FATF

Anti-money laundering and counter-terrorist financing measures

Norway

Mutual Evaluation Report

December 2014

The Financial Action Task Force (FATF) is an independent inter-governmental body that develops and promotes policies to protect the global financial system against money laundering, terrorist financing and the financing of proliferation of weapons of mass destruction. The FATF Recommendations are recognised as the global anti-money laundering (AML) and counter-terrorist financing (CFT) standard.

For more information about the FATF, please visit the website: **www.fatf-gafi.org**

This document and/or any map included herein are without prejudice to the status of or soverignty over any territory, to the delimitation of international frontiers and bounderies and to the name of any territory, city or area.

Citing reference:

FATF (2014), *Anti-money laundering and counter-terrorist financing measures - Norway,* Fourth Round Mutual Evaluation Report, FATF.
www.fatf-gafi.org/topics/mutualevaluations/documents/mer-norway-2014.html

Photocredits coverphoto: ©Thinkstock

Contents

Executive Summary

1. This report provides a summary of the anti-money laundering / counter-terrorist financing (AML/CFT) measures in place in Norway as at the date of the on-site visit 27 March 2014 to 11 April 2014. It analyses the level of compliance with the 2012 FATF 40 Recommendations and the level of effectiveness of Norway's AML/CFT system, and provides recommendations on how the system could be strengthened. The evaluation was prepared on the basis of the 2013 FATF Methodology.

A. Key Findings

- Although a national risk assessment – the first of its kind in Norway – has been published, **information on and analysis of, money laundering (ML) risks in Norway is incomplete and further work is needed to identify and understand the risks, including with respect to relevant predicate offences. Information on, and the assessment of, terrorist financing (TF) risks is much stronger**.
- **The lack of overarching national policies and strategies for AML/CFT and the lack of a policy-level coordinating mechanism have caused a number of shortcomings**, which exacerbate the limited and variable understanding of the risks. At an operational level, considerable informal and *ad hoc* cooperation is taking place and has value, but this is not sufficient to offset the lack of formal coordination mechanisms.
- **Use of financial intelligence differs significantly between competent authorities.** The National Authority for Investigation and Prosecution of Economic and Environmental Crime (ØKOKRIM) and the Norwegian Police Security Service (PST) use it effectively to 'follow the money' in criminal investigations of predicate offences, while its use in the 27 police districts and the National Criminal Investigation Service (KRIPOS) and the National Authority for Prosecution of Organised and Other Serious Crime (NAST) has limitations, and the Financial Intelligence Unit (FIU) experiences challenges in getting police to use FIU disseminations. The FIU's analytical capability functions well, but is hampered by the low quantity and quality of suspicious transaction reports (STRs) received.
- Norway has a good legal foundation and sound institutional structure for investigating and prosecuting ML, and for seizing and confiscating criminal proceeds. However, **investigation and prosecution of ML is not a high priority, primarily due to the focus on the predicate offence, thus leading to few ML prosecutions and convictions.** Limited confiscation results have been achieved, and further information is required to determine why the system is less effective than it should be.

- **Appropriate action is being taken to detect and disrupt TF in line with the identified risks, but weaknesses exist regarding targeted financial sanctions.** There is a solid legal framework in relation to the United Nations (UN) Taliban/Al Qaida sanctions, but there are serious deficiencies relating to the mechanism to designate entities and freeze assets pursuant to United Nations Security Council Resolution (UNSCR) 1373 as required by Recommendation 6, which undermines their ability to use targeted financial sanctions as an effective tool to combat TF.
- **Norway has taken significant measures to implement proliferation financing (PF) sanctions. However, effectiveness is undermined by delays in transposition of designations into Norwegian law and a lack of supervision of the sanctions implementation by reporting entities**.
- **Limited action has been taken since 2009 to update laws and other measures, particularly for preventive measures, and this is a priority for enhancing compliance and effectiveness.** The ML Act and Regulations, as well as guidance, needs updating and supplementing. Basic AML/CFT measures are being implemented, but effectiveness is variable, with banking and some designated non-financial businesses and professions (DNFBP) sectors being stronger. There is a need for a stronger application of risk-based approach (RBA), and for all sectors to more effectively implement the full range of preventive measures.
- **The Financial Supervisory Authority (FSA) conducts limited AML/CFT supervision, mostly in the context of prudential and business conduct supervision.** However, the frequency, scope and intensity of supervision are not sufficient, nor are they sufficiently based on ML/TF risk. Moreover, it is focused on technical compliance checklists rather than on the effectiveness and robustness of the preventive measures implemented. **Serious breaches of basic compliance have been identified.** However, the authorities do not have a wide enough range of powers to sanction, including no power to impose administrative fines, and **no sanctions other than written warnings have been applied to financial institutions**.
- **There is an extensive and transparent system of registers on legal ownership and control.** However, competent authorities are not able to get timely access to accurate and up-to-date beneficial ownership information of Norwegian companies when there are foreign legal persons/arrangements involved.
- **Norway takes an open and collaborative approach to international cooperation** and has demonstrated a substantively effective system of international cooperation.

B. Risks and General Situation

2. Information on ML risks in Norway is incomplete and further work needs to be done to better identify and understand ML/TF risks. Law enforcement agencies have produced threat assessments focused on predicate crime types which could assist. A national risk assessment has been published however this has significant shortcomings, as described in more detail below. Based on the available information, proceeds of crime and associated ML risks are primarily derived from domestic and foreign drug trafficking and organised crime, and fraud and other economic crimes such as bribery and tax offences. There is limited information on the nature and scope of cross border ML, though there is significantly more cash being taken out of Norway than is being brought in. More work needs to be done to assess the main ML trends, but initial findings suggest that frequently used methods include: use of cash, purchase and sale of real estate, and the assistance of professional facilitators. Money or value transfer service (MVTS) providers, both authorised and unauthorised, have been identified as an important vulnerability.

3. Information on, and assessment of, TF risks is much stronger. Norwegian authorities consider that Islamist extremist groups pose the greatest risk for terrorism and TF. Intelligence suggests that extremist groups use small scale domestic collections to fund militant Islamist groups in their former home regions. It is a concern that individuals linked to these groups in Norway travel abroad to participate in their activities. Organised left-wing and right-wing extremist groups or individuals also pose a threat.

C. Findings on Compliance and Effectiveness

C.1 Assessment of risk, coordination and policy setting

4. **The authorities do not have a sufficient understanding of ML risks**. National AML policies responses are not based on a proper understanding of risk, while the manner and extent to which various authorities implement their AML/CFT priorities based on risk, varies considerably. Norway published a National Risk Assessment (NRA) in February 2014, which is its first comprehensive ML/TF risk assessment. Prior to this, ML risks had only been considered to a limited extent in agency-level assessments of various crime types, though **the PST had assessed TF risks in a more comprehensive manner**. There were significant shortcomings in the NRA process and methodology, and gaps in inputs and areas covered. For example, few government agencies were fully engaged in the process, which has resulted in challenges concerning the acceptance of the findings of the NRA. As a result, this was not a comprehensive ML/TF risk assessment and it is limited in its usefulness as a firm basis for setting a national AML/CFT policy and setting risk mitigation priorities.

5. The understanding of ML/TF risks in Norway varies between authorities. The FIU and PST have a better understanding of the ML/TF risks which have informed their respective operational policies. However, the AML priorities of law enforcement agencies are driven by their understanding of risks associated with predicate offences. The AML/CFT activities and objectives of the FSA are not configured to a satisfactory degree to mitigate the ML/TF risks, and Norway has not taken sufficient action to ensure that financial institutions, DNFBPs and other sectors are aware of the ML/TF risk profile in Norway.

6. AML/CFT responsibilities are divided between ministries, led by the Ministry of Finance and Ministry of Justice, and other competent authorities. However, a particular concern is that **Norway does not have overarching national policies or strategies to combat ML/TF and there is no AML/CFT coordination mechanism at a national level, though coordination for TF and PF is noticeably stronger**. The approach to AML has been based around agency level threat and risk assessments of economic crimes which do not prioritise ML risks. Responsibilities are fragmented and there is no clear and consistent recognition of the importance of AML/CFT across competent authorities. At an operational level, considerable informal and *ad hoc* cooperation is taking place and has value. However, this is not sufficient to achieve an effective AML/CFT system and does not overcome the lack of formal coordination mechanisms.

7. Other than STR data, Norway does not maintain comprehensive statistics on issues related to AML. Comprehensive statistics were not available for this assessment, including on ML investigations, prosecutions

and convictions; the number and value of assets restrained, seized and confiscated; and on international cooperation. This hinders the ability of authorities to assess ML/TF risks and to establish evidence-based AML/CFT policies in response to the identified risks.

C.2 Money laundering and the use of financial intelligence

8. The use of the FIU's financial intelligence differs significantly between competent authorities. ØKOKRIM and the PST use it to effectively to 'follow the money' in criminal investigations, while its use in the 27 police districts and KRIPOS/NAST is limited, and the FIU experiences challenges in getting police to use FIU disseminations. Norway is seeking to address this by facilitating further engagement between the FIU and the police districts through the *Round Norway* initiative. **Norway has a well-functioning FIU** which develops and disseminates good quality financial intelligence based on STRs, various government registries, police information and the currency database. However, the FIU's strong analytical capability is undermined somewhat by the low quality of STRs received. In addition, the FIU has not undertaken strategic analysis since 2011 which has undermined authorities' ability to identify emerging threats.

9. Norway has a **good legal foundation and sound institutional structure for combatting ML**. ØKOKRIM handles the most significant ML cases related to economic crime and the 27 police districts also have responsibility for investigating ML through their economic crime units. The KRIPOS and NAST have important responsibilities for the investigation and prosecution of ML cases in relation to organised crime. These designated law enforcement agencies (LEAs) adopt a 'follow the money' approach and have access to a generally broad range of powers for financial investigations including ML cases.

10. **A fundamental concern is that the investigation and prosecution of ML is not prioritised by competent authorities.** Decisions not to investigate or prosecute ML are mostly due to the approach taken by all LEAs to investigate and prosecute the predicate offence rather than ML, combined with a lack of expertise and resources in the police districts. As a result, there are relatively few ML prosecutions and convictions, and many are self-laundering cases. It is not clear that the sentences applied in practice are dissuasive.

