. 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).</p> <p>2. 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.</p> <p>3. Norway has not implemented any AML/CFT measures concerning Recommendations 6 that are applicable to Reporting BPs.</p>	<p>1. The scope of the MLA 2009 is broader than the MLA 2003. According to the MLA 2009 Section 4 Paragraph 2 No 6, trust and company service providers are within the scope of the MLA and have reporting obligations in line with the obligations imposed on FIs and other BPs. The term "trust and company service providers" is defined in the MLA section 2 Paragraph 1 No. 4. This definition is based on the definition in EC Directive 2005/60/EC article 3 No. 7.</p> <p>2. In addition to comments just provided, reference is made to response to Rec.5 above. The FSA supervise that real estate agents, accountants and auditors comply with the AML/CFT framework. As regards lawyers, the Supervisory Council for Legal Practice routinely looks at compliance with the AML/CFT framework in connection with their supervision activities and follow-up with sanctions where deemed appropriate.</p> <p>3. In addition to comments just provided,</p>	

Forty Recommendations	Rating	Summary of factors underlying rating	Description of measures	Secretariat's comments / confirmation
			reference is made to response to Rec.6 above.	
18. Shell banks	PC	<ul style="list-style-type: none"> • 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. 	<p>1. The MLA section 16 Paragraph 2 prohibits credit institutions from entering into or continue correspondent banking relationships with shell banks. The term "shell banks" is defined in the MLA Section 16 Paragraph 3.</p> <p>2. Credit institutions are obliged to take appropriate measures to ensure that they do not engage in or continue correspondent banking relationships with credit institutions known to allow their accounts to be used by shell banks, cf. the MLA Section 16 Paragraph 2.</p>	
25. Guidelines & Feedback	PC	<p>Supervisory authorities:</p> <ul style="list-style-type: none"> • Almost every reporting entity that the assessors met with asked for more specific and tailored guidance concerning AML/CFT obligations. 	<p>Supervisory authorities:</p> <p>1. The FSA (Kredittilsynet) is revising its comprehensive AML/CFT guidelines in close cooperation with relevant industry organisations. The deadline for this work is second quarter 2009 (The new legislation entered into force on 15. April 2009).</p> <p>In June 2006 Kredittilsynet issued specific and tailored AML/CFT guidelines to auditors and external accountants in close cooperation with relevant industry organisations and the FIU. Reference is made to Circular 13/2006, see enclosure. These guidelines will also be revised.</p> <p>Furthermore Kredittilsynet is heavily involved in AML/CFT education and training covering the whole financial sector. On a regular basis seminars with more than 200 participants are providing the participants with both news about legislation as well as typologies and trends</p>	

Forty Recommendations	Rating	Summary of factors underlying rating	Description of measures	Secretariat's comments / confirmation
		<ul style="list-style-type: none"> • The FSA has issued 	<p>based on national and international sources, including FATF. The FSA has together with the FIU and the private sector established a "meeting place" on a yearly basis for the whole AML/CFT sector in Norway. Guest speakers from different countries are invited. The meeting place is established on a non-profit basis.</p> <p>The FSA participates in a number of ML/TF seminars covering the whole financial sector. FSA experts are giving presentations and contributions to seminars and arrangements focusing on AML/TF. Seminars focusing solely on the new AML/TF-obligations are planned to take place in second halfyear of 2009. The guidance given during presentations etc. is published on the FSA website – and FSA-experts are daily contacted by officers/managers in the private sector regarding their AML/TF-obligations.</p> <p>On November 2nd 2007 the website operated by the Norwegian FIU and the FSA (Kredittilsynet), www.hvitvasking.no, was launched and is intended to contain all relevant information regarding AML/CFT for both private and public sector. The Editorial Board members come from both the public and the private sector. The website contains i.a. information concerning:</p> <ul style="list-style-type: none"> ○ Laws and regulations ○ Announcements from the public sector ○ Court decisions ○ News from FATF, EU, etc. ○ Typologies and trends 	<p><i>Please provide the latest ratio of STRs by the Norwegian / non-Norwegian.</i></p> <p>In 2008 the MLU received 9026 STRs. This was an</p>

Forty Recommendations	Rating	Summary of factors underlying rating	Description of measures	Secretariat's comments / confirmation
		<p>detailed guidance to Reporting FIs concerning how to comply with the reporting obligations. Despite the guidance given, <u>70% of all STRs are based on transactions made by non-Norwegians</u>. 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</p>	<p>Statistical data for the 1st quarter of 2008 shows that the website had many hits by users of the service. www.hvitvasking.no had in the period 3600 hits by 1500 unique visitors. The part of the website containing reporting issues has many hits, as well as news about the new legislation. Also typology issues have many hits. The website is still under elaboration and will be further expanded and updated.</p> <p>Each year the FSA issues on ad-hoc basis written interpretations on AML-issues. These interpretations are to a large extent considered precedent. Such interpretations (and precedents) are an important tool for Norwegian authorities to guide reporting entities concerning their AML/CFT obligations.</p> <p>2. Pursuant to Norwegian AML-legislation banks and finance companies are obliged to establish electronic monitoring systems (deadline was by the end of 2004) in order to identify possible STRs (suspicious transactions), cf. MLA section 24 and MLR Section 18. These monitoring systems contribute to adequately target the nature of the transactions, and has significantly contributed to enhancing the quality of the reports. Norwegian banks and finance companies have allocated considerable resources to implementing electronic monitoring systems and follow up of STRs.</p> <p>In the communication between the authorities and entities/professions with reporting obligations, <u>emphasis has increasingly been put on mediating that citizenship is merely one of several indicators when identifying transactions that might qualify for a STR</u>. Regarding STRs</p>	<p>increase of 20% compared to 2007. The nationality of the reported person is not recorded by the reporting entities. This is due to the fact that according to the Norwegian legislation, it is the transactions and the suspicion connected to these which are the main focus.</p> <p><u>2006 and 2007</u></p> <p>There are however some numbers available concerning nationality for the years 2006 and 2007. This is due to the fact that up to the year 2008, a lot of the STRs were sent to the MLU by post or fax. Upon receiving an STR in the standardised form required, the information therein was manually put into a computer database that was specifically designed for such information. During this process the MLU also established the nationality of the subject and entered this into the database.</p> <p>Several of the persons reported in connection with suspicious transactions occurred in a number of STRs. Most of the reported persons are Norwegian nationals, but persons from an increasing number of countries were reported. In 2006 and 2007, 72 % of the persons were Norwegian nationals and 28% were foreign nationals. Persons reported in connection with currency exchange and money transfer are not included in these numbers. There is reason to believe that the share of foreign nationals would be higher if these categories were included, the reason being that the users of these services tend to be persons who send money back to their families in their countries of origin where banking services may be less developed or who stay in Norway for a short period of time, and who for different reasons need to carry out currency exchange or money transfers. During 2007 the MLU received STRs on persons from 84 different countries.</p>

Forty Recommendations	Rating	Summary of factors underlying rating	Description of measures	Secretariat's comments / confirmation
		<p>guidelines to auditors and external accountants.</p> <p>Financial intelligence unit:</p> <p>1. 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</p>	<p>from Money transfer businesses it follows from the nature of the services provided that the number of reported foreign nationals must be expected to be significant.</p> <p>Financial Intelligence Unit</p> <p>1. Cf. description under Rec. 26 and response below</p> <p>2. The MLU has assigned an official day-to-day responsibility for compliance in relation to the reporting entities. Feedback is given regularly to the reporting entities via follow-up from the person responsible for compliance at the MLU and via the analysts in connection with specific cases. The MLU holds regular follow-up meetings with several of the reporting entities and also gives lectures at courses and seminars attended by the reporting entities and their interest organisations.</p> <p>As referred to above, the new website operated by the Norwegian FIU and the FSA (Kredittilsynet), www.hvitvasking.no, was launched on 2 November 2007 and is intended to contain comprehensive and relevant information regarding AML/TF for both private and public sectors.</p> <p>In addition, the unit produces annual reports, where it provides an account of trends, cases, statistics, etc. The unit also contributes to Økokrim's report on trends in financial crime.</p> <p>Compliance in relation to reporting entities is a field that has been given high priority in recent years. One of the objectives of</p>	

Forty Recommendations	Rating	Summary of factors underlying rating	Description of measures	Secretariat's comments / confirmation
		<p>practice of sending quarterly reports recommenced as of 1 January 2005.</p> <p>2. 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".</p>	<p>the FIU is to provide training, (one-to-one, seminars and training at the Norwegian Police Academy). "Ask" enables a better structure for follow-up of reporting entities and others, while providing better data for this purpose. "Ask" provides automatic feedback to reporting entities on receipt of STRs.</p> <p>According to its plan of operations, the FIU shall also make on-site visits to Norwegian police districts in order to increase awareness of the potential of the information available from the unit and to improve the routines for receiving this information. Several such visits have been conducted in recent years in addition to the lectures held at central and regional intelligence conferences.</p>	
Institutional and other measures				
30. Resources, integrity and training	PC	<p>Financial Intelligence Unit:</p> <p>1. 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</p>	<p>Financial Intelligence Unit:</p> <p>1. Cf. description under rec. 26 2. Cf. description under rec. 26 3. Cf. description under rec. 26</p>	

Forty Recommendations	Rating	Summary of factors underlying rating	Description of measures	Secretariat's comments / confirmation
		<p>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.</p> <p>2. 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.</p> <p>3. 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.</p> <p>4. The management and resources of the MLU currently are not ring-fenced.</p>	<p>4. Ring fencing of budget resources within a unit of a public authority, is not in conformity with the concept of the so-called frame budgeting, which is the overall budgeting system within the public sector, and which allocates budget</p>	

Forty Recommendations	Rating	Summary of factors underlying rating	Description of measures	Secretariat's comments / confirmation
		<p>5. <u>High staff turnover</u> at the MLU has caused some difficulties in maintaining effective relationships with reporting entities.</p> <p>6. Only two of the MLU's</p>	<p>provisions in the institution as such. As regards the MLU, the system is designed to ensure that the Director of Økokrim is fully responsible for allocating the institution's budget so that the MLU reaches its objectives. Although the resources of the MLU are not ring-fenced as such, the Ministry of Justice has decided to allocate more money to Økokrim such that the MLU's staff has increased together with increased resources to an investigative team closely linked to the activities of the MLU. Reference is also made to the funding of approx. 4 million Euro for the "Ask" system as described above. These measures reflect the objective of strengthening the work of the MLU on a permanent basis.</p> <p>5. <u>The staffing of the unit has been relatively stable over the recent years and staff turnover is not more frequent than that of other units that it is natural to compare with.</u> The challenge is to identify appropriate candidates with relevant competence. The FIU is a unit with a need for highly specialised competence in investigation/intelligence, economy and analysis. The use of "Ask" also requires the core staff to have high competence in the use of IT tools. This competence is very attractive both in the private sector and in other state bodies. <u>The level of salaries and keen competition makes, and will continue to make staff turnover a constant issue.</u> The FIU has a goal that new employees who have not taken the operative intelligence course shall have this competence within one year following their appointment.</p>	<p>1. What are the main reasons for (high) staff turnover at the MLU?</p> <p>Staffing of the MLU has been relatively stable over the last years. This impacts positively on the ability to maintain effective relationships with reporting entities. That being said, turnover is still an issue. This is normal and not unexpected, given the skills and expertise of many of the officers working at the unit.</p> <p>2. Is it because of the multidisciplinary nature of the MLU (i.e., secondment of prosecutors, legal advisers, police investigators, etc.)?</p> <p>The multidisciplinary nature of the MLU is considered as a strength and a necessity, rather than a weakness in the context of personnel policy.</p> <p>3. Does the budgetary system that is not ring-fenced affect the level of salaries?</p> <p>The budgetary system does not to any substantial degree affect the level of salaries. The level of salaries for different categories of posts is decided by the Ministry of Government Administration and Reform for the whole state sector. There is certain flexibility with respect to how staff is assigned to different posts, but this does not have any significant impact on the budget. The budgetary system has rather an effect on the number of posts altogether.</p> <p>4. How many of the staff are "proper" MLU staff, and is the proper staff going to be increased?</p>

Forty Recommendations	Rating	Summary of factors underlying rating	Description of measures	Secretariat's comments / confirmation
		<p>staff is trained in the use of Analysts Notebook.</p> <p>7. 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.</p> <p>Law enforcement and prosecutorial authorities:</p> <p>1. The Police College currently provides an annual advanced training course to police officers and lawyers on economic crime; however, Norway</p>	<p>6. As regards training, the situation today is that all investigators/analysts at the MLU have received training in the use of Analyst Notebook. Except for one, all investigators and analysts at the unit have received additional analytical training at the National Criminal Intelligence Service or at the Norwegian Police Security Service.</p> <p>7. The Control Committee does not have any budgetary powers in relation to the MLU. The Control Committee is only mandated – by law – to supervise the MLU's handling of information focusing on issues of protection of privacy. It has no influence on the allocation of resources and the strategic and operational aspects of the MLUs work. The MLU has not experienced that the Control Committee is interfering in its daily work. The MLU and the Control Committee meet 2-3 times a year. Since 2005, ØKOKRIM has been assigned 11 new staff to work on money laundering related intelligence reports and cases (MLU and the established investigation team). The budgetary increase was supported by necessary funding for developing a sophisticated system for receiving and analysing STRs ("Ask"), cf. Rec. 26. The system has been fully operational since June 2008.</p> <p>Law enforcement and prosecutorial authorities</p> <p>1. The basic training for police officers takes place at the Police Academy. Financial investigation is part of the basic training. Furthermore, annual courses in advanced investigative techniques (financial and economic investigation) are</p>	<p>The whole of the staff at the MLU is considered as "proper" MLU staff. As of today the MLU consists of two prosecutors, eleven analysts, two secretaries/ advisors and one person designated to tasks concerning strategic analysis. There are at the moment no concrete plans to increase the number of analysts.</p> <p><i>Does the Økokrim have no conflict of interest between the training and budget allocating for MLU staff and Økokrim's core staff?</i></p> <p>Økokrim is designated with a large number of tasks in the field of economic and environmental crime. The tasks and obligations of the MLU is considered to be an important part of this assignment. MLU staff is as much "core" staff as other staff.</p>

Forty Recommendations	Rating	Summary of factors underlying rating	Description of measures	Secretariat's comments / confirmation
		<p>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.</p> <p>2. There is concern that ØKOKRIM attracts too many of the most highly trained economic crime investigators—to the detriment of the police districts.</p> <p>3. 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.</p>	<p>offered as a part of several post-graduate programmes. This course runs over a period of one year, constituting ½ year of full time studies. Approximately 30 persons are following the course each year. As part of the post-graduate training and master studies in organized crime, studies in money laundering, financial investigation and financial intelligence are offered.</p> <p>In addition to the studies offered at the Police Academy, there are other relevant training programmes as well. <u>The National Authority for investigation and prosecution of economic crime (Økokrim), offers comprehensive courses and seminars for investigators and prosecutors as well as auditors. Økokrim also offers courses at i.a. the Norwegian School of Economics and Business Administration and other institutions.</u> Oslo Police District, by far the largest police district in Norway, provides trainee programs in confiscation with a duration of five months. There is also arrangements and collaboration regarding policy and operational aspects, i.a. between police and tax authorities at local and regional level. In addition, there is collaboration between the authorities and the private sector, with i.a. yearly seminars.</p> <p>2. The posts assigned to the economic crime teams in the local police districts are to a very large extent operational. Some districts are actively searching for, and recruiting people with the right background and motivation. Although Økokrim recruits personnel from the economic crime teams, this is not reported to be a problem for the</p>	<p><i>Please provide the latest following data:</i></p> <p>1) No. of FSA's staff (183 as of end-2003) The FSA has a manning table of 245 posts</p> <p>2) No. of on-site inspection per year (approx. 50 as of 2006)</p>