11. Norway has a strong legal framework for the freezing, seizing and confiscation of criminal proceeds. However, despite authorities making confiscation a policy priority, results are not satisfactory. There is a lack of statistics regarding freezing and seizing, and the data that is available for confiscation shows a steady decline in the amounts confiscated, which are also quite low in absolute terms. There are only a limited number of good examples of successful significant confiscation cases. Overall it is difficult to determine why the system is less effective than it should be. From the available data and qualitative information, and as confirmed by the authorities, it is clear that the **confiscation results achieved are less than Norway expected and significant improvements are necessary**.

C.3 Terrorist financing and proliferation financing

12. **Norway has a sound understanding of the TF risks it faces, and is taking action to detect and disrupt TF in line with the identified risks.** The PST produces assessments on terrorism including its financial aspects. The MFA also collects and shares information on TF risk with the larger Norwegian NGOs operating in high risk areas. However, while the operational agencies possess a sound understanding of TF risks, there is little co-ordination with the FSA and the information is not used by the FSA.

13. **Norway is focusing its investigative resources and international cooperation efforts into a small number of investigations related to terrorism and potential TF charges, based on TF risk.** Norway has only had one TF prosecution, which did not lead to a conviction. However, this seems to be generally in line with the TF risks in the country. The FIU and PST work closely together and use of financial intelligence is integrated into all of PST's investigations.

14. **Some action has been taken to prevent terrorists from raising, moving and using funds. However, the effectiveness of targeted financial sanctions is undermined by the limitations in the mechanism used to implement targeted financial sanctions pursuant to UNSCR 1373 as required by Recommendation 6**. Norway has a generally sound legal framework for targeted financial sanctions pursuant

to the Taliban/Al Qaida sanctions. Banks have a good awareness of the freezing obligations and implement measures. The poor implementation by financial institutions of beneficial ownership requirements as part of customer due diligence (CDD), and the varied and limited implementation outside the banking sector impact on effectiveness. Norway's mechanism to implement targeted financial sanctions pursuant to UNSCR 1373 as required by Recommendation 6 has serious deficiencies as it can only be used as part of an ongoing criminal investigation and does not establish a prohibition on the provision of funds to persons subject to a freezing action under this mechanism. This undermines Norway's ability to use targeted financial sanctions as an effective tool to combat TF. Despite this, in several cases, Norway has taken alternative action to secure terrorist funds using confiscation and charging provisions. Finally, Norway has taken a targeted approach and effectively prevents misuse of Norwegian non-profit organisations (NPOs) that are responsible for the bulk of overseas NPO activity.

15. **Norway has taken significant measures to implement targeted financial sanctions relating to proliferation of weapons of mass destruction**. Financial institutions have frozen funds of designated persons, and others operating on their behalf, under this framework. However, **the effectiveness of the use of targeted financial sanctions to combat proliferation financing is negatively impacted by the delays in transposing designations into Norwegian law, as well as a lack of supervision**. Although the delays are mitigated to some extent by the fact that some financial institutions monitor UN lists (as encouraged to do by FSA guidance) and have frozen funds prior to transposition into Norwegian law. Norway also implements EU sanctions, which means in effect that it has already implemented targeted financial sanctions for new UN designations which are previously on EU lists. Implementation outside the banking and insurance sectors is varied and limited, and the lack of supervision for all reporting entities is a concern with the only action taken being one questionnaire to the banking sector.

C.4 Preventive measures and supervision

16. **While significant enhancements were made to the preventive measures regime in 2009, Norway has not taken the necessary steps to update the regime since.** The AML/CFT legislation remains out of step with the 2012 FATF Recommendations and limited guidance has been provided to the private sector since 2009. The requirements for ML/TF risk assessments are not clearly understood and reporting entities do not have a well-developed understanding of risk. Some sectors, such as banking have a better understanding of the criminal threats to which they are exposed, but understanding of risk in other parts of the financial sector, and by DNFBPs, is weak. While some sectors have implemented AML/CFT measures, significant weaknesses exist regarding the implementation of key preventive measures such as beneficial ownership, politically exposed persons (PEPs), wire transfers, correspondent banking and ongoing monitoring. Concerns exist over the quantity and quality of STRs which predominately relate to cash-based transactions.

17. The FSA is responsible for the supervision of reporting entities, with the exception of lawyers which come under the purview of the Supervisory Council for Legal Practice (a self-regulatory body). The supervisors do not adequately understand ML/TF risks. The FSA uses a combination of off-site and on-site supervision, carried out by sectoral supervisors primarily as a part of their prudential or other supervision. While some targeted AML/CFT supervision has taken place, **the frequency, scope and intensity of such supervision is not sufficient, nor is it sufficiently ML/TF risk based, and generally requires considerable enhancement, particularly for large complex institutions.** The FSA's supervision is focused on technical compliance checklists rather than on the effectiveness and robustness of the preventive measures implemented. There are also particular concerns with the level of AML/CFT supervision in other sectors (such as MVTS, securities and legal sectors) and certain activities (such as targeted financial sanctions and wire transfers). Overall, the limited level of supervision means that AML/CFT measures remain untested in many areas.

18. It is also a concern that **compliance with targeted financial sanctions has not been reviewed or discussed as part of on-site visits**, and has not formed a part of any supervisory work outside the banking sector. The FSA has not considered whether the measures taken are sufficient, and has only undertaken limited off-site supervision through questionnaires.

19. The FSA is aware that compliance with AML/CFT measures is not at the level it should be in several areas and has identified serious breaches. However, **no sanctions have been applied to financial institutions other than warnings**. The FSA does not have a wide enough range of powers to sanction (e.g., no power to impose administrative fines), and the sanctions available to authorities for AML/CFT breaches (that is, coercive fines and prosecutions), have not been applied. The only sanctions applied to financial institutions are in the form of letters advising entities of concerns which should be addressed. In some cases, advanced warnings have been issued which indicate that coercive fines will be initiated if concerns are not addressed within a specified time period.

C.5 Transparency and beneficial ownership

20. **Norway has not comprehensively assessed the ML/TF risks associated with legal persons and arrangements**. The information available indicates that there is a real risk that legal persons are misused to launder criminal proceeds. Foreign trusts are used in Norway and cases were provided in which the proceeds of crimes committed in Norway were laundered using trusts. There is no information on the degree to which trusts are being misused.

21. **Norway has an extensive system of registers on legal ownership and contro**l, which assists in preventing misuse and obtaining beneficial ownership information. There is considerable transparency regarding legal persons, with much of it available to not only competent authorities but also reporting entities and the general public, which helps strengthen the system.

22. **Competent authorities are able to access significant beneficial ownership information in a timely manner when only Norwegian entities are involved**, as they can follow the chain of ownership to a natural person. All Norwegian legal persons, and foreign companies conducting business activities in Norway, are obliged to register with the Bronnoysund Register Centre (BRC). Norway also requires all companies to maintain a register of shareholders which must be made available to any person on request. Other sources of basic and beneficial ownership information, including information held by the Tax Authority and in the Register of Company Accounts, are publicly available. The various registers include information on persons exercising control, including their personal identity numbers, which are cross-checked against the population register. Authorities access information in the registers by using their own IT systems and upon request. There are also private websites which aggregate a range of information from the various registers (including information on ownership and control, financial returns, and links between companies and individuals) and make it publicly available at no cost. Despite this, concerns exist regarding the accuracy of the information as the BRC is largely passive and reactive, and most information is not checked for accuracy.

23. However, **where foreign companies are involved, for example by owning shares in Norwegian companies, beneficial ownership information is not contained in the various registers, and is not available in a timely manner**. When authorities seek information about a Norwegian entity that has foreign ownership, they either have to ask the foreign entity, check registers in the home country, or seek international cooperation to determine the foreign entity's chain of ownership. While there have been successful criminal cases where the competent authorities have been able to trace the beneficial owner of a foreign company, this is not common, and this was cited by authorities as an area of difficulty.

24. Legal arrangements cannot be created under Norwegian law. However, foreign trusts are used in Norway, and authorities do not have timely access to beneficial ownership information on trusts.

C.6 International Cooperation

25. **Norway takes an open and collaborative approach to international cooperation. Cooperation between Norway and its Nordic partners is close, uncomplicated and dealt with speedily.** This includes cooperation through the use of Nordic arrest warrants, which are forwarded directly between the competent judicial authorities. Norwegian LEAs are very involved in cooperation with European Economic Area (EEA) countries under the EU framework for cooperation, including for ML, predicate offences and TF. Formal cooperation between Norway and non-EEA countries is also working well, based on a legal framework for mutual legal assistance and extradition that is generally broad. With respect to other forms of cooperation,

the FIU, LEAs and the Customs Authority are well engaged, both upon request and spontaneously. Norway does not maintain comprehensive statistics on *MLA* and extradition which makes it difficult to assess the effectiveness of their international cooperation. Despite this, based on qualitative information, Norway has shown that it has a substantively effective system of international cooperation.

D. Priority Actions

26. The following outlines the prioritised recommended actions for Norway based on the findings of this mutual evaluation:

- ***Assessment of risk, coordination and policy setting***

1. Norway should commence work as soon as possible on a more robust NRA, with full engagement by all relevant stakeholders, to comprehensively assess ML/TF risks, and disseminate the findings within government and the private sector.

2. Norway should then develop national AML/CFT policies based on ML/TF risks, and improve coordination, including by establishing a strategic level national coordination platform.

3. Norway should maintain comprehensive statistics on AML issues to inform the risk assessment and support evidence-based policy making.

- ***Money laundering and the use of financial intelligence***

4. Law enforcement agencies should prioritise and give investigative focus to further utilise financial intelligence and the ML offence to target organised crime, tax offences, foreign proceeds of crime and other high threat areas.

5. The police districts and KRIPOS/NAST should enhance their use of financial intelligence.

6. Norwegian police and prosecution authorities should continue to prioritise the confiscation of proceeds of crime and examine the chain of action to determine why actions to confiscate criminal proceeds are not effective.

- ***Terrorist financing and proliferation financing***

7. Norway should develop national policies to use targeted financial sanctions to combat TF and PF including by:

   - establishing a mechanism to implement all aspects of targeted financial sanctions pursuant to UNSCR 1373 as required by Recommendation 6;
   - removing delays in transposition of designations for PF sanctions into Norwegian law; and
   - undertaking monitoring of reporting entities for compliance with the targeted financial sanctions.

- ***Preventive measures and supervision***

8. Norway should update the MLA to ensure that AML/CFT preventive measures are consistent

with the FATF 2012 Recommendations.

9. Norway should establish a stronger, clearer and more comprehensive requirement for reporting entities to assess ML/TF risk and to implement preventive measures on a risk-sensitive basis.

10. Norway should enhance its AML/CFT supervision and ensure its future supervision is undertaken on the basis of ML/TF risk.

11. Supervisors should ensure that AML/CFT deficiencies identified during examinations lead to supervisory actions that are dissuasive, proportionate and effective.

- ***Transparency and beneficial ownership***

12. Norway should take measures to ensure that beneficial ownership information of Norwegian legal entities is available when they are owned by foreign entities.

13. Obligations (and associated sanctions) should be imposed on trustees of foreign trusts to disclose their status to reporting entities.

Table 1. Effective Implementation of Immediate Outcomes

Effectiveness

1. Risk, Policy and Coordination — Moderate

- Norway has not sufficiently identified and assessed ML risks, and does not have a sufficient understanding of ML risks. This is demonstrated by the significant shortcomings in the NRA, which has limited usefulness as a firm basis for setting a national AML/CFT policy.
- Norway does not have overarching national AML/CFT policies.
- Current AML activities are not sufficiently being carried out on the basis of ML risk.
- Norway does not have a mechanism for the coordination of AML activities at a policy level and operational level mechanisms are not effective. Coordination and cooperation is very limited at the policy level while at the operational level, mostly informal, *ad hoc* cooperation is taking place on ML.
- Norway has, in large part, properly identified, assessed and appears to have understood the TF risks, and allocated resources to address a number of priorities, with the exception of CFT-related supervision.
- Coordination and cooperation on combatting TF and PF is more effective, both at the formal and informal level.
- There have only been limited and *ad hoc* efforts to raise awareness of ML risks among reporting entities.
- Norway does not maintain comprehensive statistics on AML which limits the ability of authorities to assess the risks and establish evidence-based policies.

2. International Cooperation — Substantial

- Norway does not maintain comprehensive statistics on mutual legal assistance and extradition, nor on other forms of international cooperation (other than by the FIU), which creates difficulties in assessing effectiveness with respect to ML/TF cases.
- Norway has a strong commitment to international cooperation and prioritises the provision of international assistance.
- Norway cooperates effectively, and in a timely way, particularly with Nordic and EU countries, including direct cooperation between the competent authorities.
- With respect to other forms of cooperation the FIU, LEAs and the Customs Authority engage in effective international cooperation with their counterparts, both upon request and spontaneously.
- Norway has a sound legal framework in place to allow the FSA to exchange information with foreign counterparts in the financial sector. However, the FSA makes limited use of international information exchange for AML/CFT matters. It has provided information upon request for AML/CFT purposes in specific cases.

Effectiveness

3. Supervision — Moderate

- Licensing, market entry and regulation of financial institutions are generally comprehensive.
- ML/TF risks have not been adequately identified and or understood by the FSA and SRBs.
- The FSA is the AML/CFT supervisor for all financial institutions and DNFBPs which are reporting entities in Norway, with the exception of the lawyers which is the Supervisory Council, and trust and company service providers (TCSPs) and dealers in precious metals and stones which do not have a designated supervisor.
- The FSA undertakes both on and off-site AML/CFT supervision, based largely on prudential and business conduct risks. The frequency, scope and intensity of AML/CFT supervision are not sufficiently ML/TF risk based and requires enhancement, particularly for large complex institutions.
- The FSA and Supervisory Council generally undertake only high level on-site supervision that does not adequately test the effectiveness of controls, rather focusing on technical compliance checklists.
- Taking into account the risks of the sector, concerns exist over the lack of on-site supervision in the authorised MVTS sector, and the lack of supervision of "passported" MVTS is a significant concern[1]. Action has been taken to identify and sanction unauthorised MVTS providers, led by the FIU, though this is on an *ad hoc* basis and could be improved.
- Systems, procedures and specialised supervisory resources are not sufficient to support effective, risk-based AML/CFT supervision.
- The FSA's feedback and guidance on AML/CFT requirements has been insufficient to address knowledge gaps on some core issues.
- Although the FSA is aware that compliance is not at a level that it should be (and in some cases serious breaches have been identified), the sanctions that are legally available to the authorities, including coercive fines or prosecutions, (which have technical limitations) have not been imposed and no regulations on the amount of fines have been issued.
- There is only very limited supervision of targeted financial sanctions requirements, and the FSA has not considered the adequacy of the systems used by reporting entities.

4. Preventive Measures — Moderate

- While significant enhancements were made to the preventive measures regime in 2009 to better align with the 2003 FATF Recommendations, Norway has not taken the necessary steps to update the regime since then. As a result, a number of legislative deficiencies remain with respect to the preventive measures, which have a negative impact on effectiveness.

1 'Passported MVTS providers' refers to agents of MVTS providers authorised by other EEA countries, operating in Norway, in line with the EU Payment Services Directive. For a description see Chapter 5.

Effectiveness

- Basic AML/CFT obligations are generally well understood only in certain sectors, such as the banking, audit, accounting and real estate sectors.
- Significant compliance gaps have been identified by the Norwegian authorities across a number of sectors and the implementation of some key preventive measures has not been effective in the identification and mitigation of ML/TF risks.
- Financial institutions and DNFBPs do not have a well-developed understanding of risk or the scope and depth of measures required to mitigate varying ML/TF risks. Some sectors, such as banking, understand the criminal threats to which they are exposed, but the requirement for a ML/TF assessment is not clearly understood and is not widespread. Understanding of risk in other parts of the financial sector is weak, particularly for DNFBPs.
- Weaknesses exist over the necessary CDD measures required to understand beneficial owners, particularly where foreign ownership is involved, which undermines effectiveness.
- Concerns exist over the application of preventive measures in some key areas such as PEPs, wire transfers and correspondent banking.
- Ongoing monitoring and periodic review requirements have not been effectively implemented.
- Concerns exist over the quantity and quality of STRs.

5. Legal Persons and Arrangements — Moderate

- The NRA notes but does not analyse the vulnerabilities that exist regarding the potential for misuse of legal persons in Norway, and does not consider the risks from trusts.
- Norway has an extensive system of readily accessible registers on legal ownership and control information, with information publicly available.
- Where ownership/control is entirely Norwegian, basic information (control information in national registers and ownership information held by companies) is readily available to competent authorities in a large majority of cases.
- Beneficial ownership information of Norwegian legal persons is not readily available where there are foreign legal persons or arrangements involved in the ownership/control structure.
- The company registry system is passive and reactive, with little active monitoring and limited sanctions.
- Trusts cannot be created under Norwegian law (thus likely reducing the ML/TF risks they pose in Norway given the fewer number), but trustees and/or beneficiaries of foreign trusts do exist. Neither competent authorities nor reporting entities have timely access to beneficial ownership information on foreign trusts operating in Norway.

Effectiveness

6. Financial Intelligence — Moderate

- The FIU undertakes good quality operational analysis based on a range of information sources. However, the FIU's analytical capability is further limited by the rather low quantity and quality of the STRs received.
- The FIU and PST work closely together to develop financial intelligence on TF.
- The FIU has not undertaken any strategic analysis since 2011, which undermines the ability of authorities to identify emerging threats.
- ØKOKRIM and the PST extensively use financial intelligence in their investigations, including the use of FIU intelligence products, albeit mostly for investigations of predicate offences. However, the use of this product in the police districts and by other law enforcement bodies such as KRIPOS is limited, and mostly aimed at predicates.

7. ML Investigation and Prosecution — Moderate

- Norway has well developed financial investigative and prosecutorial capacities, however ML cases have not been prioritised and the number of ML investigations and prosecutions is low. The shortage of reliable and comprehensive statistics about ML investigations, prosecutions and confiscations makes it difficult to get a complete picture of the situation.
- ML is investigated and prosecuted to a limited extent, and prosecutors and investigators concentrate on predicate offences. This is mostly because, in line with the drafting of the legislation, the prosecutors and investigators view ML as an offence which is ancillary to the predicate offence.
- The police districts rarely handle ML cases, which is to some extent due to many districts not having the capacity and resources to deal with them.
- It is not clear that the sanctions applied by the courts for ML are dissuasive.

8. Confiscation — Moderate

- The shortage of reliable and comprehensive statistics about proceeds of crime, assets seized or frozen, the number and amount of confiscation orders and amounts recovered, makes it difficult to get a complete picture of the situation to determine why the system is not as effective as it could be.
- LEAs and prosecutors have not effectively used confiscation and related measures.
- Even though the confiscation of criminal proceeds is a policy priority, results with respect to confiscation are inadequate. The amounts confiscated by the police have declined, and significant improvements are necessary.
- The level of confiscation varies considerably between LEAs and is relatively low. It is a concern that the number and value of confiscation orders made by KRIPOS/NAST, responsible for serious drugs and organised crime cases, are negligible.

Effectiveness

- The system for cross border cash and bearer negotiable instruments (BNI) declarations has only produced limited outputs relative to the risks in this area.

9. TF Investigation & prosecution — Substantial

- Investigative resources and international cooperation efforts are focussed on conducting a small number of terrorism and TF investigations, based on their understanding of TF risks. The use of financial intelligence is integrated into all of the PST's investigations.
- Norway has had one TF prosecution which did not lead to a conviction; however this appears to be generally in line with TF risks.
- The PST has taken some other criminal justice measures to disrupt TF activities where it is not practicable to secure a TF conviction.

10. TF Preventive measures & financial sanctions — Moderate

- Banks understand their obligations relating to targeted financial sanctions for TF. However, implementation outside the banking sector is varied and limited.
- Across all sectors the effectiveness of screening is undermined by limited implementation by reporting entities regarding verification of beneficial ownership and related CDD measures.
- Norway is unable to use all aspects of targeted financial sanctions as an effective tool to combat TF, beyond the UN Taliban/Al Qaida sanctions, due to the serious technical deficiencies in the mechanism which is intended to implement targeted financial sanctions pursuant to UNSCR 1373 as required by Recommendation 6.
- Norway has taken action using asset confiscation and charging provisions in a few cases to secure terrorist funds during investigations and for confiscation.
- Norway has recognised the TF risk profile for NPOs and has taken steps to effectively implement a targeted approach to the part of the sector responsible for the bulk of overseas NPO activity.

11. PF Financial sanctions — Moderate

- Norway has taken significant measures to implement targeted financial sanctions for PF and there have been a number of cases of asset freezing related to Iran sanctions which demonstrates their effectiveness.
- The banking and insurance sectors generally understand their obligations relating to targeted financial sanctions for PF and have frozen bank accounts of designated persons. However, implementation outside these sectors is varied and limited.
- The lack of supervision for all reporting entities is a concern, as the FSA has not considered the adequacy of the systems used by reporting entities.