Forty Recommendations	Rating	Summary of factors underlying rating	Description of measures	Secretariat's comments / confirmation																																																																																																		
		<p>Supervisory authorities:</p> <p>1. Considering the number of entities that the FSA is responsible for supervising, its number of staff seems inadequate.</p>	<p>police districts.</p> <p>3. The Police Directorate has had an increasingly strong focus on economic and financial investigation over the last years. Budgets and budgetary directives in this area have been strengthened and it has been clearly communicated that the efforts of the police districts are expected to be strengthened. Organization of the work against economic crime, as well as allocation of more resources to a number of police districts, has contributed to strengthening the work of the police districts in this field. The last years have also seen budgetary increases for Økokrim, in particular the Money Laundering Unit, cf. under Rec. 26.</p> <p>Supervisory authorities:</p> <p>1. The FSA (Kredittilsynet) is an integrated supervisory body which comprises supervision of i.a. bank., finance, insurance and securities industries. This organisation and structure gives considerable flexibility to allocate resources to supervisory tasks with a high priority, including AML/CFT supervision. Illustrative of this is that two different departments at the FSA in 2005-2006 cooperated in carrying out thematic AML/CFT inspections of all MVTs providers operating in Norway, i.e. all agents representing Western Union and MoneyGram, see comments to SR VI below. This was a considerable supervisory effort.</p> <p>The FSA's supervision and on-site inspections of institutions in the banking</p>	<p>The table below provides an overview of total on-site inspections.</p> <table border="1" data-bbox="1417 392 2040 1362"> <thead> <tr> <th colspan="7" data-bbox="1417 392 2040 469">Number of on-site inspections by type of institution (including IT inspections)</th> </tr> <tr> <th data-bbox="1417 469 1576 517"></th> <th data-bbox="1576 469 1644 517">2003</th> <th data-bbox="1644 469 1711 517">2004</th> <th data-bbox="1711 469 1778 517">2005</th> <th data-bbox="1778 469 1845 517">2006</th> <th data-bbox="1845 469 1912 517">2007</th> <th data-bbox="1912 469 2040 517">2008</th> </tr> </thead> <tbody> <tr> <td data-bbox="1417 517 1576 564">Banks/finance</td> <td data-bbox="1576 517 1644 564">53</td> <td data-bbox="1644 517 1711 564">57</td> <td data-bbox="1711 517 1778 564">50</td> <td data-bbox="1778 517 1845 564">48</td> <td data-bbox="1845 517 1912 564">47</td> <td data-bbox="1912 517 2040 564">37</td> </tr> <tr> <td data-bbox="1417 564 1576 636">E-money institutions</td> <td data-bbox="1576 564 1644 636">-</td> <td data-bbox="1644 564 1711 636">-</td> <td data-bbox="1711 564 1778 636">-</td> <td data-bbox="1778 564 1845 636">1</td> <td data-bbox="1845 564 1912 636">-</td> <td data-bbox="1912 564 2040 636">-</td> </tr> <tr> <td data-bbox="1417 636 1576 708">Holding companies</td> <td data-bbox="1576 636 1644 708">-</td> <td data-bbox="1644 636 1711 708">4</td> <td data-bbox="1711 636 1778 708">2</td> <td data-bbox="1778 636 1845 708">-</td> <td data-bbox="1845 636 1912 708">2</td> <td data-bbox="1912 636 2040 708">-</td> </tr> <tr> <td data-bbox="1417 708 1576 756">Insurance</td> <td data-bbox="1576 708 1644 756">19</td> <td data-bbox="1644 708 1711 756">11</td> <td data-bbox="1711 708 1778 756">9</td> <td data-bbox="1778 708 1845 756">5</td> <td data-bbox="1845 708 1912 756">6</td> <td data-bbox="1912 708 2040 756">6</td> </tr> <tr> <td data-bbox="1417 756 1576 828">Insurance mediators</td> <td data-bbox="1576 756 1644 828">6</td> <td data-bbox="1644 756 1711 828">3</td> <td data-bbox="1711 756 1778 828">1</td> <td data-bbox="1778 756 1845 828">5</td> <td data-bbox="1845 756 1912 828">3</td> <td data-bbox="1912 756 2040 828">3</td> </tr> <tr> <td data-bbox="1417 828 1576 900">Pension funds</td> <td data-bbox="1576 828 1644 900">5</td> <td data-bbox="1644 828 1711 900">4</td> <td data-bbox="1711 828 1778 900">1</td> <td data-bbox="1778 828 1845 900">1</td> <td data-bbox="1845 828 1912 900">2</td> <td data-bbox="1912 828 2040 900">6</td> </tr> <tr> <td data-bbox="1417 900 1576 971">Investment firms</td> <td data-bbox="1576 900 1644 971">23</td> <td data-bbox="1644 900 1711 971">14</td> <td data-bbox="1711 900 1778 971">22</td> <td data-bbox="1778 900 1845 971">18</td> <td data-bbox="1845 900 1912 971">20</td> <td data-bbox="1912 900 2040 971">19</td> </tr> <tr> <td data-bbox="1417 971 1576 1107">Other institutions in the securities market</td> <td data-bbox="1576 971 1644 1107">13</td> <td data-bbox="1644 971 1711 1107">7</td> <td data-bbox="1711 971 1778 1107">14</td> <td data-bbox="1778 971 1845 1107">7</td> <td data-bbox="1845 971 1912 1107">6</td> <td data-bbox="1912 971 2040 1107">1</td> </tr> <tr> <td data-bbox="1417 1107 1576 1155">Auditors</td> <td data-bbox="1576 1107 1644 1155">19</td> <td data-bbox="1644 1107 1711 1155">65</td> <td data-bbox="1711 1107 1778 1155">52</td> <td data-bbox="1778 1107 1845 1155">52</td> <td data-bbox="1845 1107 1912 1155">22</td> <td data-bbox="1912 1107 2040 1155">29</td> </tr> <tr> <td data-bbox="1417 1155 1576 1227">External accountants</td> <td data-bbox="1576 1155 1644 1227">35</td> <td data-bbox="1644 1155 1711 1227">15</td> <td data-bbox="1711 1155 1778 1227">56</td> <td data-bbox="1778 1155 1845 1227">46</td> <td data-bbox="1845 1155 1912 1227">41</td> <td data-bbox="1912 1155 2040 1227">60</td> </tr> <tr> <td data-bbox="1417 1227 1576 1275">Estate agents</td> <td data-bbox="1576 1227 1644 1275">12</td> <td data-bbox="1644 1227 1711 1275">18</td> <td data-bbox="1711 1227 1778 1275">22</td> <td data-bbox="1778 1227 1845 1275">40</td> <td data-bbox="1845 1227 1912 1275">51</td> <td data-bbox="1912 1227 2040 1275">66</td> </tr> <tr> <td data-bbox="1417 1275 1576 1362">Debt collection agencies</td> <td data-bbox="1576 1275 1644 1362">12</td> <td data-bbox="1644 1275 1711 1362">25</td> <td data-bbox="1711 1275 1778 1362">7</td> <td data-bbox="1778 1275 1845 1362">5</td> <td data-bbox="1845 1275 1912 1362">6</td> <td data-bbox="1912 1275 2040 1362">13</td> </tr> </tbody> </table>	Number of on-site inspections by type of institution (including IT inspections)								2003	2004	2005	2006	2007	2008	Banks/finance	53	57	50	48	47	37	E-money institutions	-	-	-	1	-	-	Holding companies	-	4	2	-	2	-	Insurance	19	11	9	5	6	6	Insurance mediators	6	3	1	5	3	3	Pension funds	5	4	1	1	2	6	Investment firms	23	14	22	18	20	19	Other institutions in the securities market	13	7	14	7	6	1	Auditors	19	65	52	52	22	29	External accountants	35	15	56	46	41	60	Estate agents	12	18	22	40	51	66	Debt collection agencies	12	25	7	5	6	13
Number of on-site inspections by type of institution (including IT inspections)																																																																																																						
	2003	2004	2005	2006	2007	2008																																																																																																
Banks/finance	53	57	50	48	47	37																																																																																																
E-money institutions	-	-	-	1	-	-																																																																																																
Holding companies	-	4	2	-	2	-																																																																																																
Insurance	19	11	9	5	6	6																																																																																																
Insurance mediators	6	3	1	5	3	3																																																																																																
Pension funds	5	4	1	1	2	6																																																																																																
Investment firms	23	14	22	18	20	19																																																																																																
Other institutions in the securities market	13	7	14	7	6	1																																																																																																
Auditors	19	65	52	52	22	29																																																																																																
External accountants	35	15	56	46	41	60																																																																																																
Estate agents	12	18	22	40	51	66																																																																																																
Debt collection agencies	12	25	7	5	6	13																																																																																																

Forty Recommendations	Rating	Summary of factors underlying rating	Description of measures	Secretariat's comments / confirmation																						
			<p>and finance sector is conducted on a risk based approach. <u>The staff designated to on-site inspections within the banking sector is at the time 23.</u> (The number was 19 in the follow-up report to FATF in 2007).With regard to AML/CFT supervision, priority is given to those institutions with services, products and indicators making them exposed to money laundering and terrorist financing. The Ministry of Finance has granted the FSA resources in order to establish an additional position allocated to AML/CFT tasks.</p>	<table border="1" data-bbox="1420 277 2049 421"> <tr> <td data-bbox="1420 277 1576 376">Data processing centres</td> <td data-bbox="1576 277 1644 376">2</td> <td data-bbox="1644 277 1711 376">2</td> <td data-bbox="1711 277 1778 376">5</td> <td data-bbox="1778 277 1845 376">3</td> <td data-bbox="1845 277 1912 376">4</td> <td data-bbox="1912 277 1980 376">4</td> <td data-bbox="1980 277 2049 376"></td> </tr> <tr> <td data-bbox="1420 376 1576 421">Sum</td> <td data-bbox="1576 376 1644 421">199</td> <td data-bbox="1644 376 1711 421">225</td> <td data-bbox="1711 376 1778 421">241</td> <td data-bbox="1778 376 1845 421">231</td> <td data-bbox="1845 376 1912 421">210</td> <td data-bbox="1912 376 1980 421">244</td> <td data-bbox="1980 376 2049 421"></td> </tr> </table> <p>The major Norwegian financial institutions (DnB NOR, Nordea and the SpareBank 1 Group and its owners), which have a market share of 65% of the Norwegian banking market, are continuously supervised. This includes several on-site inspections each year at the major institutions related to different business areas, risk categories, subsidiaries etc.</p> <p>The supervision includes i.a. AML/CFT obligations and is conducted on a risk-based approach.</p> <p>AML/CFT obligations are in particularly supervised in banks and finance companies, auditors, external accountants, estate agents and investment firms. The number and extent of such inspections changes from year to year and from institution to institution and are conducted on a risk-based approach. No statistics exist concerning frequency or cycle of inspections for these kind of institutions.</p> <p>3) No. of thematic AML/CFT on-site inspection per year</p> <p>The following thematic AML/CFT inspections have been carried out in 2007 and 2008:</p> <p>2007 - 1 thematic on-site inspections at DnB NOR Bank (market share of the Norwegian banking market 39%, market share of the total Norwegian financial market 33%).</p> <p>2008 – 1 thematic on-site inspection at Nordea Bank Norge (market share of the Norwegian banking market 14%).</p> <p>In 2008 an off-site review of electronic monitoring systems at all finance companies (30 companies) was carried out.</p> <p>4) No. of supervising entities (2,518 as of end-2003)</p> <p>Please see enclosed one table in English for an overview of all supervised entities for the period 2003-2007 and one table in Norwegian of all supervised entities for the period 2004-2008. The number 2.518 is not the correct number of</p>							Data processing centres	2	2	5	3	4	4		Sum	199	225	241	231	210	244	
Data processing centres	2	2	5	3	4	4																				
Sum	199	225	241	231	210	244																				

Forty Recommendations	Rating	Summary of factors underlying rating	Description of measures	Secretariat's comments / confirmation
				supervised entities in 2003. 5) average cycle of on-site inspection to FIs Please refer to response to question 2) above.
32. Statistics	PC	<p>1. 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>i.e.</i> its computer systems) has thus impeded its statistics collection capabilities.</p> <p>2. 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.</p>	<p>1. As regards the MLU, the new "Ask"-system contains advanced functionality for developing and visualizing statistics related to AML/CFT deficiencies. These statistics are based on a new and significantly improved data-model compared to the previous system. Over time, the quality and reliability of statistics will improve greatly. In particular concerning the receipt and sending of information and requests to foreign counterparts because routines and data input are of a far better quality than previously was the case.</p> <p>2. The MLU has, via its "Ask"-system, a good overview of incoming information as well as how the information is processed and distributed. There is statistics concerning the number of cases opened, information sent to control bodies (tax, customs, etc.) and also over notifications going to the central police intelligence system (called "Indicia"). There is no particular statistics reflecting the actual use of the information. This is not considered practical, particularly since the information provided to the central police</p>	

Forty Recommendations	Rating	Summary of factors underlying rating	Description of measures	Secretariat's comments / confirmation
			<p>intelligence database frequently comes to use at a later stage.</p> <p>As regards the police districts, statistics are maintained as regards reported offences and prosecutorial decisions according to Section 317 under chapter 31 ("Receiving and Money Laundering") of the Penal Code, as amended and in force from June 29 2006:</p> <p><i>"Any person who receives or obtains for himself or another person any part of the proceeds of a criminal act (receiving) or who aids and abets the securing of such proceeds for another person (money laundering) shall be liable to fines or imprisonment for a term not exceeding three years. Aiding and abetting shall be deemed to include collecting, storing, concealing, transporting, sending, transferring, converting, disposing of, pledging or mortgaging, or investing the proceeds. Any object, claim or service substituted for the proceeds shall be regarded as equivalent thereto.</i></p> <p><i>A person who by conversion or transfer of property or by other means disguises or conceals the whereabouts or origin of the proceeds of a criminal act he has himself committed, the identity of the person or persons with disposition over it, its movements or rights associated with it shall also be guilty of money laundering.</i></p> <p><i>Such offence takes place even though no person may be punished for the act from which the proceeds are derived, by reason of the provisions of sections 44 and 46.</i></p>	