Effectiveness

- There is strong coordination and cooperation between competent authorities on PF, although this does not include engagement with the FSA.
- The delays in transposing designations into Norwegian law undermine Norway's ability to use targeted financial sanctions as a tool to combat PF. However, the delays are mitigated to some extent by financial institutions which monitor UN lists (as encouraged to do so by the FSA's guidance) and have frozen funds prior to transposition into Norwegian law. Norway also implements EU sanctions, which means that it has already implemented targeted financial sanctions for new UN designations which have been previously on EU lists.
- Across all sectors the effectiveness of screening is undermined by poor implementation by reporting entities regarding verification of beneficial ownership and related CDD measures.

Table 2: Compliance with FATF Recommendations

Compliance with FATF Recommendations

Recommendation		Rating	Factor(s) underlying the rating
1.	**Assessing risks & applying a risk-based approach**	PC	• Norway has not pursued a comprehensive process to assess current ML risks and develop a shared understanding of those risks. • There are significant shortcomings in the NRA's assessment of ML/TF risks, although TF risk has been assessed in PST assessments. • The mechanism used to develop the NRA did not co-ordinate actions to assess risks. • The mechanisms to share ML/TF risk information with reporting entities are insufficient. • The allocation of resources is not linked to ML/TF risks, other than for operational CFT activities. • Exemptions from AML/CFT requirements are permitted, and simplified measures may be permitted (it is unclear) but this is not based on an assessment of risk, and the preconditions regarding risk have not been demonstrated. • Supervisors do not ensure that financial institutions and DNFBPs are implementing their obligations to assess and mitigate their risks. • The requirement on reporting entities to keep risk assessments updated is only partially and implicitly met, and there is no mechanism that ensures that risk assessment information held by reporting entities is provided to competent authorities and SRBs. • There is no requirement that internal controls relating to risk be monitored.
2.	**National cooperation and coordination**	PC	• Norway does not have overarching national AML/CFT policies informed by the risks identified. • Agency level priorities are not sufficiently informed by ML risk. • Norway does not have a coordination mechanism that is responsible for national AML policies and priorities. • Norway does not have adequate mechanisms in place to enable the various authorities at an operational level to cooperate and coordinate on AML.

Compliance with FATF Recommendations

Recommendation		Rating	Factor(s) underlying the rating
3.	**Money laundering offence**	C	
4.	**Confiscation and provisional measures**	LC	• There is no mechanism to manage property that has been seized, whether before or after a confiscation order has been made.
5.	**Terrorist financing offence**	LC	• The collection of funds in the intention that they are to be used (for any purpose) by a terrorist organisation or an individual terrorist is not criminalised as a stand-alone offence.
6.	**Targeted financial sanctions related to terrorism & TF**	PC	• Norway has implemented only certain aspects of targeted financial sanctions pursuant to UNSCR 1373, as required by Recommendation 6, as the terrorist asset freezing mechanism under the Criminal Procedure Act (CPA) can only be used as part of an ongoing criminal investigation and does not establish a prohibition from making funds available to persons subject to a freezing action under this mechanism.
7.	**Targeted financial sanctions related to proliferation**	PC	• Designations under the relevant UNSCRs are not implemented without delay. • The FSA has adopted only very limited measures to monitor and ensure compliance with the targeted financial sanctions by financial institutions and DNFBPs.
8.	**Non-profit organisations**	LC	• NPOs that are not in receipt of public funding are not required to implement controls and standards for NPOs • There is a lack of proportionate and dissuasive sanctions for violations of the standards for NPOs.
9.	**Financial institution secrecy laws**	LC	• It is not clear in what circumstances reporting FIs can share CDD information, particularly within financial groups.

Compliance with FATF Recommendations

Recommendation		Rating	Factor(s) underlying the rating
10.	**Customer due diligence**	PC	• For occasional wire transfers between 1 000 EUR and 15 000 EUR there is no requirement to identify and verify the identity of the beneficial owner behind the payer (customer). • The process for certifying copies of original identity documents has limited safeguards in place to ensure the reliability of the information. • No clear obligation for reporting FIs to have a broad understanding of a customer's business and its ownership and control structure. • Customers that are listed public companies in EEA states (and other equivalent countries) are exempt from CDD requirements. There are no requirements to ensure that there is adequate transparency regarding beneficial ownership of such companies. • While Norwegian law does not recognise trusts, trustees of foreign trusts may operate in Norway, and the CDD requirements only cover beneficiaries with a defined/vested interest above 25%. • There are no CDD requirements regarding the beneficiaries of life or investment related insurance policies, nor in relation to any beneficial owners standing behind the beneficiary. • The FSA guidance creates exceptions to the requirement to conduct CDD before or during the establishment of the relationship e.g., for PEPs, which are not in line with the FATF Standards. • CDD on existing customers is not required to be conducted on the basis of materiality and risk. • Simplified CDD is allowed, but the defined categories of "simplified CDD" are in fact exemptions from CDD, and the preconditions for such exemptions have not been demonstrated. • Relationships can be continued even when it has not been possible to conduct adequate CDD. • No provision that allows reporting FIs not to perform CDD in situations where the customer would be tipped off.

Compliance with FATF Recommendations

Recommendation		Rating	Factor(s) underlying the rating
11.	**Record keeping**	LC	• Records of analysis conducted are retained only for five years after the transaction is conducted, and not five years after the termination of a business relationship as required.
12.	**Politically exposed persons**	PC	• The definition of foreign PEP is too narrow as it is restricted to people who have held high public office in the past year, which is not in line with a RBA. • The requirements for foreign PEPs in the MLA do not include PEPs that are the beneficial owners of individual customers. • The measures relating to international organisation PEPs are limited as it only covers positions in international organisations that correspond to government positions listed. The list of government positions does not correspond well to the concept of senior management positions in an international organisation. • There are no measures relating to domestic PEPs. • The inclusion of family members and close associates in the definition of a PEP creates a confusing and circular definition.
13.	**Correspondent banking**	PC	• Core requirements for correspondent banking are limited to respondent credit institutions located outside the EEA.
14.	**Money or value transfer services**	LC	• Norway has taken limited and *ad hoc* action regarding unauthorised MVTS providers. • The agents of MVTS providers from other EEA countries, in Norway, are not monitored for AML/CFT compliance, nor are the MVTS providers located in other EEA countries that offer services in Norway monitored for AML/CFT compliance.

Compliance with FATF Recommendations

Recommendation		Rating	Factor(s) underlying the rating
15.	**New technologies**	PC	• Although the NRA identifies ML/TF risks in relation to new technologies, there has not been a proper assessment of the risks. • There are no specific requirements for reporting FIs to identify and assess the ML/TF risks in relation to new technologies. There are general requirements for institutions to conduct risk assessments and mitigate risks but as it is not referred to in the regulations or associated guidance. It is unclear whether this applies to ML/TF risks and therefore whether financial institutions are required to assess and mitigate ML/TF risks.
16.	**Wire transfers**	PC	• There are no requirements on financial institutions to include and maintain the required beneficiary information in cross-border and domestic wire transfers. • There is no requirement for intermediary institutions to take reasonable measures to identify cross-border wire transfers that lack originator or beneficiary information. • There is no requirement for intermediary institutions to have risk-based policies and procedures on when to execute, reject or suspend a wire transfer with missing information. • The definition of transfers within the EEA in the EU Regulation is wider than that permitted as a domestic transfer in Recommendation 16. • It is unclear whether the EU Regulation applies to cases where a credit or debit or prepaid card is used as part of a payment system to effect a person-to-person wire transfer.

Compliance with FATF Recommendations

Recommendation		Rating	Factor(s) underlying the rating
17.	**Reliance on third parties**	PC	• There are no requirements for FIs to take steps to satisfy themselves that copies of identification data and other relevant documentation relating to CDD requirements will be made available from the third party upon request without delay. • When relying on third parties, while third parties must be regulated and supervised for CDD and record keeping, FIs are not required to satisfy themselves that the third party has measures in place for compliance with these requirements in line with Recommendations 10 and 11. • Norway does not give regard to information on the level of country risk when determining in which countries a third party can be based.
18.	**Internal controls and foreign branches and subsidiaries**	PC	• FIs are not required to have screening procedures to ensure high standards when hiring employees (other than key functionaries), and the requirement to have an independent audit function to test the AML/CFT system only applies to certain types of FIs. • Financial groups are not required to implement group-wide programmes against ML/TF. • While the MLA contains provisions to satisfy the requirements of c.18.3, their scope of application is limited to branches and subsidiaries established in states outside the EEA even though a large majority of branches and subsidiaries are located within the EEA.
19.	**Higher-risk countries**	LC	• FIs are not automatically required to apply enhanced CDD, proportionate to the risks, to business relationships and transactions with natural and legal persons (including FIs) from countries for which this is called for by the FATF.
20.	**Reporting of suspicious transaction**	C	
21.	**Tipping-off and confidentiality**	LC	• There is a tipping off prohibition, but there is no sanction applicable to individuals for breaching that prohibition and the only sanctions are those generally applicable to reporting entities.

Compliance with FATF Recommendations

Recommendation		Rating	Factor(s) underlying the rating
22.	**DNFBPs: Customer due diligence**	PC	• Scope issue: certain ship-based and internet-based casino gaming activities are not covered. • The deficiencies identified in relation to Recommendations 10-12, 15 & 17 equally apply to DNFBPs.
23.	**DNFBPs: Other measures**	LC	• Scope issue: certain ship- and internet-based casino gaming activities are not covered. • The deficiencies identified in relation to Recommendations 18-19, & 21, equally apply to DNFBPs.

Compliance with FATF Recommendations

Recommendation		Rating	Factor(s) underlying the rating
24.	**Transparency and beneficial ownership of legal persons**	PC	• While Norway has a publicly available guide on the features and creation of the various types of legal entities, this does not extend to a description of the process for obtaining and recording basic and beneficial ownership information. • The ML/TF risks associated with legal persons have not been adequately assessed. • Norway does not have adequate mechanisms to ensure that competent authorities have timely access to beneficial ownership information on companies in Norway that have foreign ownership. • Norway takes limited measures to ensure that beneficial ownership information is accurate and up-to-date. • The measures to ensure that companies cooperate with authorities by making information available in Norway (by always having a natural person or DNFBP resident in Norway and representing the company), are inadequate, as it is possible that directors/management are resident elsewhere in the EEA. • There are no requirements on registries to keep records for 5 years after a company is dissolved. • Other than controls on the use of nominees for foreign investors in public limited liability companies (PLLCs), there are no measures in place to prevent the misuse of nominee shareholders and directors in Norway. • The level of fines for breaches of registration or other requirements is relatively low and not dissuasive. • There are no direct sanctions for the failure of legal persons to provide access to ownership information. • Norway does not adequately monitor the quality of assistance it receives from other countries in response to requests for basic and beneficial ownership information.

Compliance with FATF Recommendations

Recommendation		Rating	Factor(s) underlying the rating
25.	**Transparency and beneficial ownership of legal arrangements**	PC	• There are no obligations (or associated sanctions) on trustees of foreign trusts to disclose their status to reporting entities, or to give authorities access to information held by them in relation to the trust. • It is unclear whether the authorities rapidly provide international cooperation on information relating to trusts and other legal arrangements that may hold assets in Norway, or where the trustee resides in Norway
26.	**Regulation and supervision of financial institutions**	PC	• Although commercial banks, insurance and finance companies are required to ensure that fit and proper requirements are met at all time, there is no obligation to notify the FSA of any changes in key functionaries, nor is there an explicit obligation to conduct fit and proper tests on new functionaries. • Supervision for AML/CFT of the insurance and securities sectors is very limited. • MVTS providers authorised in other EEA countries operating in Norway are not monitored for AML/CFT compliance and no on-site supervision has been undertaken of any MVTS provider. • The FSA does not determine the frequency and intensity of on-site and off-site AML/CFT supervision sufficiently on the basis of ML/TF risks. • The FSA does not conduct a proper review of the ML/TF risk profiles of financial institutions and groups under its supervision.
27.	**Powers of supervisors**	LC	• The sanctions for failure to comply with the AML/CFT requirements, both in the MLA and the FS Act, are not proportionate and dissuasive, especially for directors and senior management, and the range of sanctions is not sufficient.

Compliance with FATF Recommendations

Recommendation		Rating	Factor(s) underlying the rating
28.	**Regulation and supervision of DNFBPs**	PC	• Scope issue: certain casino gaming activities through the internet or on ships are not covered. • Norway has no designated competent authority for AML/CFT monitoring and supervision of TCSPs and dealers in precious metals and stones. • The sanctions for failure to comply with the AML/CFT requirements, both in the MLA and the FS Act, are not proportionate and dissuasive, especially for directors and senior management. • The FSA and SRBs do not determine the frequency and intensity of on-site and off-site AML/CFT supervision on the basis of ML/TF risks. • The FSA and SRBs do not conduct a proper review of the ML/TF risk profiles of DNFBPs under their supervision.
29.	**Financial intelligence units**	LC	• The FIU does not serve as the central agency for the receipt of disclosures filed by reporting entities regarding wire transfers reports and other threshold-based declarations. • The FIU has not produced any strategic analysis products since 2011. • The FIU's operational independence and autonomy is negatively impacted by the functions given to the Supervisory Board under the legal framework.
30.	**Responsibilities of law enforcement and investigative authorities**	C	
31.	**Powers of law enforcement and investigative authorities**	LC	• Norway's mechanism to identify whether natural or legal persons hold or control accounts is limited since the register is only updated annually.
32.	**Cash couriers**	C	

Compliance with FATF Recommendations

Recommendation		Rating	Factor(s) underlying the rating
33.	**Statistics**	PC	• Norway does not keep comprehensive and reliable statistics on matters relevant to the effectiveness and efficiency of their AML/CFT systems, particularly: ▸ ML investigations, prosecutions and convictions; ▸ Property frozen; seized and confiscated; and ▸ Mutual legal assistance, extradition and other international requests for co-operation made and received by LEAs and supervisors.
34.	**Guidance and feedback**	LC	• The FSA's guidance issued in 2009 is not sufficiently detailed in some areas to assist the implementation of the key building blocks of Norway's AML/CFT regime, including the application of the RBA and the detection of suspicious transactions. • The FSA is not pro-actively engaged in providing feedback to the reporting entities it supervises.
35.	**Sanctions**	PC	• Sanctions applicable to reporting entities, including their directors and senior management, for failure to comply with AML/CFT obligations are not proportionate (insufficient range of sanctions) or dissuasive. For example, the FSA has no power to impose administrative fines. • Criminal penalties for both natural and legal persons in the MLA (fines and imprisonment) can only be applied for breaches of a specific subset of MLA provisions which do not cover several of the essential requirements underpinning Norway's preventive AML/CFT regime, including ongoing monitoring, certain aspects of CDD (e.g., timing and reliance on third parties), corresponding banking relationships, tipping off and internal control requirements. • The coercive fines for breaching an order to stop contravening the MLA are not dissuasive in the absence of any amounts. In any event, coercive fines cannot be applied to directors and senior managers.
36.	**International instruments**	C	

Compliance with FATF Recommendations

Recommendation		Rating	Factor(s) underlying the rating
37.	**Mutual legal assistance**	LC	• *MLA* requests made directly to or from authorities other than the MoJ are not monitored in a case management system.
38.	**Mutual legal assistance: freezing and confiscation**	LC	• In cases of requests that are not made under the Vienna, Merida or Strasbourg Convention, Norway must start its own confiscation proceedings which could delay action. • It has not been shown that non-conviction based confiscation orders and related measures can be enforced in Norway. • There are no mechanisms to manage seized and confiscated property.
39.	**Extradition**	LC	• Extradition requests made directly to or from authorities other than the MoJ are not monitored in a case management system.
40.	**Other forms of international cooperation**	LC	• Customs authorities do not have secure gateways for the transmission and execution of requests.

Mutual Evaluation of Report of Norway

Preface

This report summarises the AML/CFT measures in place in Norway as at the date of the on-site visit. It analyses the level of compliance with the FATF 40 Recommendations and the level of effectiveness of Norway's anti-money laundering / counter-terrorist financing (AML/CFT) system, and recommends how the system could be strengthened.

This evaluation was based on the 2012 FATF Recommendations, and was prepared using the 2013 Methodology. The evaluation was based on information provided by Norway, and information obtained by the assessment team during its on-site visit to Norway from 27 March to 11 April 2014.

The evaluation was conducted by an assessment team consisting of: Mr Tomas Lindstrand, Chief Public Prosecutor, Sweden (legal expert); Ms Shereen Billings, T-Deputy Director-Legal, National Crime Agency, United Kingdom, and Ms Kamla Govender, Senior Legal and Policy Adviser, Financial Intelligence Centre, South Africa (law enforcement experts); Mr Stewart McGlynn, Division Head, Hong Kong Monetary Authority, Hong Kong, China and Ms Karina Hansen, Special Adviser, Danish Financial Supervisory Authority, Denmark (financial experts); Mr John Carlson, Ms Lia Umans and Mr Timothy Goodrick from the FATF Secretariat; Mr David Shannon from the Asia-Pacific Group on Money Laundering (APG) Secretariat and Mr Richard Lalonde from the International Monetary Fund. The report was reviewed by Ms Karin Zartl, Austria; Mr Alvin Koh, Singapore and Mr André Corterier, World Bank.

Norway previously underwent a FATF Mutual Evaluation in 2005, conducted according to the 2004 FATF Methodology. The 2005 evaluation and 2009 follow-up reports have been published and are available at www.fatf-gafi.org.

Norway's 2005 Mutual Evaluation concluded that the country was compliant with 13 Recommendations; largely compliant with 18; partially compliant with 12; non-compliant with 4 and 2 were not applicable. Norway exited the regular follow-up process in 2009. At that time, it was determined that Norway had reached a satisfactory level of compliance with all core Recommendations and eight of the key Recommendations, but had not reached a satisfactory level of compliance with two of the key Recommendations, old Special Recommendation III and Special Recommendation I (though the issues identified were related). It was determined that Norway had made substantial progress on the overall set of Recommendations that were rated partially compliant or non-compliant.

1. MONEY LAUNDERING / TERRORIST FINANCING RISKS AND CONTEXT

1.1. The Kingdom of Norway covers an area of 385 155 square kilometres, including the islands of Jan Mayen and Svalbard. Bordering Sweden, Finland and Russia, Norway forms the western part of the Scandinavian Peninsula in north-western Europe. The capital of Norway is Oslo. The population of Norway is approximately 5.1 million persons (as of January 1 2014), about 10% of whom are immigrants. In 2013, Norway's GDP was approximately NOK 3 trillion (EUR[1] 390 billion)[2] and total money supply (M2) at end of June 2014 was NOK 1,964 million (EUR 255 million)[3].

1.2. Norway maintains a parliamentary democratic system of government. The Head of State is the King and the Norwegian government is comprised of the Prime Minister and State Council. The legislative power lies within the unicameral Norwegian Parliament (*Storting*). Norway's legal system combines customary law, common law traditions and a civil law system. Primary legislation is in the form of laws. Secondary legislation is in the form of regulations. Both may be further explained in Parliamentary "preparatory works", the purpose of which is to give explanations to the Parliament prior to the adoption of the new legislation and to give guidance to the courts and other users of the legislation regarding the meaning of various provisions in the legislation. Norway has a legal system which requires that international legally-binding instruments, such as the UNSC Regulations and relevant EU-law, have to be transposed into the Norwegian legal order under separate national procedures.

1.3. Norway is not a member of the European Union (EU), but participates in the EU common market as a signatory of the European Economic Area (EEA) Agreement between the countries of the EU and the three European Free Trade Association (EFTA) states: Iceland, Liechtenstein and Norway. EU financial regulations are then generally applied in Norway, and Norway is bound to implement EC legislation concerning financial services, such as the EU's 3rd Anti-Money Laundering Directive (3AMLD). Norway's laws include measures based on 3 AMLD (which implemented the 2003 FATF Standards). Norway has participated in the Schengen agreement since 25 March 2001.