Forty Recommendations	Rating	Summary of factors underlying rating	Description of measures	Secretariat's comments / confirmation
			<p><i>An aggravated offence shall be punishable with imprisonment for a term not exceeding six years. In deciding whether an offence is aggravated, particular importance shall be attached to what kind of criminal act the proceeds are derived from, the value of the proceeds, the amount of any advantage the offender has received or obtained for himself or another person, and whether the offender has habitually been engaged in such offences. If the proceeds are derived from a drug felony, importance shall also be attached to the nature and quantity of the substance with which the proceeds are connected.</i></p> <p><i>If the offence is concerned with the proceeds of a drug felony, imprisonment for a term not exceeding 21 years may be imposed under especially aggravating circumstances.</i></p> <p><i>If the offence is committed through negligence, it shall be punishable by fines or imprisonment for a term not exceeding two years.</i></p> <p><i>No penalty pursuant to this section shall, however, be applicable to any person who receives the proceeds for the ordinary maintenance of himself or another person from a person who is obliged to provide such maintenance, or to any person who receives the proceeds as normal payment for ordinary consumer goods, articles for everyday use or services."</i></p>	<p><i>Is there any statistics available now?</i></p> <p>There is still no statistics available concerning the nature of the mutual legal assistance request.</p> <p><i>Does this mean that nobody overlooks the overall communication? Why?</i></p> <p>The Ministry of Justice and the Police has a close collaboration with the Norwegian Police and prosecution Authorities as to mutual legal assistance requests. Thus, the Ministry has a good overview of the judicial cooperation regarding such requests. The impression of the Ministry is that this communication functions very well, and therefore, we have not considered it necessary to maintain detailed statistics as of today.</p> <p><i>Does this mean that nobody overlooks the overall communication among Nordic countries? Why?</i></p> <p>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. Hence, these requests are forwarded directly to/from different Police Districts and not to/from one central authority. This facilitates for very rapid feedback without any unnecessary red tape. The Ministry of Justice and the Police has a close collaboration with the Norwegian Police and prosecution Authorities as to mutual legal assistance requests, including requests for extradition. Thus, the Ministry considers that it has a good overview of the judicial cooperation also in this respect and</p>

Forty Recommendations	Rating	Summary of factors underlying rating	Description of measures	Secretariat's comments / confirmation
		<p>3. Norway does not maintain statistics concerning sanctions imposed for failing to comply with AML/CFT obligations.</p> <p>4. <u>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.</u> Norway does not</p>	<p>Statistics from the police districts on reported offences and prosecutorial decisions according to section 317 under chapter 31 ("Receiving and Money Laundering") of the Penal Code is enclosed. The statistics can be divided into the "ordinary offences" punishable with up to three years imprisonment, the aggravated offences (up to six years imprisonment), self laundering of proceeds, drug felony related offences (up to 21 years imprisonment) and negligent offences (up to two years imprisonment) and forwarded to the FATF if that is desirable. The statistics does not however cover decisions by the courts, with the exception of acquittals.</p> <p>3. The FSA has established a registration system concerning administrative sanctions including i.a. written corrective measures, orders and coercive measures. Enclosed is a list of administrative sanctions imposed by Kredittilsynet in 2008. Kredittilsynet imposed 59 administrative sanctions in 2008:</p> <ul style="list-style-type: none"> o banks (7) o auditors and accountants (35) o real estate agents (17) <p>4. Mutual Legal Assistance: In accordance with the Schengen Convention Article 53 and the EU 2000 MLA Convention Article 6, to which Norway is a party, requests for Mutual Legal Assistance may be <u>communicated directly between the competent judicial authorities.</u> This direct communication contributes to making</p>	<p>that it generally functions in accordance with the objectives. Also in this context the understanding of the Ministry of Justice is that this well established system works very well. Hence, we have not considered it necessary to maintain statistics concerning such requests as of today</p> <p>Please provide the latest statistics.</p> <p>Formal requests for assistance from FIU's</p> <p>The total number of requests in:</p> <ul style="list-style-type: none"> - 2007 was 34 - 2008 was 65 - so far in 2009 it is 33 <p>How is the accuracy of the figures ensured?</p> <p>The accuracy of the figures is ensured by the fact that the request from Egmont Group members and the answers to these are exchanged through the Egmont Secure Web system. All requests are also logged, filed and handled in the "Ask" system. Three analysts and one secretary have been assigned with a special responsibility for these requests.</p>

Forty Recommendations	Rating	Summary of factors underlying rating	Description of measures	Secretariat's comments / confirmation												
		<p>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.</p> <p>5. 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.</p> <p>6. 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.</p>	<p>judicial cooperation between EU/Schengen states much more efficient. Requests to and from EU/Schengen represent the majority of the MLA requests in Norway.</p> <p>Concerning the requests that are sent through the Ministry of Justice, either because the requesting state is not a EU/Schengen state or because the requesting authority for some reason decided not to send the request directly to the competent judicial authority in Norway, the average time required to respond varies from one to three months. If the request is urgent, it will be given priority accordingly. Whenever a request has not been complied with within three months, the Director of Public Prosecutions will remind the State Prosecutor of the case. We expect that requests communicated directly between the judicial authorities of the requesting and the requested state require less time, as they involve fewer levels of communication.</p> <p>5 & 6. Statistics related to extradition 2005 - 2007:</p> <table border="1" data-bbox="936 1034 1391 1225"> <thead> <tr> <th></th> <th>2005</th> <th>2006</th> <th>2007</th> </tr> </thead> <tbody> <tr> <td>Extradition from Norway</td> <td>26</td> <td>24</td> <td>25</td> </tr> <tr> <td>Extradition to Norway</td> <td>42</td> <td>29</td> <td>25</td> </tr> </tbody> </table> <p>The statistics include all extradition requests to and from Norway, <u>except requests for extradition between Norway and other Nordic countries</u>, the reason being that these requests are</p>		2005	2006	2007	Extradition from Norway	26	24	25	Extradition to Norway	42	29	25	
	2005	2006	2007													
Extradition from Norway	26	24	25													
Extradition to Norway	42	29	25													

Forty Recommendations	Rating	Summary of factors underlying rating	Description of measures	Secretariat's comments / confirmation
		<p>7. <u>Norway does maintain statistics concerning the number of formal requests for assistance</u> made to or received by the FIU from foreign counterparts.</p> <p>8. <u>The figures are uncertain</u> because the registration routines are not quite clear, especially as regards the requests made to foreign counterparts.</p>	<p>communicated directly between the competent judicial authorities.</p> <p>The Nordic countries concluded an agreement on a Nordic Arrest Warrant on 15 November 2005. This agreement has been implemented in Norwegian law through the Nordic Arrest Warrant Act 11 June 2008, which is expected to enter into force in 2009. The Nordic Arrest Warrant will replace the Nordic Extradition Act from 1961, and goes further than both the Nordic Extradition Act and the European Arrest Warrant (EAW), both regarding admissible grounds for refusal of surrender and regarding the time-limits for deciding on the warrant and surrender of the person concerned.</p>	
International Co-operation				
38.MLA on confiscation and freezing	PC	<p>1. 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.</p>	<p>1. In 2006, <u>Regulation of 01.02.1995</u> to Act of 20.07.1991 no. 67, was amended so that the UN Convention Against Corruption was added to the Vienna and Strasbourg Conventions. This means that competent authorities are mandated to give effect to confiscation orders – related to property acquired through or involved in the commission of an offence established in accordance with the convention (i.e. money laundering) - issued by the courts of other parties to the convention.</p> <p>At the same point in time, Section 24 (2) of the Act relating to extradition of offenders was amended to read:</p> <p><i>“The request shall be submitted to the Ministry unless otherwise stipulated in the agreement with the foreign state. The request shall contain information as to the</i></p>	<p><i>Please provide the underlined regulation and Act.</i></p> <p>The Act and regulations are unfortunately not available in in english versions. We will provide the English texts a soon as possible</p> <p><i>Please provide the underlined regulation.</i></p>

Forty Recommendations	Rating	Summary of factors underlying rating	Description of measures	Secretariat's comments / confirmation
			<p><i>nature, time and place of the punishable offence. Unless otherwise stipulated in the agreement with the foreign state, the request may only be complied with if it is established that a decision has been made concerning the use of coercive measures, issued in accordance with the legislation of the state in question."</i></p> <p>This means that requests regarding the use of coercive measures in order to seize assets are not dependent on a decision regarding coercive measures in the requesting state if this is stipulated in the agreement.</p> <p><u>Regulation of 1. February 1995 no. 90</u> has now added to it the UN Convention against corruption. This means that a decision by a State party to confiscate can be executed on the basis of the decision of a foreign court.</p> <p>As from 01.01.2006, the Penal Code section 37, third paragraph regulates the issue of asset sharing, and decides that:</p> <p><i>"The Ministry may decide that the confiscated assets shall be divided between the Norwegian state and one or several other states. The decision shall be based on inter alia; the expenses incurred by the states involved, in which state the detrimental impact has occurred and where the proceeds have originated. Sharing in accordance with this paragraph can not lead to a reduction in the reimbursement of a compensation claim decided by the court in accordance with paragraph two (of section 37 d)."</i></p> <p>(unofficial translation)</p>	<p>The regulation is unfortunately not available in in English versions. We will provide the english texts a soon as possible</p>

Forty Recommendations	Rating	Summary of factors underlying rating	Description of measures	Secretariat's comments / confirmation
Nine Special Recommendations	Rating	Summary of factors underlying rating		
SR VI AML requirements for money/value transfer services	PC	<p>1. 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.</p> <p>2. 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.</p>	<p>1. The MLA 2009, which entered into force 15. April 2009, applies i.a to "undertakings operating activities consisting of transfer of money ...". Reference is made to the MLA section 4 Paragraph 1 No. 4. As regards Recommendations 5-7 please refer to response under these recommendations above. Rec. 15 is implemented in the MLA Section 23. Section 23 is based on EC Directive 2005/60/EC articles 34 and 35. The obligation to have in place internal procedures and systems to ensure fulfilment of the MLA applies to all reporting entities, including MVTS. Rec. 22 is implemented through the MLA Section 26. The obligation pursuant to Section 26 only applies to branches and subsidiaries outside the EEA area because the EU/EEA countries are legally obliged to implement Directive 2005/60/EC, and failure to implement can be sanctioned by the EFTA Court or European Court of Justice, see Introduction to the report for more information on the EU/EEA structure.</p> <p>2. In 2006 the Norwegian MVTS sector reported 3 941 STRs to the MLU (ØKOKRIM) (in 2005 – 2 512 STRs). The total number of STR reports from all entities with a reporting obligation was 7 042 (in 2005 – 4 893 STRs). In 2007 the Norwegian MVTS sector reported 3 385 STRs to the MLU (ØKOKRIM). The total number of STR reports from all entities with a reporting obligation was 7 543. In 2008 the Norwegian MVTS sector reported 6 680 STRs to the MLU (ØKOKRIM). The total number of STR</p>	

Forty Recommendations	Rating	Summary of factors underlying rating	Description of measures	Secretariat's comments / confirmation
		<p>3. 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.</p>	<p>reports from all entities with a reporting obligation was 9 026. Statistics referenced clearly shows that there is significant increase in the number of reports from this sector from 2005 to 2008. The increase in STRs and the supervisory activities carried out by the FSA indicates that Rec. 13 is reasonable effectively implemented in this sector.</p> <p>3. The MVTs provider referred to by the FATF in the report template reported 1173 STRs to ØKOKRIM in 2006 (in addition to this, 796 STRs concerning selling and buying of currency). The total number of reports from the MVTs industry was 3 941 in 2006. Kredittilsynet conducted a thematic AML/CFT inspection at the mentioned MVTs provider in 2005 and the home state supervisor was informed about problems with the company's reporting obligation. Meetings between the company, the FIU and Kredittilsynet were arranged in order to solve the reporting problems. In the view of the FSA, the particular problems concerning this provider are now adequately addressed</p> <p>As mentioned above under Rec. 30 the FSA (Kredittilsynet) has since 2005 carried out thematic AML/CFT on-site inspections in the whole MVTs sector (all agents representing MoneyGram and Western Union in Norway). The inspections comprised i.a. compliance with AML/CFT legislation, including internal routines and control, identity control and STR reporting</p>	<p>1. Please provide the No. of the MVTs The number of MVTs is 3 (1 agent representing MoneyGram and 2 agents representing Western Union).</p> <p>2. Do all the MVTs providers submit STRs? All the 3 providers submit STRs From January 1 until medio March 2009 the three agents reported respectively 320, 168 and 228 STRs to ØKOKRIM (FIU). The total number of STRs from all reporting entities for this period was 1 438.</p> <p>3. How long is the average cycle of on-site inspection to the MVTs providers? The FSA (Kredittilsynet) has since 2005 carried out thematic AML/CFT on-site inspections in the whole MVTs sector (the three agents representing MoneyGram and Western Union in Norway). The inspections comprised i.a. compliance with AML/CFT legislation, including internal routines and control, identity control and STR reporting routines. Considerable resources were allocated to this inspection program. If deemed necessary, the inspections will be followed-up. The FSA has not been informed of any major problems in handling AML/CFT issues by these providers. In addition to the on-site inspections provided by the FSA, the FIU and det Police Security Service (PST) are also visiting the MVTs in order to assess the activity and/or give information. The cooperation between the FSA, the FIU and the Police Security Service is fruitful.</p>

Forty Recommendations	Rating	Summary of factors underlying rating	Description of measures	Secretariat's comments / confirmation
			routines. Considerable resources were allocated to this inspection program. If deemed necessary, the inspections will be followed-up.	
SR VII Wire transfer rules	NC	<p>1. 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.</p> <p>2. 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.</p> <p>3. 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</p>	1-7. The deficiencies have been addressed by the implementation of regulation (EC) 1781/2006. The Regulation is implemented through the MLR Section 20. EC Regulation 1781/2006 aims to implement FATF SR VII. Supervision for compliance with reporting obligations under the Money Laundering regime is carried out by the FSA (Kredittilsynet), and in the case of breaches, administrative sanctions can be imposed.	

Forty Recommendations	Rating	Summary of factors underlying rating	Description of measures	Secretariat's comments / confirmation
		<p>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.</p> <p>4. 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.</p> <p>5. 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.</p> <p>6. 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.</p> <p>7. There are no sanctions for breaching many of the obligations under SR VII because many of the obligations themselves have not been implemented.</p>		
SR. VIII Non-profit organisations	NC	1. Norway has not yet carried out a review of the laws and regulations that relate to non-profit organisations (NPOs)	1 & 2. The Ministry of Justice conducted, in the spring of 2007, a review of laws and regulations which affects this area, cf. attachment. The review shows that a	1. Do these regulations for NPOs originally contain the AML/CFT aspects, or are the AML/CFT effects expected as the reflex of these regulations?