1.4. Norway's administration is divided into national and regional authorities. The Central government handles national security, economic and political issues, while also retaining overriding authority and supervision of Norway's 428 municipalities and 19 county authorities. In addition, the Islands of Svalbard and Jan Mayen are special status territorialities. Jan Mayen is a scientific outpost in the Arctic Ocean which is, with the exception of a scientific base, uninhabited. Svalbard, which in 2013 reported 1921 inhabitants of mostly either Norwegian or Russian background, is a sparsely inhabited archipelago in the Arctic Ocean, roughly halfway between Norway and the North Pole. Today, the economy on Svalbard is focused mainly on mining, tourism and international scientific research. The Governor of Svalbard is the highest authority in Svalbard and maintains police, as well as prosecutorial authority on the island. Residents in Svalbard benefit from low income taxes and exemptions from value added taxes and excise duties. The office of the Governor of Svalbard reports to the Norwegian Ministry of Justice, and also carries out tasks for other ministries within the Norwegian government. Very limited financial services are provided on the island. For the purposes of this assessment, all relevant anti-money laundering / count-terrorist financing (AML/CFT) laws apply on the island. While the Norwegian government reports that one case of corruption occurred between 2006 and 2008, no other instances of money laundering (ML)-related crimes are reported to have taken place on the island.

1 The figures in this report were provided in NOK and are converted using a rate of 1 NOK = 0.13 EUR, which is the average exchange rate over the period 2009-2013.

2 Statistics Norway (2014a)

3 Statistics Norway (2014b)

1

1.1 Money Laundering / Terrorist Financing Risks[4]

1.5. This section of the mutual evaluation report presents a summary of the assessment team's understanding of the money laundering / terrorist financing (ML/TF) risks in Norway. Norway's assessment and understanding of the risk is set out in Chapter 2.

1.6. This summary is based on material provided by Norway as well as open source material, as well as discussions with competent authorities and the private sector during the on-site visit. This includes consideration of Norway's National Risk Assessment (NRA) which was published in March 2014. However, the NRA has many weaknesses which make it of limited value to assess ML/TF threats. The NRA is considered in Chapter 2.

1.7. Proceeds of crime in Norway are generated by a range of criminality. The major sources for the proceeds of crime in Norway are generally considered to be drug trafficking and organised crime, tax crimes and fraud. Norway has not been able to supply the review team with assessments or aggregated data that provide a clear picture of the nature or level of proceeds generating crime in Norway. However, Norwegian threat assessments and reports demonstrate that new and existing organised criminal groups continue to maintain a presence within Norway.

1.8. The National Authority for Investigation and Prosecution of Economic and Environmental Crime (ØKOKRIM) Threat Assessment of Economic and Environmental Crime 2013 ranks a number of crime types in terms of their threat and consequence to Norwegian society. The top six crimes listed were: tax crimes; corruption; working environment crime; insurance fraud; illegal pollution and other environmental crimes; and securities crimes. Criminal convictions and related confiscation show that human trafficking and prostitution offences also generate significant criminal proceeds. There have also been cases involving domestic and foreign corruption which generate proceeds inside and outside Norway.

1.9. Norway has a strong taxation regime with a relatively high level of taxation. During the on-site visit, participants recognised the significant risks in tax evasion in various sectors including the construction industry, the labour market and small businesses, and a trend of smuggling consumable goods and related tax offences.

1.10. Norway does not have specific data available to estimate the country's exposure to cross-border illicit flows (related to crimes in other countries). There is little information on the techniques used or the degree to which foreign proceeds are being laundered in Norway. Discussions with investigative authorities and the FIU did not provide a great deal of information regarding the source, nature and scope of the threat from cross border illicit flows, though financial institutions active in border areas were able to give some observations. Indicators are that Norway has not, in general, been a significant transit route for illicit goods. The authorities did provide details of significant risks from Norwegian and foreign currency being smuggled out of Norway, and that a significant volume of NOK is circulating in Lithuania.

1.11. Threat reports by the National Criminal Investigation Service (KRIPOS) and other specialist law enforcement agencies in Norway indicate a range of criminal activities by organised crime groups active in Norway, including domestic groups (e.g., motor cycle gangs, etc.), Swedish organised crime groups, organised crime groups from Baltic countries, West Africa and Asia. Organized crime consists increasingly of informal and flexible networks that cooperate across nationality, ethnicity and other cultural affinities. Norwegian organised crime groups are increasingly using information technology to commit crimes, such as fraud, ICT-based offences, distribution of drugs, and for contacting potential victims of trafficking and the simplification of illegal migration. Amphetamines are a challenge for most police districts, with Eastern European criminals being the main suppliers and receiving much of the profits.

1.12. The main ML techniques used in Norway as identified in the NRA appear to be cash deposits and withdrawals, the use of professional facilitators such as lawyers and accountants, the buying and selling of

4 See Chapter 2 for the assessment of Norway's understanding of risk.

high value assets, and the use of cash couriers or money or value transfer systems to move funds out of the country. In addition, the MVTS sector poses ML/TF risks in Norway due to the nature of the activity, combined with limited supervision of the sector.

1.13. Norwegian authorities report that Islamist extremist groups pose the greatest security risk in regard to terrorism and TF. An asylum seeker (in jail in Norway) is designated on the United Nations Security Council Resolution (UNSCR) 1267 list and press reports indicate at least one Norwegian was involved in terror attacks in East Africa. Norwegian intelligence reports suggest that Islamist extremist groups in Norway are better organised than previously. These groups support militant groups in their former home regions through the collection of funds and propaganda activity. Individuals from these groups in Norway travel abroad to train and to join these groups and participate in their activities. The PST threat assessment and discussions with police indicate that TF risk arises chiefly from small scale domestic collection, provision and use of funds for radicalised persons in Norway or for the support of foreign groups operating outside of Norway. Organised left-wing and right-wing extremist groups or individuals can also pose a threat, as was shown by the Breivik case, and could carry out violent attacks against individual political opponents or religious or ethnic minorities.

1.14. There are a significant number of asylum seekers (including refugees) from conflict and post-conflict countries. Norwegian threat assessments note the ML and TF risks arising from connections back to such countries, including the sending of funds through informal remittance systems which service immigrant populations. Media reports have also highlighted TF risks in Norway beyond those identified in public government reports, including TF associated with the Liberation Tigers of Tamil Eelam (LTTE).

1.15. The risks from proliferation financing (PF) primarily stem from Norway's heavy involvement in the international oil and gas industry, shipping and related specialist technology.

1.2 Materiality

1.16. Norway is one of the wealthiest economies per capita in the world and has an open, export-oriented economy. The total assets of Norwegian financial institutions and branches of foreign institutions amount to approximately 320 percent of mainland GDP.

1.17. Norway maintains sizeable sovereign wealth funds, which are largely financed through taxation of and profits from the Norwegian oil industry. The petroleum industry accounts for around a quarter of Norway's GDP and Norway is the world's fifth largest oil exporter. Norway has long maintained a mixed economy, with considerable participation of state-owned companies and banks. Norway's main trading partners include the EU countries, Canada, China, Japan, Korea and the U.S.[5]

1.18. Norway has a strong currency with significant circulation of Norwegian Kroner circulating in other economies. The NRA reported the findings of a study carried out by the FIU which demonstrates that an especially large amount of Norwegian kroner is exchanged in the Baltic countries. In 2007 the Customs region of Oslo and Akershus estimated that in that year approximately NOK 1.5 billion (195 million EUR) in foreign currency was smuggled out of Norway.

1.19. Norway has a relatively high income tax rate (top marginal rate in 2010 was 47.8%) and a moderate corporate rate (28% in 2010). Norway has taken a leadership role in promoting mutual assistance among governments in the assessment and collection of taxes. Norway is a longstanding and active participant in the work of the OECD and has been a proponent of automatic and spontaneous exchange of information.

5 Statistics Norway (2014c)

1

1.3 Structural Elements

1.20. The key structural elements for effective AML/CFT controls appear to be present in Norway. Political and institutional stability and accountability; rule of law; and adequate transparency are all present. There is a Parliamentary *Ombudsman* who provides citizens with a mechanism to directly lodge complaints against, or start investigations of, public supervisory authorities. Norway also has a capable and independent judicial system, headed by the Supreme Court (*Hoyesterett*).

1.21. Norway's institutional structure provides it with the necessary framework to implement its AML/CFT regime. Norway takes a multi-agency approach to developing and implementing national AML/CFT policies. The responsibilities for Norway's AML/CFT policies are divided between the Ministry of Finance, the Ministry of Justice and Public Security, and the Ministry of Foreign Affairs, and entities subordinated to these ministries. Norway has entered into a high-level political commitment with the FATF towards international cooperation on AML/CFT standards. The competent authorities involved in Norway's AML/CFT efforts and their roles are as follows:

- **Ministry of Justice and Public Security (MoJ):** Responsible for policy and legislation relating to criminal law and confiscation. MoJ also acts as the central authority for *MLA* and extradition requests (excluding requests from Nordic/EU countries).
- **Ministry of Finance (MoF):** Responsible for policy and legislation relating to AML/CFT preventive measures such as the *MLA/MLR* and the *Currency Register Act*.
- **Ministry of Foreign Affairs (MFA):** Responsible for the implementation of UNSCRs related to terrorism and proliferation including the legal framework, the notification of changes and as the point of contact between Norway and the relevant UN Committees.
- **FIU:** The FIU is a unit in ØKOKRIM which is responsible for receiving, analysing and disseminating STRs and other information.
- **ØKOKRIM:** Investigates and prosecutes serious and complicated economic and environmental crime. ØKOKRIM handles the most significant ML cases related to such criminality, and provides assistance domestically and internationally in relation to such matters. It may also assist in TF investigations upon request.
- **National Police Directorate:** Manages and co-ordinates the Norwegian police including the 27 local police districts and 5 central police institutions.
- **Police districts:** Responsible for investigating and prosecuting ML (other than cases handled by ØKOKRIM or KRIPOS). There are 27 police districts and all districts have specialised economic crime units which would handle such cases.
- **Director General of Public Prosecutions:** Responsible for handling criminal prosecutions, including those related to ML/TF. There are 10 Heads of District Public Prosecution Offices, each under the leadership of a Chief State Prosecutor, and Public Prosecutors in the 27 police districts.
- **National Authority for Prosecution of Organised and Other Serious Crime (NAST):** Overall responsibility for the prosecution of cases investigated by KRIPOS and PST (ML cases in relation to organised crime and TF).
- **National Criminal Investigation Service (KRIPOS):** Responsibility for the investigation of ML cases in relation to organised crime.
- **Police Security Service (PST):** Responsible for monitoring and securing interior security in Norway, including counter-terrorism, CFT and counter proliferation. PST investigates and prosecutes crimes relating to terrorism, weapons of mass destruction, threats against national security and government, and espionage.