Forty Recommendations	Rating	Summary of factors underlying rating	Description of measures	Secretariat's comments / confirmation
		<p>that may be abused for the financing of terrorism.</p> <p>2. 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.</p> <p>3. The system is further weakened by the fact that Recommendation 5 has not been implemented with regards to beneficial ownership.</p>	<p><u>number of NPOs are subject to obligations of registration, auditing and control.</u> The Police Security Service were also consulted in the context of the review.</p> <p>In addition, from January 2008, <u>a new law for registering NPOs</u> has been made operational and over 10.000 NPO's have registered .</p> <p>3. Cf. response to Rec. 5. According to MLA Section 7 Paragraph 1 No 3 reporting entities are obliged to verify the identity of beneficial owners on the basis of reasonable measures. The term "beneficial owner" is defined in the MLA Section 2 Paragraph 1 No 3. According to the MLA Section 8 Paragraph 5 reporting entities shall also record data uniquely identifying beneficial owners.</p>	<p>These regulations does not originally contain AML/CFT aspects</p> <p>3. Does the new law cover all forms of voluntary organizations?</p> <p>The law covers a wide scope of voluntary organizations with different purposes. The registration procedures contains some specific requirements as regards the organisation of the NPO in question</p>
SR. IX Cash couriers	Cash PC	<p>1. 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</p>	<p>1. According to the <u>Regulation of 17 December 2008 No. 1502 to the Customs Act (RCA)</u> Section 3-1-2 each person that carries Norwegian and foreign banknotes, coins or a bearer of negotiable instruments above 25.000 NOK (approx. EUR 2.800) to and from the Customs area, shall declare the amount to the Customs officers. Any person that does not collaborate with the Customs officers can be penalized with fines or imprisonment pursuant to the Customs Act (CA) of 21 December 2007 No. 119 Section 16-5 Paragraph 1. On the same legal basis, a penalty for falsely declaring statements, information or documents, is in place, cf. CA Section 16-5 Paragraph 2.</p>	<p>Please provide the copy of this regulation.</p> <p>Regulation No 1502 of 17 December 2008 provides for a host of rules concerning customs and movement of goods. The Regulation is not translated to English. However, the relevant provision for the case at hand reads in unofficial translation:</p> <p><i>"§ 3-1-2 Duty to declare imported and exported means of payment</i></p> <p><i>Anyone that carries Norwegian or foreign banknotes and coins exceeding an amount of NOK 25 000 to or from the customs area shall declare or present these unsolicited to the custom authorities. Of the same standing as banknotes and coins are travellers' cheques and other cheques that can be paid to the bearer, bearer bills, bearer debentures or other physical securities whose rights can be exercised by the bearer".</i></p>

Forty Recommendations	Rating	Summary of factors underlying rating	Description of measures	Secretariat's comments / confirmation
		<p>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.</p> <p>2. The police and Prosecution Authority (including ØKOKRIM and the MLU) can only access the Currency Transaction Register after an investigation is started.</p> <p>3. 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, <u>lists of persons/entities designated pursuant to S/RES/1373(2001) are not.</u></p>	<p>2. The Currency Transaction Register Act of 28 May 2004 no. 29 Section 6 Paragraph 1 has been amended regarding the access to the Currency Transaction Register. It entered into force 15 December 2006. The police and Prosecution Authority has full access to the Currency Transaction Register at any time</p> <p>3. In the Norwegian regulations implementing S/RES/ 1267 (1999) into Norwegian legislation (Regulations relating to sanctions against Usama bin Laden, Al Qaida and the Taliban), there is included a link to the consolidated list on the UN web site, and consequently the Norwegian regulations are always fully updated. Further to that, The Ministry of Foreign Affairs duly forwards all notifications from the UN Secretariat on amendments to the list to all relevant authorities for informational purposes. Norway does not operate with a national list on terrorists and do not believe that there is an</p>	<p><i>Is a communication channel established / confirmed between the law enforcement authorities and the customs authorities for implementing the asset freezing measures under the S/RES/1373 as well?</i></p> <p>As stated in Norway's fourth follow up report, Norway does not operate with a national list on terrorists and does not believe that there is an obligation to do so following from S/RES/ 1373 (2001). Information about persons/entities designated by other jurisdictions pursuant to S/RES/1373 (2001) are not automatically given effect to, but the Norwegian regime allows the examination and use of the</p>

Forty Recommendations	Rating	Summary of factors underlying rating	Description of measures	Secretariat's comments / confirmation
			<p>obligation to do so following from S/RES/1373 (2001). <u>Information about persons/entities designated by other jurisdictions pursuant to S/RES/1373 (2001) is duly forwarded to relevant authorities, i.a. the customs authorities.</u></p>	<p>information after an individual assessment of each case. The Ministry of Foreign Affairs receives lists of designated persons and entities originating from other jurisdictions. The Ministry, in turn, distributes the lists to the relevant Norwegian Authorities, i.a. the customs authorities. The Criminal Procedure Act. Section 202 d authorizes the Police authorities to decide freeze of property belonging to persons suspected of terrorism or terrorism financing, any entity owned by the suspect or over which he has control, or any person or entity that acts on behalf of, or at the direction of the suspect, or such entity as mentioned. The decisions to freeze property are taken by the chief or the deputy chief of the Norwegian Police Security Service, or by a public prosecutor.</p>

ANNEX 2

SUPPORTING MATERIAL RECEIVED FROM NORWAY

TABLE OF CONTENTS

LIST OF SUPPORTING MATERIAL RECEIVED FROM NORWAY 81

MONAY LAUNDERING ACT (MLA) 82

MONEY LAUNDERING REGULATIONS (MLR) 92

PROPOSITION NO. 3 (2008-2009) TO THE ODELSTING (PARLIAMENT):
CONCERNING AN ACT RELATING TO COMBAT MONEY LAUNDERING
AND THE FINANCING OF TERRORISM, ETC. (MONEY LAUNDERING ACT) 99

REGULATIONS RELATING TO SANCTIONS AGAINST USAMA BIN LADEN,
AL-QAIDA AND THE TALIBAN 103

GUIDELINES CONCERNING THE OBLIGATIONS TO FREEZE ASSETS, E.G.,
RELATED TO TERRORISM 105

THE CRIMINAL PROCEDURE ACT (excerpts) 109

THE PENAL CODE (excerpts) 110

LIST OF SUPPORTING MATERIAL RECEIVED FROM NORWAY

1. Act relating to measures to combat money laundering and the financing of terrorism, etc. (Money Laundering Act).
2. Regulations concerning measures to combat money laundering and the financing of terrorism, etc.
3. Proposition No.3 (2008-2009) to the Odelsting: Concerning an Act relating to combat money laundering and the financing of terrorism, etc. (Money Laundering Act).
4. Regulations concerning the Supervisory Board for Measures to Combat the Laundering of the Proceeds of Crime.
5. The General Civil Penal Code.
6. The Criminal Procedure Act.
7. The Act on Customs Duties and Movements of Goods (Customs Act).
8. Regulations relating to sanctions against Usama bin Laden, Al-Qaida and the Taliban.
9. Proposition No.8 (2007-2008) to the Odelsting (Parliament).
10. Circular no. 13/2006: Legislation on Measures to Combat the Laundering of Proceeds of Crime – Guidance related to issues of particular importance for auditors and external accountants.
11. Guidelines concerning the obligations to freeze assets, *e.g.* related to terrorism.
12. A review of the non-profit sector in Norway.
13. Statistics – General Civil Penal Code Section 317.
14. Report on administrative sanctions (money laundering and terrorist financing) (**CONFIDENTIAL**).

ACT RELATING TO MEASURES TO COMBAT MONEY LAUNDERING AND THE FINANCING OF TERRORISM, ETC.

(Money Laundering Act)

Chapter 1. Introductory provisions

Section 1 *The purpose of the Act*

The purpose of the Act is to prevent and detect transactions associated with proceeds of crime or associated with acts of terrorism.

Section 2 *Definitions*

For the purposes of this Act, the following definitions shall apply:

1. entity with a reporting obligation: such person as is referred to in section 4,
2. transaction: any transfer, mediation, exchange or placement of assets,
3. beneficial owners: natural persons who ultimately own or control the customer and/or on whose behalf a transaction or activity is being carried out. A natural person shall in all cases be regarded as a beneficial owner if the person concerned:
 - a) directly or indirectly owns or controls more than 25 per cent of the shares or voting rights in a company, with the exception of companies that have financial instruments listed on a regulated market in an EEA state or are subject to disclosure requirements consistent with those that apply to listing on a regulated market in an EEA state,
 - b) exercises control over the management of a legal entity in a manner other than that referred to in (a),
 - c) according to statutes or other basis is the beneficiary of 25 per cent or more of the assets of a foundation, trust or corresponding legal arrangement or entity,
 - d) has the main interest in the establishment or operation of a foundation, trust or corresponding legal arrangement or entity, or
 - e) exercises control over more than 25 per cent of the assets of a foundation, trust or corresponding legal arrangement or entity.
4. trust and company service providers: natural and legal persons who provide one or more of the following services:
 - a) forming companies or other legal persons,
 - b) acting as a trustee or senior employee of a company, partner in a general partnership or limited partnership, or a similar position in relation to other legal persons,
 - c) providing business addresses, administrative addresses or postal addresses and related services for legal persons,
 - d) administering or managing a trust or corresponding legal arrangement,
 - e) acting as a shareholder for a third party, unless this is a company that has financial instruments listed on a regulated market in an EEA state or is subject to disclosure requirements consistent with those that apply to listing on a regulated market in an EEA state, or
 - f) arranging for other persons to act in positions referred to in (b), (d) and (e).

Section 3 *Geographical scope*

This Act applies to entities with a reporting obligation that are established in Norway, including branches of foreign undertakings.

This Act applies to Svalbard and Jan Mayen. The Ministry may in regulations provide that parts of this Act shall not apply to Svalbard and Jan Mayen and provide separate rules for these areas in order to promote the purpose of the Act.

Section 4 *Entities with a reporting obligation*

The Act applies to the following legal entities:

1. financial institutions,
2. Norges Bank (Central Bank of Norway),
3. e-money institutions
4. undertakings operating activities consisting of transfer of money or financial claims,
5. investment firms,
6. management companies for securities funds,
7. insurance companies,
8. undertakings operating as insurance intermediaries other than reinsurance brokers,
9. postal operators in connection with provision of insured mail services,
10. security registers, and
11. undertakings that operate deposit activities.

The Act also applies to the following legal and natural persons in the exercise of their professions:

1. state authorized and registered public accountants,
2. authorized external accountants,
3. lawyers and other persons who provide independent legal assistance on a professional or regular basis, when they assist or act on behalf of clients in planning or carrying out financial transactions or such transactions involving real property or movable property of a value exceeding NOK 40 000,
4. real estate agents and housing associations that act as real estate agents,
5. undertakings that, in return for remuneration, provide services corresponding to those referred to in (1) to (4),
6. trust and company service providers, and
7. dealers in movable property, including auctioneers, commission agents and the like, in connection with cash transactions of NOK 40 000 or more or a corresponding amount in foreign currency.

This Act also applies to undertakings and persons who perform services on behalf of or for persons as referred to in the first and second paragraphs.

When a lawyer acts as manager of a bankrupt's estate, the provisions laid down in sections 17, 18, 20, 21, 27 and 28 shall apply.

The Ministry may in regulations provide exceptions from one or more of the provisions of the Act in respect of certain entities with a reporting obligation. The Ministry may in regulations make one or more of the provisions of the Act applicable to dealers in movable property in connection with transactions in excess of specific thresholds when using specific types of payment instrument.

The Ministry may in regulations lay down rules further specifying who shall be subject to section 4, first and second paragraphs, and rules making the Act applicable to undertakings operating gaming activities, debt collection agencies, pension funds and intermediaries of shares in general partnerships and limited partnerships.

Chapter 2. Customer due diligence measures and ongoing monitoring

Section 5 *Risk-based customer due diligence measures and ongoing monitoring*

Entities with a reporting obligation shall apply customer due diligence measures pursuant to sections 6 to 13 and ongoing monitoring pursuant to section 14. Customer due diligence measures and ongoing monitoring shall be applied on the basis of assessment of the risk of transactions associated with proceeds of crime or offences subject to sections 147 a, 147 b or 147 c of the Penal Code, where risk is assessed on the basis of customer type, customer relationship, product or transaction.

Entities with a reporting obligation shall be able to demonstrate that the extent of measures carried out is adapted to the risk concerned.

Section 6 *Obligation to apply customer due diligence measures*

Entities with a reporting obligation shall apply customer due diligence measures in connection with

1. establishment of customer relationships,
2. transactions involving NOK 100 000 or more for customers with whom the entity with a reporting obligation has no established customer relationship,
3. suspicion that a transaction is associated with proceeds of crime or offences subject to section 147 a, 147 b or 147 c of the Penal Code, or
4. doubt as to whether previously obtained data concerning the customer are correct or sufficient.

The thresholds referred to in the first paragraph (2) shall be assessed collectively in respect of transactions carried out in several operations that appear to be associated with each other. If the transaction amount is not known when the transaction is carried out, the customer due diligence measures shall be applied as soon as the entity with a reporting obligation becomes aware that the threshold has been exceeded.

The Ministry may in regulations lay down further rules concerning when a customer relationship shall be deemed to be established.

Section 7 *Applying customer due diligence measures*

Customer due diligence measures as referred to in section 6 shall comprise

1. record keeping as referred to in section 8,
2. verification of the customer's identity on the basis of a valid proof of identity,
3. verification of the identity of beneficial owners on the basis of reasonable measures, and
4. gathering of information concerning the purpose and intended nature of the customer relationship.

If the customer is a legal person, the identity of the person acting on behalf of the customer shall be verified on the basis of a valid proof of identity. Documentation shall furthermore be provided in the form of a certificate of company registration, memorandum of association, written power of attorney or the like that the person concerned has the right to represent the customer externally.

If persons other than the customer have been granted a right of disposal over an account or a deposit, or have been granted the right to carry out the transaction, the identity of the persons concerned shall be verified on the basis of a valid proof of identity.

If a natural person's identity is to be verified on the basis of physical proof of identity without personal appearance by the person concerned, further documentation shall be presented to verify the person's identity.

Pursuant to the first paragraph (2), second paragraph and third paragraph, a natural persons' identity may be verified on a basis other than a valid proof of identity if the entity with a reporting obligation is sure of the person's identity.

The Ministry may in regulations lay down further rules concerning the application of customer due diligence measures including what is deemed valid proof of identity.

Section 8 *Record keeping*

Entities with a reporting obligation shall record the following data concerning customers:

1. full name or name of undertaking,
2. personal identity number, organization number, D-number or, if the customer has no such number, another unique identity code,
3. permanent address, and
4. reference to proof of identity used to verify the customer's identity.

The obligation to record the customer's permanent address pursuant to the first paragraph (3) shall not apply if the National Population Register has decided that the customer's address is to be classified as IN CONFIDENCE or STRICTLY IN CONFIDENCE.

In the case of natural persons who have not been assigned a Norwegian personal identity number or D-number, the date of birth, place of birth, sex and nationality shall be recorded. If the entity with a reporting obligation is aware that the customer holds dual nationality, this shall be recorded.

In the case of legal persons not registered in a public register, data shall be recorded concerning the form of organization and date of establishment as well as the name of the general manager, managing director, proprietor or corresponding contact person. If the contact person is a legal entity, a natural person shall also be registered as contact person and data as referred to in the first paragraph shall be recorded concerning the person concerned.

Entities with a reporting obligation shall record data unequivocally identifying beneficial owners.

Section 9 *Timing of customer due diligence measures*

Customer due diligence measures shall be applied prior to the establishment of a customer relationship or carrying out a transaction.

The following exceptions to the first paragraph shall apply:

1. It shall be possible to verify the identity of customers and beneficial owners during the establishment of a customer relationship if the establishment of the customer relationship is necessary so as to avoid the prevention of general business operations and there is little risk of transactions associated with crime or offences subject to section 147 a, 147 b or 147 c of the Penal Code.
2. Verification of the identity of the beneficiary of a life insurance policy may be conducted after the policy is taken out provided that verification of the identity is conducted prior to the time of payment or the time that the beneficiary exercises his or her rights according to the policy.
3. Verification of the identity of the customer and beneficial owners may be conducted after the opening of a bank account provided that measures exist to ensure that transactions associated with the account cannot be carried out by or on behalf of the customer before the identity is verified.

Section 10 *Consequences of the inability to apply customer due diligence measures*

If customer due diligence measures cannot be applied, entities with a reporting obligation shall not establish a customer relationship or carry out the transaction. An established customer relationship shall be terminated if continuation of the customer relationship entails a risk of transactions associated with proceeds of crime or offences subject to section 147 a, 147 b or 147 c of the Penal Code.

The first paragraph shall not apply when lawyers and other persons who provide independent legal assistance on a professional or regular basis are ascertaining a client's legal status or representing the client in legal proceedings.