- **Customs Authority:** Responsible for management of the Customs Register, and for cross-border movements of currency and BNIs, as well as normal customs functions.

- **Financial Supervisory Authority (FSA):** Responsible for AML/CFT supervision of financial institutions, including banks, insurance companies, finance companies, payment institutions, investment firms, fund management companies. The FSA is also the AML/CFT supervisor for auditors, external accountants and real estate agencies. The FSA is the supervisor for all reporting entities for targeted financial sanctions.

- **Supervisory Council for Legal Practice:** Self-regulatory body for the legal profession. It is an independent governmental body financed by lawyers and responsible for AML/CFT supervision of lawyers and assistant attorneys. The governing body is a three person Supervisory Board which is appointed by the MoJ.

1.4 Other Contextual Factors

1.22. A feature of Norway's legal framework is the system of public registers used to promote transparency across many aspects of society, which the Norwegian authorities maintain for various purposes. In addition, authorities maintain a range of registers and databases that authorities only have access to. An overview of the registers and databases which play an important role in Norway's AML/CFT framework is at Annex 2 – Overview of Registers and Databases Used for AML/CFT.

1.23. Norway has taken strong measures and prioritised action to combat corruption. This includes domestic measures, and measures to combat foreign bribery by Norwegian companies abroad. Norway has a robust legal framework and a strong record of enforcement of anti-corruption measures which is one of the contextual factors that can help to support the implementation of an effective AML/CFT system[6]. Reports by international bodies have highlighted several reasons for this, including the high moral standards and independence of public officials, combined with a zero tolerance approach to corruption on the one hand, and the wide transparency of institutions and public scrutiny performed by the media, on the other hand.

1.5 Scoping of Issues of Increased Focus

1.24. During the on-site visit, the assessment team gave increased focus to the areas below. The issues listed represent not only areas of higher ML/TF risk (threats and vulnerabilities), but also contain issues that are of significant interest or concern to the assessment team based on the material provided before and during the on-site visit.

- **Risk-based approach and national cooperation,** including the level and nature of coordination between competent authorities given the absence of a lead authority or coordinating mechanism.

- **ML investigation and use of financial intelligence**, including the reasons for the relatively low number of successful ML prosecutions and convictions in Norway.

- **Money and Value Transfer Services sector**, including the level of AML/CFT compliance by MVTS providers given their identification as a high risk sector in risk and threat assessments.

6 See for example the *Fourth Evaluation Round – Corruption prevention in respect of members of parliament, judges and prosecutors – Evaluation Report of Norway* (2014), Group of States Against Corruption (GRECO), the *Phase 3 Report of Implementing the OECD Anti-Bribery Convention in Norway* (2011), Organisation of Economic Cooperation and Development (OECD), and the Country Review Report of Norway against the United Nations Convention against Corruption (UNCAC) (2013), United Nations Office on Drugs and Crime (UNODC)

- **AML/CFT supervision**, including the level and nature of supervision and the application of an approach based on ML/TF risks.
- **Misuse of corporate vehicles and Professional facilitators**, including the threat posed by professional facilitators, including lawyers and trust and company service providers (TCSPs), and the level of supervision and compliance with AML/CFT obligations.
- **Terrorist financing**, including the response to risks identified in the relevant PST threat assessments.
- **Banks and other reporting entities**, including the level of compliance with customer due diligence (CDD) requirements, including on beneficial owners, and the risk-based approach.
- **Tax crimes**, including how the proceeds of such crimes were being laundered and whether adequate measures were being taken.

1.25. **High risk sectors**, including the ML risks in the shipping, fisheries and labour market sectors and how these risks informed Norway's AML/CFT measures.

Bibliography

Statistics Norway (2014a), *Annual national accounts, 2013*, www.ssb.no/en/nasjonalregnskap-og-konjunkturer/statistikker/nr/aar/2014-02-12?fane=tabell&sort=nummer&tabell=162784, accessed on 1 September 2014

Statistics Norway (2014b), *The money supply M2, June 2014.* www.ssb.no/en/bank-og-finansmarked/statistikker/m2/maaned/2014-08-08, accessed on 1 September 2014

Statistics Norway (2014c), *External trade in goods, 2013, preliminary figures*, www.ssb.no/en/utenriksokonomi/statistikker/muh/aar-forelopige/2014-01-16?fane=tabell&sort=nummer&tabell=144581, accessed on 18 March 2014

2. NATIONAL AML/CFT POLICIES AND COORDINATION

Key Findings

- Norway has not pursued a comprehensive process to assess and develop a shared understanding of its money laundering and terrorist financing (ML/TF) risks. The National Risk Assessment (NRA) is Norway's first comprehensive ML/TF risk assessment. However, there are significant shortcomings in the process and methodology, and significant gaps in inputs and areas covered. As a result, it is limited in its usefulness as a firm basis for setting a national anti-money laundering / counter-terrorist financing (AML/CFT) policy.
- The authorities do not have a sufficient understanding of ML risks, and AML policies are not based on identified ML risks. The authorities possess a better understanding of the TF risk and context and have pursued a comprehensive process to assess and share information on TF risks over a number of years, which has informed CFT policies to a greater extent.
- Results of risk assessments are not used to justify exemptions and support the application of AML/CFT measures depending on risk. The activities and objectives of competent authorities and self-regulating bodies (SRBs) are not to a satisfactory degree configured to mitigate the ML/TF risks which have been identified. Norway has not ensured that financial institutions, designated non-financial businesses and professions (DNFBPs) and other sectors affected by the application of the FATF Standards are aware of the ML/TF risk profile in Norway.
- While Norway has expressed its commitment to AML/CFT it does not have overarching national policies or strategies to combat ML and TF.
- There is no AML/CFT coordination mechanism at a national level. Responsibility is fragmented and there is not a clear and consistent recognition of the importance of AML/CFT across all competent authorities. Norway has however identified this as a critical vulnerability in the NRA, accurately describing policy development and to a degree, coordination, as not being top-down.
- Considerable informal cooperation is taking place at the operational level and has value. This is particularly the case on TF and proliferation financing (PF), although improvement is necessary for the coordination of operational AML activities.

2.1 Background and Context

(a) Overview of AML/CFT Strategy

2.1. Norway adopts a multi-agency approach to developing and implementing national AML/CFT policies, with responsibility divided between the MoJ, MoF and MFA, and entities subordinated to these ministries[1]. A much wider range of agencies and ministries beyond those portfolios have roles in AML/CFT in Norway.

2.2. Norway has no overarching AML/CFT strategy in place. The MoJ, the Police and the MoF have jointly issued a series of action plans for combating economic crime (1992, 1995, 2000, 2004, and the latest in 2010). Norway has advised that these plans are the key strategy documents for Norway's AML/CFT efforts. However, the Action Plan against Economic Crime (2010-11), which covers the period 2010-14, has not been made available in English and it has therefore not been possible to judge the scope and focus of the most recent plan. Other criminal justice strategies have AML elements. For example, the MoJ issued the Government's Plan of Action against Human Trafficking (2011–2014), which includes a strategy to ensure human traffickers are prosecuted and the use of a number of AML-related measures to achieve this. These include calling on the police to follow the money/proceeds of human trafficking, including more specifically targeted financial investigations.

2.3. Norwegian officials articulated an overarching national strategy to combat extremism and terrorism, including measures to combat TF. The national policies and strategies for TF incorporate AML/CFT preventive elements, but these are fragmented, not up-to-date and AML/CFT is generally a secondary consideration. Norway has acknowledged this vulnerability in the NRA.

(b) The Institutional Framework

2.4. Norway has a sound institutional framework in place that should provide a sound basis for an effective AML/CFT regime, although the failure to adequately identify ML risks makes any risk-based policy response within that framework challenging.

2.5. Norway does not however have a principal body or mechanism that coordinates and manages AML/CFT at the strategic level, or which develops national AML/CFT policies. The absence of a framework or procedural base to coordinate the ministries efforts in this area is recognised in the NRA; the policy response which does take place is largely ad hoc, and initiated by individual agencies arising from functions associated with FATF related work.

(c) Coordination and Cooperation Arrangements

2.6. Regarding policy setting and coordination, higher level coordination and cooperation is less clearly defined. Various pieces of legislation allocate tasks to particular institutions, but the authorities have a concern that there is a lack of overall coordination of effort and that operational coordination is undertaken on an informal and ad hoc basis. At the highest level the Norwegian delegation to FATF consists of representatives from various stakeholders. Formal operational coordination takes place between the FSA and ØKOKRIM and includes the FIU twice a year. However, this is at a very senior management level and AML is only one of many issues that can be discussed. There are also some other formal annual forums, such as the ministries Permanent Committee against Economic Crimes, which coordinates a large number of ministries on a broad range of topics relating to economic crimes. In terms of TF and PF, the Coordinating and Advisory Committee

1 The fact that several of these ministries administer different parts of the relevant legislation also represents challenges for coordination, as recognised in the NRA. No legislative committee has ever been established that has examined all aspects of legislation related to AML/CFT

for Intelligence, Surveillance and Security Services (*KRU*)[2] ensures coordination between the secret services (including the Norwegian Police Police Security Service (PST)) and the Government. A coordination group on serious crime, involving both public and private sector, has also been recently established, but none of these arrangements is AML/CFT specific. A new high-level coordination mechanism between the Ministry of Justice (MoJ), the Ministry of Finance (MoF) and the Prime Minister's Office in relation to counter terrorism was put in place. AML is not yet part of that mechanism, but the authorities indicated that broader AML strategies are likely to be included in this tripartite coordination structure.

(d) Country's Assessment of Risk

2.7. In March 2014, Norway produced its first National Risk Assessment (NRA) on ML/TF risks. Prior to this, Norway undertook threat and risk assessments of economic and other crimes (including ML/TF to a limited extent) which tended to be agency-level assessments, rather than a combined national risk assessment for ML/TF. The nature and scope of these risk assessments is analysed below.

2.2 Technical Compliance (R.1, R.2, R.33)

Recommendation 1 – Assessing Risks and applying a Risk-Based Approach

2.8. Norway is rated partially compliant (PC) with Recommendation (R.) 1. There has not yet been a comprehensive process to assess and develop a shared understanding of ML risks. Norway issued its first NRA in March 2014, following an eight month study, under the authority of an inter-governmental expert group led by the MoJ. However, there were a number of significant shortcomings in the process which meant that the NRA does not properly identify and assess the ML risks. Norway has established an inter-governmental group to assess ML/TF risks through the NRA and has allocated funds to update the NRA biannually. This is outlined further under Immediate Outcome (IO.) 1 below. As regards TF, the PST issues annual threat assessments and there are noticeably stronger mechanisms and products identifying and assessing TF risk.