Section 11 *Customer due diligence measures applied by third parties*

For the application of customer due diligence measures as referred to in section 7 (2) to (4), entities with a reporting obligation may rely on measures applied by the following third parties:

1. financial institutions,
2. investment firms,
3. management companies for securities funds,
4. insurance companies,
5. undertakings operating insurance mediation other than reinsurance brokerage,
6. security registers,
7. state authorized and registered public accountants,
8. authorized external accountants,

9. lawyers and other persons who provide independent legal assistance on a professional or regular basis, when they assist or act on behalf of clients in planning or carrying out financial transactions, transactions involving real property or transactions involving movable property of a value exceeding NOK 40 000,
10. real estate agents and housing associations that act as real estate agents, or
11. corresponding legal and natural persons as referred to in (1) to (4) and (6) to (10) from another state, provided these are subject to statutory registration requirements and rules concerning customer due diligence measures, the retention of documents and information and supervision pursuant to the provisions of this Act.

The right to rely on customer control measures applied by third parties pursuant to the first paragraph does not entail that the entity with a reporting obligation is exempt from

1. the obligation to record data as referred to in section 8 and to retain information and documents as referred to in section 22, or
2. the responsibility for ensuring that customer due diligence measures are applied in accordance with this Act and with regulations issued pursuant to this Act.

Entities with a reporting obligation may rely on customer due diligence measures applied by third parties not established in Norway, although verification of the customer's identity, cf. section 7, first paragraph (2), is conducted on a basis other than a valid proof of identity.

A third party shall make the data gathered for the application of measures as referred to in section 7 (2) to (4), available to the entity with a reporting obligation to which the customer is being referred. A third party shall, when so requested, immediately forward copies of identification and verification data and other relevant documentation on the identity of the customer or the beneficial owner to the entity with a reporting obligation. Disclosure of information and documents necessary to the entity with a reporting obligation in fulfilling its obligations pursuant to section 5, second paragraph, section 8 or section 22 shall not constitute a breach of statutory duty of secrecy when the customer is informed that the information will be disclosed.

The Ministry may in regulations provide exceptions from the right to rely on customer due diligence measures applied by third parties.

Section 12 *Outsourcing of the application of customer due diligence measures*

Entities with a reporting obligation may enter into written contracts with service providers concerning outsourcing of the application of customer due diligence measures.

The following legal and natural persons may function as service providers pursuant to the first paragraph:

1. entities with a reporting obligation, with the exception of trust and company service providers as referred to in section 4, second paragraph (6), and dealers in movable property as referred to in section 4, second paragraph (7), and
2. licensed postal operators.

The entity with a reporting obligation is responsible for ensuring that customer due diligence measures are applied in accordance with current statutes and regulations and that appropriate procedures and necessary measures are applied pursuant to section 23.

Disclosure of information and documents obtained by the service provider on the basis of outsourcing of the application of customer due diligence measures that are necessary to the entity with a reporting obligation in fulfilling its obligations pursuant to section 5, second paragraph, section 8 and section 22, shall not constitute a breach of statutory duty of secrecy.

The Ministry may in regulations provide that persons other than those covered by the second paragraph may function as service providers.

Section 13 *Simplified customer due diligence measures*

The Ministry may in regulations provide exceptions from the obligation to apply customer due diligence measures pursuant to section 6, first paragraph (1), (2) and (4) and second paragraph. Entities with a

reporting obligation shall before applying such exceptions obtain sufficient information to establish that the circumstances are covered by the exception concerned.

The first paragraph does not entail an exemption from the obligation to record data pursuant to section 8, first to third paragraph, in connection with the opening of an account.

Section 14 *Ongoing monitoring*

Entities with a reporting obligation shall conduct ongoing monitoring of existing customer relationships, and ensure that transactions they become aware of are consistent with their knowledge of the customer and its activities. Entities with a reporting obligation shall update documentation and information concerning customers.

Section 15 *Enhanced customer due diligence measures*

In situations that by their nature involve a high risk of transactions associated with proceeds of crime or offences subject to section 147 a, 147 b or 147 c of the Penal Code, entities with a reporting obligation shall on the basis of a risk assessment apply other customer due diligence measures in addition to the measures that follow from sections 5 to 14.

Entities with a reporting obligation shall have at their disposal appropriate customer due diligence measures to establish whether the customer is a politically exposed person. Entities with a reporting obligation shall, in connection with customer relationships with or transactions for such persons,

1. ensure that the decision-maker obtains approval from senior management before establishing a customer relationship,
2. take appropriate measures to ascertain the origin of the customer's assets and of the capital involved in the customer relationship or the transaction, and
3. carry out enhanced ongoing monitoring of the customer relationship.

By politically exposed person, as referred to in the second paragraph, is meant a natural person who

1. holds or during the last year has held a high public office or post in a state other than Norway,
2. is an immediate family member of a person as referred to in (1), or
3. is known to be a close associate of a person as referred to in (1).

Entities with a reporting obligation shall pay particular attention to products and transactions that might favour anonymity, and take measures if needed to prevent transactions associated with proceeds of crime or offences subject to section 147 a, 147 b or 147 c of the Penal Code.

The Ministry may in regulations lay down further rules concerning what situations shall be subject to the first paragraph and what control measures shall be applied in such cases. The Ministry may in regulations lay down further rules concerning who shall be deemed to be politically exposed persons.

Section 16 *Correspondent banking relationships*

In connection with the use of an institution in a state outside the EEA area as a correspondent bank, credit institutions shall

1. gather sufficient information concerning the correspondent institution to understand fully the nature of its activities and on the basis of publicly available information determine the reputation of the institution and the quality of supervision,
2. assess the correspondent institution's control measures for prevention and combating of acts as described in sections 317 and 147 b of the Penal Code,
3. ensure that the decision-maker obtains approval from senior management before establishing new correspondent banking relationships,
4. document the respective responsibilities of each institution, and
5. with respect to settlement accounts, ascertain that the correspondent institution
 - a) has verified the identity of and performs ongoing monitoring of customers having direct access to accounts at the credit institution, and

b) is able on request to provide relevant due diligence data to the credit institution. Credit institutions shall not enter into or continue correspondent bank relationships with shell banks. Credit institutions shall take appropriate measures to ensure that they do not engage in or continue correspondent banking relationships with credit institutions known to allow their accounts to be used by shell banks. By shell bank as referred to in the second paragraph is meant a credit institution incorporated in a jurisdiction in which it has no physical presence involving meaningful mind and management, and which is unaffiliated with a regulated financial group.

Chapter 3. Enquiries and reporting

Section 17 The obligation to make enquiries

If an entity with a reporting obligation suspects that a transaction is associated with proceeds of crime or with offences subject to section 147 a, 147 b or 147 c of the Penal Code, further enquiries shall be made in order to confirm or disprove the suspicion.

Entities with a reporting obligation shall in writing or electronically record the results of such enquiries. The Ministry may in regulations lay down further rules concerning the obligation to make enquiries.

Section 18 Obligation to report

If enquiries as referred to in section 17 fail to disprove the suspicion, the entity with a reporting obligation shall on its own initiative submit information to the National Authority for Investigation and Prosecution of Economic and Environmental Crime in Norway (Økokrim) concerning the transaction in question and the circumstances that gave rise to the suspicion. The entity with a reporting obligation shall, if so required, provide Økokrim with all necessary information concerning the transaction and the suspicion.

Lawyers and other persons providing legal advice either professionally or on a regular basis shall have no obligation to report information obtained in connection with work on ascertaining the legal status of a client or on information obtained before, during or after judicial proceedings when the circumstances to which the information applies are directly associated with the litigation. This shall apply correspondingly to public accountants and entities with a reporting obligation when they assist lawyers or other persons providing legal advice either professionally or on a regular basis as referred to in the first sentence.

The Ministry may in regulations order entities with a reporting obligation to submit information to Økokrim electronically. The Ministry may in regulations lay down further rules concerning the obligation to report.

Section 19 Suspicious transactions

The entity with a reporting obligation shall not carry out transactions entailing an obligation to report as referred to in section 18 before Økokrim has been notified. In special cases, Økokrim may order that such transactions shall not be carried out.

A transaction may nevertheless be carried out before notifying Økokrim if omission to carry out the transaction might impede Økokrim's enquiries or investigations or if it is not possible to omit carrying out the transaction. In such case, Økokrim shall be notified immediately after the transaction is carried out.

Section 20 Duty of secrecy

Communication of information to Økokrim in good faith pursuant to section 18 shall not constitute a breach of the duty of secrecy and does not provide a basis for compensation or penalties.

Financial institutions and insurance companies may notwithstanding the duty of secrecy exchange necessary customer data when this is deemed a necessary step in enquiries as referred to in section 17.

Section 21 Prohibition against disclosure of enquiries, reporting or investigations

Customers or third parties shall not be informed that enquiries are being conducted as referred to in section 17, that information has been provided as referred to in section 18 or that investigations are being carried out.

The first paragraph shall not preclude exchange of data as referred to in section 20, second paragraph.

The first paragraph shall not preclude entities with a reporting obligation as referred to in section 4, second paragraph (1) to (3), from attempting to persuade a client to refrain from committing an illegal act.

The Ministry may in regulations provide exceptions from the first paragraph.

Chapter 4. Retention of information and documents

Section 22 Retention of information and documents

Entities with a reporting obligation shall retain copies of documents used in connection with customer due diligence measures, as referred to in section 7, and recorded data, as referred to in section 8, for five years after the customer relationship has ended or following the carrying out of the transaction unless longer time limits follow from other statutes or regulations. If a qualified certificate is used, the identification code of the certificate and information concerning the identity of the certificate issuer shall be kept. By means of an account number or by other means, a unique connection shall be registered between the customer relationship and recorded data as referred to in section 8.

Entities with a reporting obligation shall retain documents associated with transactions as referred to in section 17 for a period of at least five years after the transaction is carried out.

Documents and information as referred to in the first and second paragraphs shall be kept securely, be protected against access by unauthorized persons and be destroyed within a year following expiry of the retention requirement. The Personal Data Act applies to the retention of personal data by entities with a reporting obligation.

The Ministry may in regulations lay down further rules concerning the means of retention and destruction of information.

Chapter 5. Internal procedures and systems, etc.

Section 23 Control and communication procedures

Entities with a reporting obligation shall have satisfactory internal control and communication procedures that ensure fulfilment of the obligations pursuant to this Act.

The procedures shall be established at the highest management level of the entity with a reporting obligation. A person in the management shall be assigned special responsibility for following up the procedures.

Entities with a reporting obligation shall apply the necessary measures to ensure that employees and other persons who perform tasks on behalf of the entity with a reporting obligation

1. are familiar with the obligations incumbent upon the entity with a reporting obligation pursuant to this Act,
2. learn to recognize transactions as referred to in section 17, and
3. are familiar with the internal routines of the entity with a reporting obligation for handling such transactions.

Section 24 Electronic surveillance systems

Financial institutions shall establish electronic surveillance systems.

The Ministry may in regulations order other entities with a reporting obligation to establish electronic surveillance systems and may lay down further rules concerning such systems.

Section 25 *Systems for overview of customer relationships*

Entities with a reporting obligation as referred to in section 4, first paragraph, shall have systems enabling rapid and complete responses to enquiries from Økokrim or supervisory authorities concerning whether during the last five years they have had customer relationships with specific persons and concerning the type of customer relationship.

Section 26 *Branches and subsidiaries in states outside the EEA area*

Entities with a reporting obligation as referred to in section 4, first paragraph, shall ensure that branches and subsidiaries established in states outside the EEA area

1. are familiar with control and communication procedures as described in section 23
2. apply corresponding measures for customer due diligence measures, ongoing monitoring and the retention of documents and information described in chapters 2 and 4.

If the law of the state concerned does not allow application of measures as referred to in the first paragraph (2), the entity with a reporting obligation shall:

1. inform the supervisory authority of this, and
2. apply other measures suitable for counteracting the risk of transactions associated with proceeds of crime or offences as described in section 147 a, 147 b or 147 c of the Penal Code.

Chapter 6. Final provisions

Section 27 *Orders and coercive measures*

Supervisory bodies may order an entity with a reporting obligation to put an end to matters that contravene this Act or provisions laid down pursuant thereto. Supervisory bodies may set a time limit for such matters to be brought into conformity with the order.

If the entity with a reporting obligation fails to comply with orders pursuant to the first paragraph, supervisory bodies may impose a coercive fine. The coercive fine may be imposed in the form of a single payment fine or a recurrent fine. Such a fine may be enforced by execution proceedings.

The Ministry may in regulations lay down further rules concerning the imposition of coercive fines, including the amount of such fines.

Section 28 *Penalties*

Any person who wilfully or with gross negligence contravenes or is accessory to contravening section 5, 6, 7, 8, 15, 17, 18 or 22 of this Act or regulations issued pursuant to these provisions shall be liable to fines.

In the case of particularly aggravating circumstances, imprisonment for a term not exceeding one year may be imposed.

Section 29 *Økokrim's handling of information*

Information received by Økokrim pursuant to section 18 shall be destroyed no later than five years after such information is recorded unless new information has been recorded or investigations or legal proceedings have been instituted against the registered person during this period.

If Økokrim's enquiries show that no criminal act has been committed, the information shall be destroyed as soon as possible.

The Ministry may in regulations lay down further rules concerning the procedures of Økokrim and the police associated with reports received, including destruction of information.

Section 30 *Exchange of information for combating of acts of terrorism, etc.*

Økokrim may provide information that it receives pursuant to section 18 to public authorities other than the police that have responsibilities associated with prevention of offences subject to section 147 a, 147 b or 147 c of the Penal Code.

Section 31 *Supervisory Board for Measures to Combat Money Laundering*

The Supervisory Board for Measures to Combat Money Laundering (the Supervisory Board) shall supervise:

1. Økokrim's handling of information received pursuant to section 18,
2. Økokrim's orders and authorizations pursuant to section 19, first paragraph, and
3. Økokrim's handling of information pursuant to section 29.

The Supervisory Board shall consist of at least three members who shall be appointed by the King. In addition, one or more deputies shall be appointed. The chairman of the board shall satisfy the requirements applicable to Supreme Court judges. The Supervisory Board's members shall treat as confidential information to which they gain access in the exercise of their duties.

Økokrim shall provide the Supervisory Board with the information, documents, etc. that the Supervisory Board finds necessary for its supervision. When so required by the Supervisory Board, Økokrim's officials are obliged to give evidence to the Supervisory Board without regard to the duty of secrecy.

The Ministry may in regulations lay down further rules concerning the responsibilities and procedures of the Supervisory Board.

Section 32 *Data that shall accompany a transaction in the payment chain, etc.*

The Ministry may in regulations lay down rules concerning what data concerning a remitter shall accompany a transaction in the payment chain, and rules concerning money transmitters' disclosure and due diligence obligations in connection with such transactions.

Section 33 *Persons or undertakings associated with countries or areas that have not implemented satisfactory measures*

The Ministry may in regulations lay down

1. special rules concerning reporting of transactions with or for persons or undertakings associated with countries or areas that have not implemented satisfactory measures to combat acts as described in sections 317 and 147 b of the Penal Code, and
2. prohibition against or restrictions as regards the right of entities with a reporting obligation to establish customer relationships with or carry out transactions with or for persons or undertakings associated with countries or areas that have not implemented satisfactory measures to combat acts as described in sections 317 and 147 b of the Penal Code.

Chapter 7. Commencement and amendments to other Acts

Section 34 *Commencement*

The Act shall enter into force on the date decided by the King.

The obligation to terminate customer relationships pursuant to section 10, first paragraph, shall apply only to customer relationships established after commencement of the Act.

Section 35 *Amendments to other Acts*

From the commencement of this Act, the following amendments shall take effect in other Acts:

1. Act of 20 June 2003 No 41 on measures to combat the laundering of proceeds of crime etc. (Money Laundering Act) shall be repealed.
2. In the Act of 24 May 1985 No. 28 on Norges Bank and the Monetary System (Central Bank Act), the following amendments shall be made:

section 12, second paragraph, shall read:

The duty of confidentiality pursuant to the preceding paragraph shall not apply to Kredittilsynet or to the central banks of other EEA states. Nor shall the duty of confidentiality pursuant to the preceding paragraph apply to Økokrim in respect of the provision of information pursuant to *section 18 of the Act relating to measures to combat money laundering and the financing of terrorism, etc. (Money Laundering Act)*.

REGULATIONS CONCERNING MEASURES TO COMBAT MONEY LAUNDERING AND THE FINANCING OF TERRORISM, ETC.

Laid down by the Ministry of Finance 13 March 2009 pursuant to sections 4, 6, 7, 12, 13, 15, 17, 18, 21, 22, 24, 29, 32 and 33 of the Act of 6 March 2009 No. 11 relating to measures to combat money laundering and the financing of terrorism, etc. (Money Laundering Act).

Chapter 1. Introductory provisions

Section 1. Scope

These Regulations shall apply to entities with a reporting obligation as referred to in section 4 of the Act [date and number] relating to measures to combat money laundering and the financing of terrorism, etc. (Money Laundering Act).

Chapter 2. Customer due diligence measures and ongoing monitoring

Section 2. Establishment of customer relationships

Customer relationships shall be deemed to be established when the customer can use the services of the entity with a reporting obligation, for example on the opening of an account or issue of a payment card.

State authorised and registered public accountants are deemed to have established a customer relationship when they have taken on an assignment involving consultancy or other services or have sent an auditor's declaration to the Register of Business Enterprises, cf. section 4-4 of the Act relating to the Registration of Business Enterprises.

Authorised external accountants are deemed to have established a customer relationship when they have concluded a written assignment agreement with a client or have taken on an assignment for which a written agreement is required, cf. section 3 of the Act relating to authorisation of external accountants.

Real estate agents when acting as real estate agents are deemed to have established a customer relationship with a client when they have taken on a sale or purchase assignment. In connection with an assignment to sell, the real estate agent shall in addition require the purchaser to present a valid proof of identity prior to settlement. The first and second sentence shall apply correspondingly to housing associations and lawyers that act as real estate agents, when the assignment concerns such activities.

Lawyers and other persons who provide independent legal assistance on a professional or regular basis are deemed to have established a customer relationship when they have taken on an assignment as referred to in section 4, second paragraph (3), of the Money Laundering Act. Lawyers and other persons who provide independent legal assistance on a professional or regular basis are in all cases deemed to have taken on an assignment as referred to in the first sentence when confirmation of acceptance of the assignment is received by the client.

Section 3 Special provisions concerning dealers in objects

Entities with a reporting obligation under section 4, second paragraph (7) of the Money Laundering Act shall apply customer due diligence measures pursuant to section 7 of the Money Laundering Act.

1. in connection with cash transactions of NOK 40 000 or more or a corresponding amount in foreign currency where it is suspected that a transaction involves the proceeds of crime or circumstances covered by the sections 147 a, 147 b or 147 c of the Penal Code, and
2. in connection with all transactions of NOK 100 000 or more or a corresponding amount in foreign currency, where NOK 40 000 or more or a corresponding amount in foreign currency is paid in cash.

Where transactions comprise a series of operations that appear to be interrelated, the threshold amount shall be calculated collectively.

Section 4 Lawyers and other persons who provide independent legal assistance on a professional or regular basis

For entities with a reporting obligation as referred to in section 4, second paragraph (3), of the Money Laundering Act, the provisions of the Money Laundering Act shall apply when entities with a reporting obligation assist or act on behalf of clients in:

1. planning or carrying out financial transactions
2. transactions concerning real property, and
3. transactions concerning objects paid for in cash of NOK 40 000 or more, or a corresponding amount in foreign currency.

Section 5. Physical proof of identity of natural persons

Valid proof of identity of a natural person is originals of documents that:

1. have been issued by a public authority or by another body that has adequate control routines for issue of documents, have a satisfactory level of security, and
2. contain the full name, signature, photograph and personal identity number or D-number.

In the case of natural persons who have not been assigned a Norwegian personal identity number or D-number, identity documents shall, in addition to the requirements laid down in the first paragraph, contain the date of birth, place of birth, sex and nationality.

If a natural person's identity shall be verified on the basis of physical proof of identity without the personal appearance of the person concerned in compliance with section 7, fourth paragraph, of the Money Laundering Act, certified copies of documents as referred to in the first and second paragraph may be used. The requirement that physical proof of the identity of natural persons shall contain a signature shall not apply to passports.

Section 6. Electronic proof of identity of natural persons

Valid proof of identity of natural persons is an electronic signature that fulfils the requirements of section 3 of the Regulations of 21 November 2005 No. 1296 concerning voluntary self-declaration arrangements for issuers of certificates, and which is included in a published list pursuant to section 11, first paragraph, of the Regulations referred to above.

Section 7. Physical proof of identity of legal persons

Valid proof of identity of a legal person registered in the Register of Business Enterprises is a certificate of registration not older than three months.

Valid proof of identity of a legal person registered in the Central Coordinating Register for Legal Entities, but not in the Register of Business Enterprises, is a transcript not older than three months from the Central Coordinating Register for Legal Entities containing all recorded information concerning the entity, cf. sections 5 and 6, second paragraph, of the Act relating to the Central Coordinating Register for Legal Entities.

Valid proof of identity of a legal person not registered in the Central Coordinating Register for Legal Entities but in another public register is a certificate or transcript from the register providing information of the name, address of the place of business or head office and any foreign organisation number. Such a certificate or transcript shall state which public register can confirm the information.

Valid proof of identity of a legal person not registered in a public register is:

1. documentation of the person's existence, and
2. a written declaration from a natural contact person, as referred to in section 8, fourth paragraph, of the Money Laundering Act, that the recorded information concerning the legal person is correct and valid proof of the identity of the person concerned.

Section 8. Subsequent retrieval of proof of identity

When verifying identity on the basis of valid proof of identity as referred to in section 7, fourth paragraph, for legal persons that shall be registered in the Register of Business Enterprises, entities with a reporting obligation shall require a certificate of registration to be produced within four weeks following expiry of the time limit for registration pursuant to section 4-1, first paragraph, of the Act relating to the Registration of Business Enterprises for the legal persons referred to there.

When verifying identity on the basis of valid proof of identity as referred to in section 7, fourth paragraph, for legal persons that shall be registered in the Central Coordinating Register of Legal Entities but not in the Register of Business Enterprises, entities with a reporting obligation shall require a transcript from the Central Coordinating Register of Legal Entities to be produced as referred to in section 7, second paragraph, within four weeks following the expiry of the time limit for registration in the Central Coordinating Register of Legal Entities pursuant to section 12 of the Act relating to the Central Coordinating Register for Legal Entities.

When verifying identity on the basis of proof of identity as referred to in section 7, fourth paragraph, of a legal person that shall be registered in another public register, entities with a reporting obligation shall require production of a certificate or transcript from the register providing information of the name, the address of the place of business or head office and any foreign organisation number within four weeks following registration in the register concerned, or within four weeks following the time limit for registration in the register where such a time limit applies.

For legal persons registered in the Register of Business Enterprises, the Central Coordinating Register of Legal Entities or other public register, entities with a reporting obligation shall demand valid proof of identity as referred to in section 7, first, second or third paragraph, to be produced within six months following establishment of the customer relationship.

If the requirements of this provision concerning subsequent retrieval of proof of identity are not complied with, the entity with a reporting obligation shall terminate the customer relationship.

Section 9 Outsourcing of execution of customer due diligence measures

In addition to the natural and legal persons who, pursuant to section 12 of the Money Laundering Act, may function as contractors, entities with a reporting obligation may enter into written agreements concerning outsourcing of execution of customer due diligence measures with undertakings and persons who perform such services for or on behalf of entities with a reporting obligation when such entities are part of the distribution system of the entities with a reporting obligation.

Section 12, third and fourth paragraph, of the Money Laundering Act shall apply correspondingly when the customer due diligence measures are outsourced to undertakings or persons as referred to in the first paragraph.

Section 10. Simplified customer due diligence measures

The obligation to apply customer due diligence measures pursuant to section 6, first paragraph (1), (2) and (4), of the Money Laundering Act shall not apply:

1. if the customer is a legal person as referred to in section 4, first paragraph, of the Money Laundering Act, with the exception of (4), (8) and (9), or an undertaking operating as an insurance intermediary,
2. if the customer is a legal person subject to article 2 (1) (1) and (2) of Directive 2005/60/EC or a corresponding legal person in a state outside the EEA area that imposes requirements corresponding to those laid down in Directive 2005/60/EC, and compliance with the requirements is supervised,
3. if the customer is a company that has financial instruments listed on a regulated market in an EEA state or is subject to disclosure requirements consistent with those that apply to listing on a regulated market in an EEA state,
4. if the customer is a Norwegian state or municipal administrative body,
5. in relation to recording of information concerning and verification of the identity of beneficial owners of accounts with funds from several persons held by lawyers or other independent legal professionals from EEA member states, or
6. in relation to recording of information concerning and verification of the identity of beneficial owners of accounts with funds from several persons held by lawyers and other independent legal professionals from third states, provided that:
 - a. they are subject to requirements regarding the combating of acts referred to in sections 317 and 147b of the Penal Code in accordance with international standards,
 - b. compliance with the requirements is supervised, and
 - c. information concerning the identity of beneficial owners is available on request to credit institutions that keep the accounts concerned.

The obligation to apply customer due diligence measures pursuant to section 6, first paragraph (1), (2) and (4) of the Money Laundering Act shall not apply to:

1. life insurance policies if the annual premium does not exceed EUR 1000 or if a single premium is no more than EUR 2500,
2. insurance policies for pension schemes if the policy does not contain a surrender clause and the policy cannot be used as collateral,
3. non-life insurance policies, including travel insurance policies and credit insurance policies,
4. schemes providing retirement benefits to employees, where contributions are made by way of deduction from wages and the scheme rules do not permit the assignment of a member's interest under the scheme, or
5. electronic money, provided that:
 - a. the maximum amount stored in the device is no more than EUR 150 and the device cannot be recharged, or
 - b. a limit of EUR 2 500 is imposed on the total amount transacted in a calendar year, except when an amount of EUR 1 000 or more is redeemed in that same calendar year.

Section 11. Politically exposed persons

By holder of high public office or post as referred to in section 15, third paragraph (1), of the Money Laundering Act is meant:

1. a Head of State, Head of Government, Minister or Deputy Minister,
2. a member of a national assembly,
3. a member of a higher court that takes decisions that only exceptionally may be appealed,
4. a member of the board of an auditor general, court of auditors or central bank,

5. an ambassador, chargé d'affaires or high-ranking military officer,
6. a member of an administrative, managerial or controlling body in a state-owned undertaking,
7. a holder of a corresponding office or post as referred to in (1) to (5) in an international organisation.

By immediate family member as referred to in section 15, third paragraph (2) of the Money Laundering Act, is meant:

1. a spouse or a partner who, pursuant to national legislation, is equivalent to a spouse,
2. a child,
3. a spouse or partner of a child, and
4. a parent.

By close associate as referred to in section 154, third paragraph (3) of the Money Laundering Act, is meant a natural person who is known to:

1. be a beneficial owner in a legal arrangement or entity jointly with a person as referred to in section 15, third paragraph (1) or (2) of the Money Laundering Act,
2. have a close business connection to a person as referred to in section 15, third paragraph (1) or (2), of the Money Laundering Act, or
3. be the only beneficial owner in a legal arrangement or entity that in reality was established for the benefit of a person as referred to in section 15, third paragraph, (1) or (2), of the Money Laundering Act.

Chapter 3. Enquiries and reporting

Section 12. Enquiries concerning suspicious transactions

Circumstances that may activate the obligation to make enquiries pursuant to section 17 of the Money Laundering Act include that the transaction seems to lack a legitimate purpose, is exceptionally large or complex, is unusual compared with the business or personal transactions commonly associated with the customer, is carried out to or from a customer in a country or area that lacks satisfactory measures to combat acts as referred to in sections 317 and 147b of the Penal Code or is in any other way unusual.

Section 13. Submission of information to Økokrim

The person assigned responsibility pursuant to section 23, second paragraph, of the Money Laundering Act shall be responsible for submission of information to the National Authority for Investigation and Prosecution of Economic and Environmental Crime in Norway (Økokrim) as referred to in section 18 of the Act.

Information provided pursuant to section 18 of the Money Laundering Act shall as far as possible contain a description of the basis for the suspicion, including information concerning the suspect, any third parties, any details of accounts and activity on accounts, information concerning the type and size of the transaction and whether the transaction has been carried out and to whom the funds are to be transferred and the origin of the funds. Relevant documents supplementing the information should be enclosed or forwarded separately.

Information shall be submitted electronically via AltInn¹. Should this not be possible, the information may be submitted by means of a standardised form prepared by Økokrim.

¹ Translator's note: AltInn is an Internet-based reporting channel enabling business enterprises and private individuals to submit information to Norwegian public agencies.

Section 14. Disclosure of enquiries, reporting or investigation

The prohibition against informing third parties that enquiries, reporting or investigations are being conducted pursuant to section 21 of the Money Laundering Act, shall not apply to:

1. communication of information to the public prosecution authority or the authority that supervises compliance with the Money Laundering Regulations by the entity with a reporting obligation.
2. exchange of information between legal persons that belong to the same group, as defined in section 1–3 of the Norwegian Accounting Act, where these are:
 - a. legal persons as referred to in section 4, first paragraph, with the exception of (4), (8) and (9) of the Money Laundering Act, or an undertaking operating as an insurance intermediary,
 - b. legal persons subject to article 2 (1) (1) or (2) of Directive 2005/60/EC, or
 - c. corresponding legal persons in a state outside the EEA area that imposes requirements corresponding to those laid down in Directive 2005/60/EC, and compliance with the requirements is supervised.
3. Exchange of information between persons who conduct their professional activities within the same legal person or network, where these are:
 - a. persons as referred to in section 4, second paragraph (1) to (3) of the Money Laundering Act or an undertaking that, in return for remuneration, provide corresponding services,
 - b. persons subject to article 2 (1) (3) (a) or (b) of Directive 2005/60/EC, or
 - c. corresponding persons in a state outside the EEA area that imposes requirements corresponding to those laid down in Directive 2005/60/EC.
4. Exchange of information between persons as referred to in (2) (a) to (c) or (3) (a) to (c) concerning a common customer in a transaction involving the person concerned, provided that corresponding obligations are imposed on such persons as regards the duty of secrecy and protection of personal data.

By network as referred to in the first paragraph (3), is meant a structure that has common ownership, management or internal control of compliance with relevant rules.

Information that is exchanged pursuant to the first paragraph (2), (3) and (4) may only be used for prevention of transactions associated with proceeds of crime or offences subject to section 147a 147b or 147 c of the Penal Code.

Section 15 Special reporting of transactions associated with countries or areas which have not implemented satisfactory measures against money laundering and financing of terrorism, etc.

The Ministry of Finance may in response to a decision by the Financial Action Task Force on Money Laundering (FATF) impose a special, systematic obligation to report to ØKOKRIM transactions with or on behalf of persons or undertakings associated with countries or areas which have not implemented satisfactory measures against the laundering of proceeds of acts as described in sections 317 and 147 b of the Penal Code.

Section 16 Prohibition of or restrictions on the right of entities with a reporting obligation to establish customer relationships with or undertake transactions to or from countries which have not implemented satisfactory measures against money laundering and financing of terrorism, etc.

The Ministry of Finance may in response to a decision by the Financial Action Task Force on Money Laundering (FATF) impose a special prohibition of or restrictions on the right of entities with a reporting obligation to establish customer relationships with or carry out transactions with persons or undertakings associated with countries or areas which have not implemented satisfactory measures against the laundering of proceeds of crime or acts described in sections 317 and 147 b of the Penal Code.

Chapter 4. Retention

Section 17. Retention of information

Copies of identity documents as referred to in sections 5 and 7 shall be marked “rett kopi bekrefte” [“certified true copy”] with the signature of the person who has applied the customer due diligence measures and the date the measures were applied.

Documents and information shall be retained in a medium that maintains legibility throughout the retention period.

Backup copies shall be kept of electronic material. The backup copy shall be stored separately from the original.

Chapter 5. Internal routines and systems, etc.

Section 18. Electronic surveillance systems

Financial institutions as referred to in section 4 , first paragraph (1), of the Money Laundering Act shall establish electronic surveillance systems for the purpose of identifying transactions that may be associated with proceeds of crime or offences subject to section 147a, 147b or 147 c of the Penal Code.

Kredittilsynet may by individual decision derogate from the first paragraph.

Chapter 6. Final provisions

Section 19. Procedures followed by Økokrim and the police

Økokrim shall prepare guidelines for its internal procedures in order to ensure adequate systems for receipt of information from entities with a reporting obligation and prevent access to such information by unauthorised persons.

The police shall keep entities with a reporting obligation informed of the status of the investigation of reported matters.

Section 20. Information on the payer accompanying a transaction in the payment chain

Annex IX No. 23d to the EEA agreement (Regulation (EC) No. 1781/2006) on information on the payer accompanying transfers of funds shall apply as regulations with the adjustments resulting from annex IX, protocol 1 of the Agreement and elsewhere in the Agreement.

Section 21. Commencement

These Regulations shall enter into force when so decided by the Ministry.

From the date these Regulations enter into force, the Regulations of 10 December 2003 No. 1487 concerning measures to combat money laundering of the proceeds of crime, etc. (Money Laundering Regulations) shall be repealed.

The obligation to terminate customer relationships pursuant to section 8 shall apply only to customer relationships established after the entry into force of these Regulations.

PROPOSITION NO. 3 (2008-2009) TO THE ODELSTING

CONCERNING AN ACT RELATING TO MEASURES TO COMBAT MONEY LAUNDERING AND THE FINANCING OF TERRORISM, ETC. (MONEY LAUNDERING ACT)

1 The main content of the Proposition

Money can now be transferred more easily and more rapidly than ever, both domestically and across national borders. This increases the demand for effective measures to combat money laundering and financing of terrorism. In this Proposition, the Ministry presents proposals designed to make it more difficult to make use of the financial system for the purposes of money laundering. The fight against money laundering and terror financing is an important element of the work on creating a more secure society and on curbing economic crime. The Bill is intended to ensure that Norway contributes to the international fight against money laundering and terror financing.

In this Proposition, the Ministry proposes a new Act relating to measures to combat money laundering and financing of terrorism to replace the current Money Laundering Act. The Bill provides for continued application of the key elements of the current Money Laundering Act, with the requirement that financial institutions and certain other undertakings shall conduct customer due diligence measures in accordance with the “know-your-customer principle”, and report suspicious transactions to ØKOKRIM. In relation to certain key issues, the Ministry proposes extending the measures against money laundering and the financing of terrorism in consistency with international obligations and recommendations, among other ways, by strengthening the “know-your-customer principle”.

In the Ministry’s assessment, the Bill pays due regard to the statutory requirement that the handling of personal data shall be carried out in a manner that does not unwarrantably violate major interests relating to protection of privacy.

The Bill is based on proposals presented in Official Norwegian Report NOU 2007:10 concerning measures to combat money laundering and terror financing. This report was submitted in August 2007 by a commission appointed by Royal Decree in November 2006.

According to the Bill, the Money Laundering Act shall be extended to include provisions concerning commercial providers of trust and company services. These include undertakings and persons whose activities consist of establishing companies for others, including those who offer services to Norwegian undertakings involving establishment of Norwegian Registered Foreign Companies (NUF). Undertakings and persons with a reporting obligation pursuant to the current legislation will also be subject to the new Act. These include financial institutions, investment firms, lawyers and accountants.

Denmark and France, among other countries, have exempted dealers in objects from the money laundering legislation and have instead introduced a prohibition against dealers receiving cash payments of amounts over EUR 15 000. In consistency with the Board’s assessment, the Ministry has concluded that such an arrangement should not be introduced in Norway before observing good experience of it in other countries. According to the Bill, dealers in objects will still be subject to the Money Laundering Act in connection

with cash transactions of NOK 40 000 or more. Out of regard for limiting the administrative burdens associated with the Act, the Ministry will not implement a proposal from the commission that dealers should be required to conduct customer due diligence measures in connection with all cash transactions over NOK 40 000. This shall still only apply in cases where the transaction is suspicious. Dealers will otherwise only be required to conduct customer due diligence measures in connection with transactions over NOK 100 000.

The Ministry proposes that the current rules concerning identification of customers be replaced by more extensive and detailed requirements regarding customer due diligence measures. At the same time, the requirements regarding customer due diligence measures should be adapted to the risk of money laundering and terror financing. In consistency with this, it is proposed that customer due diligence measures be both strengthened and simplified. According to the Bill, risk-based customer due diligence measures entail both the right and the obligation to assess the risk of money laundering and to adapt customer due diligence measures on the basis of such risk assessments. In view of personal privacy considerations, the Ministry rejects making general exceptions from the duty of secrecy in order to achieve more effective risk assessments in company groups. The proposal provides that customer due diligence measures may be conducted by specific third parties or be outsourced, and, within this framework, exchange of information and exceptions from the duty of secrecy will be allowed.

Requirements regarding strengthened due diligence measures are proposed in relation to “politically exposed persons” and correspondent banks⁸, among others. According to the proposal, “politically exposed persons” include natural persons who hold, or during the last year have held, a high public office or post in a state other than Norway, as well as immediate family members and persons known to be close associates of such persons. Further rules shall be provided in regulations. It is proposed that entities with a reporting obligation shall have access to suitable risk-based procedures for establishing whether a customer is a politically exposed person. Entities with a reporting obligation shall furthermore, in connection with customer relationships with or transactions for politically exposed persons, implement special due diligence measures, including ensuring that decision makers obtain the consent of their superiors before establishing customer relationships, and adopt appropriate measures to establish the origin of the customer’s assets and the capital involved in the customer relationship or transaction.

The Board proposes provisions requiring credit institutions to conduct strengthened due diligence measures in respect of correspondent banks. It is proposed, inter alia, that credit institutions shall assess the correspondent institutions’ due diligence measures for prevention and combating of money laundering and terror financing. It is further proposed that credit institutions be prohibited from entering into or maintaining correspondent bank relationships with shell banks, and that they shall take appropriate measures to ensure that they do not engage in or maintain correspondent banking relationships with financial institutions known to allow their accounts to be used by shell banks.

Exceptions are proposed from the requirements regarding customer due diligence measures (simplified customer due diligence measures) for customers who cannot in practice act under a false identity. The Bill provides for simplified customer due diligence measures, inter alia, if the customer is a financial institution, investment firm, management company for securities funds, insurance company, insurance broking undertaking or company whose financial instruments are listed on a regulated market in the EEA. This exception does not apply to the obligation to conduct customer due diligence measures on suspicion that a transaction is associated with money laundering or terror financing.

⁸ Unlike in the case of domestic payment transfers, it is not possible for a Norwegian bank to credit recipients in a foreign bank directly. Instead, the Norwegian banks must use accounts in foreign banks (correspondent banks). Payments are made with the help of correspondent banks, and are then transferred to the national payment systems.

According to the Bill, entities with a reporting obligation pursuant to the Money Laundering Act shall be obliged to conduct ongoing monitoring of existing customer relationships. Further customer due diligence measures shall be conducted if there is any doubt concerning the correctness and adequacy of any previously obtained information concerning the customer.

A new requirement is proposed that entities with a reporting obligation shall verify the identity of the person(s) who own or control the customer (beneficial owners). For example, when a limited company wishes to open an account or take up a loan, the bank must verify the identity of the shareholders who control the company.

It is proposed that it be provided that an entity with a reporting obligation may not establish a customer relationship or carry out transactions if customer due diligence measures cannot be conducted.

It is proposed that the requirements regarding the recording of information and verification of the identity of legal persons not registered in a public register be made more stringent.

In some cases, it may be more economical if entities with a reporting obligation can make use of customer due diligence measures conducted by other entities with a reporting obligation. For example, this may be appropriate when a customer has a customer relationship with a company in a financial group, and later wishes to establish a customer relationship with another company in the same group. There are also situations where a foreign company wishes to acquire a company in Norway, and engages a Norwegian auditing firm attached to an international auditing network for financial due diligence. It will then be natural for the Norwegian auditing firm to take contact with the auditing network's office in the country where the company is located in order to carry out customer due diligence measures. The Bill provides that customer due diligence measures may be conducted by specified third parties. Entities with a reporting obligation shall still have responsibility for customer due diligence measures conducted by such a third party, and it is required that information deriving from the customer due diligence measures shall be disclosed to the entity with a reporting obligation. The customer shall be informed of such disclosure of information.

The Ministry proposes that entities with a reporting obligation shall be able to enter into agreements with other entities with a reporting obligation whereby they can conduct customer due diligence measures on their behalf (outsourcing). The Ministry does not consider that it would be appropriate to allow outsourcing without restrictions, as proposed by the Board. It may however be appropriate to extend this access somewhat, and the Ministry proposes the extension of such access to postal operators holding public licenses. The Ministry proposes that there be access in regulations to provide for further extension.

It is proposed that it be provided that customer due diligence measures shall be conducted before establishing customer relationships or carrying out transactions. At the same time, some exceptions from this main rule are proposed in certain cases where subsequent verification is deemed adequate.

The Ministry stresses that provisions should be made for electronic customer identification without it being necessary for the customer to appear in person at the office of the entity with a reporting obligation in order to have his identity verified. According to the Bill, the customer's identity shall be verified on the basis of valid proof of identity. It is proposed that there shall be a power to issue regulations containing further rules concerning the conduct of customer due diligence measures including what shall be deemed to be valid proof of identity. It is envisaged that the specific requirements regarding valid electronic proof of identity will be laid down in regulations.

The Ministry proposes a statutory prohibition against informing customers or third parties that inquiries are being conducted, that information has been provided to ØKOKRIM or that investigations have been instituted. It is further proposed that there be exceptions from this prohibition, including exceptions in connection with communication of information to the prosecuting authorities and supervisory authorities,

and in connection with exchange of information between accountants, bookkeepers and lawyers within the same legal person or network.

The Bill implements EEA rules corresponding to Directive 2005/60/EC (Third Money Laundering Directive) and to certain associated Acts. In the Bill, the Ministry has also taken into consideration recommendations adopted by the Financial Action Task Force (FATF)⁹.

⁹ The FATF is the central international organisation involved in developing recognised recommendations for measures to combat money laundering and financing of terrorism. Norway is a member of the FATF, and has actively participated there for several years. See also 2.4.1.

REGULATIONS RELATING TO SANCTIONS AGAINST USAMA BIN LADEN, AL-QAIDA AND THE TALIBAN

Laid down by Royal Decree of 22 December 1999 pursuant to section 1 of the Act of 7 June 1968 No. 4 relating to the implementation of mandatory decisions of the United Nations Security Council. Submitted by the Ministry of Foreign Affairs.

§ 1. The following measures apply to Usama bin Laden, members of Al-Qaida and the Taliban, and any individuals, groups, undertakings and entities associated with them as referred to in the list compiled by the UN Al-Qaida and Taliban Sanctions Committee:¹⁰

1. Any funds and other financial assets or economic resources in Norway that belong to these individuals, groups or undertakings, or entities associated with them, shall be frozen. This includes any funds derived from property owned or controlled, directly or indirectly, by them or by persons acting on their behalf or at their direction. No funds, financial assets or economic resources shall be made available, directly or indirectly, for such persons' benefit.

2. It is prohibited for such individuals to enter or pass in transit through Norwegian territory. This does not apply to Norwegian nationals or where entry or transit is necessary for the fulfilment of a judicial process or the Al-Qaida and Taliban Sanctions Committee determines on a case-by-case basis that entry or transit is justified.

3. Any individual, group, undertaking or entity that is subject to a decision to freeze funds pursuant to this section may submit a request to the UN focal point for de-listing in accordance with UN Security Council resolution 1730 (2006).¹¹

¹⁰ The list of individuals and legal entities covered by the sanctions is to be found at the following address: <http://www.un.org/sc/committees/1267/consolist.shtml>.

¹¹ Resolution 1730 (2006) Adopted by the Security Council at its 5599th meeting, on 19 December 2006.

De-listing procedure:

The Security Council requests the Secretary-General to establish, within the Secretariat (Security Council Subsidiary Organs Branch), a focal point to receive de-listing requests. Petitioners seeking to submit a request for de-listing can do so either through the focal point process outlined below or through their state of residence or citizenship.¹

The focal point will perform the following tasks:

1. Receive de-listing requests from a petitioner (individual(s), groups, undertakings, and/or entities on the Sanctions Committee's lists).
2. Verify if the request is new or is a repeated request.
3. If it is a repeated request and if it does not contain any additional information, return it to the petitioner.
4. Acknowledge receipt of the request to the petitioner and inform the petitioner on the general procedure for processing that request.
5. Forward the request, for their information and possible comments to the designating government(s) and to the government(s) of citizenship and residence. Those governments are encouraged to consult with the designating government(s) before recommending de-listing. To this end, they may approach the focal point, which, if the designating state(s) so agree(s), will put them in contact with the designating state(s).
6. (a) If, after these consultations, any of these governments recommend de-listing, that government will forward its recommendation, either through the focal point or directly to the Chairman of the Sanctions Committee, accompanied by that government's explanation. The Chairman will then place the de-listing request on the Committee's agenda.

4.

- a) It is prohibited for Norwegian legal entities or any person who is present in Norwegian territory to sell, supply or transfer, directly or indirectly, arms and related materiel, including ammunition, military vehicles, military and paramilitary equipment and spare parts for the aforementioned, to such individuals, groups, undertakings or entities. The prohibition also applies to the use of vessels and aircraft registered in Norway.
- b) It is prohibited for Norwegian legal entities or any person present in Norwegian territory to sell, supply or transfer, directly or indirectly, technical assistance or training related to military activities to such individuals, groups, undertakings or entities.

5. In certain cases, the Al-Qaida and Taliban Sanctions Committee may grant exemptions from the prohibition set out in sub-paragraphs 1 and 2 on the grounds of humanitarian need, including religious obligations. With regard to the prohibition set out in sub-paragraph 2, the Al-Qaida and Taliban Sanctions Committee may grant exemptions on the grounds that the particular flight promotes discussion of a peaceful resolution of the conflict in Afghanistan or is likely to promote Taliban compliance with Security Council demands. Applications for such exemptions are to be submitted via the Ministry of Foreign Affairs.

6. The prohibition set out in sub-paragraph 2 does not apply to humanitarian flights to and from Afghanistan operated by or on behalf of government agencies or humanitarian organisations that appear on a list compiled by the Al-Qaida and Taliban Sanctions Committee.

7. Section 17b (4) of the Act of 4 August 1995 No. 53 relating to the police applies.

§ 2. The Ministry of Foreign Affairs is authorised to amend, suspend or repeal these regulations.

§ 3. These regulations enter into force immediately.

(b) If any of the governments, which were consulted on the de-listing request under paragraph 5 above oppose the request, the focal point will so inform the Committee and provide copies of the de-listing request. Any member of the Committee, which possesses information in support of the de-listing request, is encouraged to share such information with the governments that reviewed the de-listing request under paragraph 5 above.

(c) If, after a reasonable time (3 months), none of the governments which reviewed the de-listing request under paragraph 5 above comment, or indicate that they are working on the de-listing request to the Committee and require an additional definite period of time, the focal point will so notify all members of the Committee and provide copies of the de-listing request. Any member of the Committee may, after consultation with the designating government(s), recommend de-listing by forwarding the request to the Chairman of the Sanctions Committee, accompanied by an explanation. (Only one member of the Committee needs to recommend de-listing in order to place the issue on the Committee's agenda.) If after one month, no Committee member recommends de-listing, then it shall be deemed rejected and the Chairman of the Committee shall inform the focal point accordingly.

7. The focal point shall convey all communications, which it receives from Member States, to the Committee for its information.

8. Inform the petitioner:

(a) Of the decision of the Sanctions Committee to grant the de-listing petition; or

(b) That the process of consideration of the de-listing request within the Committee has been completed and that the petitioner remains on the list of the Committee.

GUIDELINES CONCERNING THE OBLIGATIONS TO FREEZE ASSETS, E.G.

RELATED TO TERRORISM

In the following Kredittilsynet provides some guidelines concerning the obligations to freeze funds, financial assets or financial resources related to terrorism.

The primary purpose of the obligations to freeze assets is to prevent the financing of terrorism. Financing of terrorism is a punishable offence pursuant to section 147 b, cf. section 147 a, of the General Civil Penal Code:

***Section 147 b.** Any person who obtains or collects funds or other assets with the intention that such assets should be used, in full or in part, to finance terrorist acts or any other contraventions of the provisions of section 147 a shall be liable to imprisonment for a term not exceeding 10 years.*

Any person who makes funds or other assets, or bank services or other financial services, available to any of the following shall be liable to the same penalty

- a) a person or enterprise that commits or attempts to commit any offence mentioned in section 147 a,*
- b) any enterprise owned or controlled by such a person or enterprise as is mentioned in a above, or*
- c) any person or enterprise that acts on behalf of or at the direction of such person or enterprise as is mentioned in (a) or (b) above.*

Any person who aids and abets such an offence shall be liable to the same penalty.

Added by the Act of 28 June 2002 no. 54.

***Section 147 a.** Any criminal act mentioned in section 148, 151 a, 151 b first paragraph, cf. third paragraph, 152 second paragraph, 152 a second paragraph, 152 b, 153 first to third paragraphs, 153 a, 154, 223 second paragraph, 224, 225 first or second paragraph, 231, cf. 232, or 233 is considered to be a terrorist act and is punishable by imprisonment for a term not exceeding 21 years when such an act has been committed with the intention of*

- a) seriously disrupting a function of vital importance to society, such as 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) unlawfully compelling public authorities or an intergovernmental organization to perform, tolerate or abstain from performing any act of substantial importance for the country or the organization, or for another country or other intergovernmental organization.*

No penalty less than the minimum penalty prescribed in the penal provisions mentioned in the first sentence may be imposed.

Any person who, with such intent as is mentioned in the first paragraph threatens to commit such criminal act as is mentioned in the first paragraph under such circumstances that the threat is likely to provoke serious intimidation shall be liable to imprisonment for a term not exceeding 12 years. If the threat has such consequences as are mentioned in the first paragraph (a), (b) or (c), a sentence of imprisonment for a term not exceeding 21 years may be imposed. Any person who aids and abets such an offence shall be liable to the same penalty.

Any person who plans or prepares such terrorist act as is mentioned in the first paragraph by conspiring with another person for the purpose of committing such an act shall be liable to imprisonment for a term not exceeding 12 years.

Added by the Act of 28 June 2002 no. 54, amended by the Act of 20 June 2003 no. 45 (came into force on 1 July 2003 pursuant to the Royal Decree of 20 June 2003 no. 712).

1. Information relating to the Regulations on sanctions against Usama Bin Laden, Al-Qaida and the Taliban of 22 December 1999 no. 1374 (“The Taliban Regulations”)

According to UN Security Council Resolution 1267 (1999) all states are obliged to freeze assets belonging to groups and individuals associated with the Taliban or al-Qaida.

Section 1 no. 1 of The Taliban Regulations implements this obligation into Norwegian law with respect to “*Funds and other financial assets or economic resources located in Norway and which belong to these persons, groups, enterprises or entities*” that are listed on the UN’s Sanctions Committee’s list. The UN’s Sanctions Committee’s list “the consolidated list” includes individuals and entities associated with Al-Qaida, Usama bin Laden and/or the Taliban. The consolidated list is included as a hyperlink in the web edition of the text of the Regulations on Lovdata (www.lovdata.no). The Taliban Regulations is consequently always up to date.

Kredittilsynet publishes notifications of amendments to the list, which it receives from the Ministry of Foreign Affairs, on www.kredittilsynet.no under “Lists issued by the UN and FATF and similar announcements”. These will normally be published within days after the actual amendment is made to the consolidated list.

According to Section 1 no. 1 of the Regulations, there is an obligation to immediately freeze the above-mentioned funds and assets, Kredittilsynet would therefore urge the financial institutions to monitor the list from the UN's Sanctions Committee through their electronic monitoring systems. The institutions must also work on developing real-time freezing functionality for transactions linked to persons and entities on the UN list.

Other listings of terrorist organisations received, e.g. from the US authorities and the EU Commission, do not trigger the obligations to automatically and immediately freeze assets pursuant to the Taliban Regulations. Such lists are however important indicators to the institutions that they might be dealing with suspicious transactions that normally would trigger the obligation to investigate and report pursuant to section 7 of the Money Laundering Act¹² and such transactions should as a minimum be subject to further monitoring and scrutiny.

The term “*Funds and other financial assets or financial resources*” in section 1 no. 1 of the Regulation’s text is very broad and Kredittilsynet assumes that in reality it covers all types of assets that are included in transactions executed in relation to customers and third parties. Freezing funds and other financial assets or financial resources is defined as preventing someone from having actual or legal control over assets. Typical examples of this include blocking access to a bank account, managed funds, or not performing or executing the transfer of a payment.

According to Section 1 no. 5 of the regulations, the al-Qaida and Taliban Sanctions Committee may grant exemptions from the obligation to freeze. This is done with regard to basic expenses necessary for subsistence by UN Security Council Resolution 1452.

¹² This reference refers to the previous MLA. Section 7 of the MLA 2003 correspond to the MLA 2009 Section 17 and 18.

The exemption for basic expenses includes, inter alia, funds for food, living expenses, medicines or medical treatment, taxes, insurance premiums, public duties, or expenses relating to necessary legal assistance in connection with the asset freezing order.

Proposition to the Odelsting no. 61 (2001-2002) pg. 61, first column, stipulates: *“that a decision to freeze a bank account should not prevent the bank from performing ordinary asset management. The purpose of the provision does not necessitate precluding the debiting of fees or crediting of interest to the account.”*

As far as the scope of the obligations to freeze assets is concerned, it may be natural to seek guidance from Proposition to the Odelsting no. 61 (2001-2002) pg. 59, second column:

“However, the Ministry maintains the proposal that the provisions concerning the freezing of assets ought to be general and not just directed at funds that have links to terrorist activities. Limiting the freezing of assets to apply to funds that are linked to terrorist activities would not be particularly effective because the suspect would then be able to use other assets to achieve the same goal.”

Even though this quote is from the preliminary legislative work on the obligations to freeze assets in chapter 15 b of the Criminal Procedure Act, see below, Kredittilsynet assumes that the same considerations apply here in relation to the obligations to freeze assets in the Taliban Regulations.

In the event of a freeze of assets pursuant to the Taliban Regulations, such measure should immediately be reported to the Ministry of Foreign Affairs, Legal Department, Section for International Humanitarian and Criminal Law. According to a case by case assessment The Financial Intelligence Unit of the Norwegian National Authority for Investigation and Prosecution of Economic and Environmental Crime (ØKOKRIM) can also be notified of this immediately as a suspicious transaction, cf. section 7 of the Money Laundering Act.¹³ Finally, Kredittilsynet should be informed promptly about measures involving the freezing of assets.

The Ministry of Foreign Affairs is responsible for these regulations. Questions concerning the understanding and implementation of the regulations should therefore be directed to the Ministry's, Legal Department, Section for International Humanitarian and Criminal Law.

2. Other obligations to freeze and confiscate assets related to terrorism

Under the UN Convention for the suppression of financing of terrorism and UN Security Council Resolution 1373 (2001) there is an obligation to freeze assets that can be linked to the commission of terrorist acts in general (that are not linked to al-Qaida and the Taliban). This obligation is implemented by chapter 15 b. “Freezing of assets” of the Act relating to legal procedure in criminal cases (“The Criminal Procedure Act”) of 22 May no. 25 1981. Such freezing of assets does not follow from any of the lists mentioned above, but from a special decision, made on a case by case basis, pursuant to section 202 d of the Criminal Procedure Act.

¹³ This reference refers to the previous MLA. Section 7 of the MLA 2003 correspond to the MLA 2009 Section 17 and 18.

3. Other obligations to freeze assets

Pursuant to Act of 7 June 1968 No. 4 relating to the implementation of mandatory decisions of the Security Council of the United Nations and Act of 27 April 2001 No. nr 14 relating to the implementation of other international non-military measures, the Ministry of Foreign Affairs has adopted regulations containing sanctions and restrictive measures. Some of these include obligations to freeze the assets of named persons and entities. An overview of these regulations can be found on Lovdata (www.lovdata.no) under regulations that fall under the Ministry of Foreign Affairs' responsibility.

The institutions are obliged to maintain an overview of the aforementioned obligations to freeze and confiscate, establish systems and routines that identify such transactions, and be able to implement without undue delay the necessary freezing and confiscation measures.

4. Useful background material, including preliminary legislative work, guidelines or the like concerning the obligations to freeze and confiscate assets.

Proposition to the Odelsting no. 61 (2001-2002) (White Paper related to measures against terrorism and terrorist financing).

The Financial Action Task Force (FATF) has stipulated 9 special recommendations on measures against terrorist financing. In this regard we especially refer to recommendation no. III "Freezing and confiscating terrorist assets". FATF has drawn up "International Best Practices" and an "Interpretative Note" for special recommendation no. III.

FATF has also produced the document "Terrorist Financing" dated 29 February 2008. The document contains examples, typologies and trends within terrorist financing.

This material is published on www.fatf-gafi.org.

THE CRIMINAL PROCEDURE ACT (Excerpts)

Chapter 15 b. Freezing of assets

Section 202 d. When any person is with just cause suspected of a contravention or attempt to contravene section 147 a or 147 b of the Penal Code, the head or deputy head of the Police Security Service, or a public prosecutor, may decide to freeze any assets belonging to

- a) the suspected person
- b) an enterprise that the suspect owns or controls, or
- c) an enterprise or a person that acts on behalf of or on the instructions of any person specified in (a) or (b).

Assets that are necessary for the maintenance of the person to whom the decision is directed, his household or any person whom he maintains, may not be frozen.

The decision shall be in writing, shall identify the suspect and briefly describe the grounds for the decision.

Section 202 e. The prosecuting authority shall as soon as possible, and not later than seven days after it has made a decision pursuant to section 202 d, bring the case before the District Court, which will by order decide whether the decision shall be affirmed. Section 149, first paragraph, of the Courts of Justice Act shall apply correspondingly. If the court affirms the decision, it shall at the same time determine a specific time-limit for the freezing of the assets. Section 185, first paragraph, shall apply correspondingly. Before the court makes the order, the suspect and other persons concerned in the case shall be notified and given an opportunity to express their views.

If it is strictly necessary in regard to the investigation, the court may decide that notice as specified in the first paragraph shall be omitted and the giving of information about the order deferred. In this case the court shall in the order set a time-limit for when information shall be given. The time-limit shall not exceed four weeks but may be extended by a court order by up to four weeks at a time. When the time-limit expires, the suspect and other persons concerned in the case shall be informed of the order and that they may require the court to decide whether the freezing of assets shall be affirmed.

Section 202 f. If the court decides to freeze assets pursuant to section 202 d, the prosecuting authority shall as soon as possible consider whether there are grounds for seizing or creating a charge on the assets cf. chapters 16 and 17. If the conditions for freezing the assets are no longer fulfilled, such freezing shall be terminated without undue delay. The freezing of assets shall at the latest cease when the case is decided by a final and binding judgment.

Section 202 g. The prosecuting authority may order persons other than those specified in section 122, first and second paragraphs, to provide assistance necessary for freezing assets. If an application is to be made for deferment of the giving of information pursuant to section 202 e, second paragraph, the prosecuting authority may order persons other than those specified in section 122, first and second paragraphs, to keep secret the decision to freeze assets until deferment of the giving of information is granted. When the duty of secrecy has ceased, the prosecuting authority shall as soon as possible notify any person who has been so ordered.

THE PENAL CODE (Excerpts)

Chapter 14. Felonies against public safety

Section 147 a. Any criminal act mentioned in section 148, 151 a, 151 b first paragraph, cf. third paragraph, 152 second paragraph, 152 a second paragraph, 152 b, 153 first to third paragraphs, 153 a, 154, 223 second paragraph, 224, 225 first or second paragraph, 231, cf. 232, or 2331 is considered to be a terrorist act and is punishable by imprisonment for a term not exceeding 21 years when such act has been committed with the intention of

a) seriously disrupting a function of vital importance to society, such as 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) unlawfully compelling public authorities or an intergovernmental organization to perform, tolerate or abstain from performing any act of substantial importance for the country or the organization, or for another country or another intergovernmental organization.

No penalty less than the minimum penalty prescribed in the penal provisions mentioned in the first sentence may be imposed.

Any person who, with such intent as is mentioned in the first paragraph, threatens to commit such criminal act as is mentioned in the first paragraph under such circumstances that the threat is likely to provoke serious intimidation shall be liable to imprisonment for a term not exceeding 12 years. If the threat has such consequences as are mentioned in the first paragraph (a), (b) or (c), a sentence of imprisonment for a term not exceeding 21 years may be imposed. Any person who aids and abets such an offence shall be liable to the same penalty.

Any person who plans or prepares such terrorist act as is mentioned in the first paragraph by conspiring with another person for the purpose of committing such an act shall be liable to imprisonment for a term not exceeding 12 years.

Section 147 b. Any person who obtains or collects funds or other assets with the intention that such assets should be used, in full or in part, to finance terrorist acts or any other contraventions of the provisions of section 147 a shall be liable to imprisonment for a term not exceeding 10 years.

Section 147 c. Any person who makes funds or other assets, or bank services or other financial services, available to any of the following shall be liable to the same penalty

a) a person or enterprise that commits or attempts to commit any offence mentioned in section 147 a.

b) any enterprise owned or controlled by such person or enterprise as is mentioned in a above, or

c) any person or enterprise that acts on behalf of or at the direction of such person or enterprise as is mentioned in (a) or (b) above.

Any person who aids and abets such an offence shall be liable to the same penalty