2.9. Norway has indicated that its annual national budget process can consider various risks, including ML/TF risk, when allocating resources. However, no link was demonstrated between allocation of resources and findings on ML/TF risks. Moreover ML risks have not yet been properly assessed, although TF risks have been identified and assessed. As regards risk-based measures, some basic concepts are in place e.g., high risk requires enhanced measures, but overall the concept of the risk-based approach (RBA) is not well framed, with exemptions for CDD measures but no evidence of proven low risk, confusion between simplified measures for lower risk and exemptions for low risk etc. The supervision of AML/CFT requirements is limited in scope and intensity, and is not based on ML/TF risk.

2.10. Reporting entities are required to conduct CDD and related record keeping measures using RBA, by reference to certain risk categories e.g., customer type and relationship, product etc., and to have satisfactory internal control and communication procedures approved at senior level. They must also be able to demonstrate (though not document), on an ongoing basis, that the extent of measures carried out is commensurate to the risk. Risk assessment information held by industry is not provided to competent authorities and self-regulating bodies (SRBs). As noted, certain risk-based measures are required or exist, but are not comprehensive or fully consistent with the FATF Standards.

Recommendation 2 – National Cooperation and Coordination

2.11. Norway is rated PC with R.2. Norway takes a multi-agency approach to developing and implementing national AML/CFT policies but does not have a coordination mechanism, nor does it have overarching national

2 The KRU has six members including representatives from the Ministry of Defence, MoJ and the MFA, the Chief of the Norwegian Intelligence Service, the Chief of the Norwegian National Security Authority and the Chief of the PST.

AML/CFT policies which are sufficiently informed by ML/TF risk. AML/CFT policies are nominally established through the annual budget allocation to relevant agencies. However, there is a lack of a pro-active strategic approach to AML/CFT and policies that exist are not implemented in a coordinated manner. There are high-level meetings between the senior management of some of the agencies, but AML/CFT forms only a minor part of the agenda. As a result, AML/CFT priorities vary between competent authorities and ML/TF risk has only been considered on a limited and ad hoc basis. In addition, Norway does not have adequate coordination mechanisms at the operational level, particularly in relation to the investigation and prosecution of ML and the implementation of AML/CFT preventive measures. Cooperation on these issues is undertaken on an informal and ad hoc basis and varies between agencies. There is a greater level of coordination in relation to TF and PF issues. The PST has established mechanisms to cooperate with relevant agencies, including law enforcement agencies and the FIU. However, it is a concern that the PST and FSA do not have any mechanisms to coordinate, particularly given the FSA's role in the implementation of the targeted financial sanctions.

Recommendation 33 – Statistics

2.12. Norway is rated PC with R.33. Overall, Norway does not maintain comprehensive and reliable statistics on matters relevant to the effectiveness and efficiency of its AML/CFT systems. A clear exception is the FIU which keeps comprehensive statistics regarding STRs received and disseminated by its IT system *"Ask"* that has specific tools for developing and visualising these types of statistics. In addition, PST keeps statistics regarding TF investigations as well as other actions it takes to prevent TF. These two institutions also keep comprehensive statistics regarding information exchange with their foreign counterparts. Apart from these details, Norway was not able to provide the assessment team with adequate and reliable statistics regarding: ML investigations, prosecutions and convictions; property frozen, seized and confiscated; and *MLA* and extradition requests or other international requests for cooperation made and received.

2.3 Effectiveness: Immediate Outcome 1 (Risk, Policy and Coordination)

Understanding of ML/TF risks

National Risk Assessment ('NRA')

2.13. The March 2014 NRA, which was commissioned jointly by the Ministries of Justice and Finance, is the first time that Norway has produced an inter-agency assessment of risk for ML/TF at the national level, which is an important step to move the AML/CFT system to a risk-sensitive framework. This work reflects a cabinet-level decision to assess current ML/TF risks as well as a commitment of resources to prepare an updated NRA within two years. The NRA was an eight month study, under the authority of an inter-governmental expert group led by the MoJ with the FIU undertaking significant drafting.

2.14. Norway's first NRA process was not supported by a comprehensive process to assess and develop a shared understanding of ML/TF risks. Discussions with the authorities and the contents of the NRA confirm that the process by which the NRA was delivered was not effective which led to important deficiencies in the report. The process appears to have been under-resourced; and the project plan did not allow sufficient time, resulting in the need to adopt a truncated process and methodology. Government stakeholder engagement was poor with few government agencies fully engaged in the process which has resulted in challenges concerning the acceptance of the findings of the NRA by all stakeholders.

2.15. The NRA was based on a limited range of data sources and the private sector was only peripherally consulted. Despite the capacities and resources of judicial and regulatory authorities in Norway, the systems and processes do not provide for the collection of good quality quantitative and qualitative data that allows the authorities to make judgements on the risks facing Norway. The NRA was principally based on STR data from a 2011 trend report, though some other STR data was used, but overall the data does not adequately consider thematic and sectoral issues. The NRA does not consider (directly or by cross-reference to previous threat assessments) the types and trends with proceeds generating predicate offences and the volumes of proceeds of crime from various predicate offences (domestic and foreign). In this respect, the NRA does not take into account the findings of threat assessments conducted by Norwegian LEAs. In addition, it was also

noted that the Norwegian authorities expressed concern in the NRA over the quality of the STRs being filed by reporting entities which questions their value as the basis of analysis.

2.16. The NRA is not clear on its assumptions regarding the nature of ML threats, although interviews with agencies involved in the production of the NRA indicated that the crime situation in Norway is well known to authorities. The NRA does not set out information or findings in relation to the nature of threats, the sources of proceeds of crime and the nature, extent and actors intending to conduct ML in Norway or with the involvement of Norwegian natural or legal persons. Finally, there is limited assessment of the relative importance and level of the ML/TF risks or threats.

2.17. The assessment of vulnerabilities in the NRA is more detailed. It takes a robust and critical view of a number of the weaknesses regarding the policies, the operation of the institutional framework, political level support and prioritisation of AML measures. The analysis of vulnerabilities reflects a stated willingness by the authorities to critically examine strengths and weaknesses. Despite the frank articulations of these vulnerabilities, a challenge in the findings on vulnerabilities arises from the lack of comprehensive consideration of ML threats, which leaves the findings on vulnerabilities relatively general and rather focused on issues of technical compliance.

2.18. As a result of these concerns, it is concluded that the NRA does not adequately identify and assess the ML/TF risks and has limited usefulness as a basis for setting a national AML/CFT policy. Given the timing of the NRA, national AML/CFT policies, have not been adjusted to take into account the findings of the NRA. Neither the NRA nor other information demonstrates that all relevant authorities possess a sound understanding of the ML/TF risks in Norway. Despite this, the NRA is an important first step for Norway, and the government's decision to allocate funding to conduct a follow-up NRA within two years is also a positive development. This represents an opportunity for Norway to address the concerns outlined above as soon as possible.

ML Risks

2.19. Norway has the institutional framework, technical capacities and resources to collect and analyse information related to risk. Despite this, policy settings and activities in recent years have not supported an effective process to collect and analyse information regarding ML risk.

2.20. Prior to the NRA, Norway had produced a number of agency-level criminal threat assessments including ØKOKRIM's Threat Assessments of Economic and Environmental Crime 2010 & 2013, the Oslo Police District trend report on crime 2012 (including a sub-chapter on ML), FIU reports of case studies and trends (intended to support reporting entities better understanding of ML risks) and KRIPOS reports on Organised Crime in Norway. Norway provided these reports on crime types and trends in Norwegian and therefore they were unable to be properly assessed by the team[3]. Criminal threat assessments have been done on issues such as organised crime, drug trafficking, smuggling, tax offences, outlaw motorcycle gangs, human trafficking environmental crime, and other criminal trends. These threat assessments appear to set out trends with crime types, the interaction between domestic and foreign organised crime actors and other information on various crime types. Norway also advised that the police districts prepare a strategic analysis of the crime situation in each police district on an annual basis. Norwegian authorities did not provide the assessment team with details of any estimates, or findings of studies of the nature, extent and value of profit driven crime, including ML, and the threat of foreign proceeds of crime, nor the level of ML risk in Norway.

2.21. Despite a lack of materials provided to the FATF on ML threats, the team was able to identify some credible information on trends with ML threats from open source materials (such as reports from international or regional bodies and NPOs) and interviews with officials. These sources indicate that authorities have developed a reasonably detailed picture of the operation of organised crime in Norway. Overall, it is apparent that the various reports give limited consideration to ML risks in specific contexts, and the reports do not demonstrate that the competent authorities have an adequate understanding of ML risks in Norway and they do not consider ML issues in sufficient detail.

3 The FATF procedures require all documents to be made available to the team in one of the FATF languages.

2.22. ØKOKRIM published a Threat Assessment of Economic and Environmental Crime in 2011 and 2013 which appears to include some assessment of the consequences of certain crimes. While a version was not available in English, the report appears to set out a model for ØKOKRIM to assess the probability of crime and the consequences of the crimes and assigning a score based on these variables. The risk model is indicator-based, and is intended to support consideration of priorities, strategies, target selection and resource allocation. Consequences are considered in terms of threats to life and health; threats to society; economic loss; and threats to public moral sense. The NRA does not reference consequences or the findings of these earlier ØKOKRIM Threat Assessments directly and does not use such risk modelling.

2.23. Below is the 'Scoring of Probability + Impact' from ØKOKRIM's Threat Assessment of Economic and Environmental Crime:

Table 2.1. ØKOKRIM's Predicate threat assessment

	Scoring of Probability + Impact		Scoring of Probability + Impact
Tax Crimes	90	Money laundering	64
Corruption	88	Subsidy crime	56
Fee Crime	81	Fraud	56
Working environmente crime	81	Pirated products	56
Insurance Fraud	80	Crime competition	49
Illegal pollution	80	Arts and Culture crime	48
Nature Crime	72	Bankruptcy crime	42
Securities Crimes	64	Embezzlement	40

Source: ØKOKRIM's Threat Assessment of Economic and Environmental Crime.

TF Risks

2.25. Norway has demonstrated that it has, in a large part, properly identified, assessed and appears to have understood its TF risk. Norway has applied its generally well developed institutional framework, technical capacities and resources to collect and analyse information related to TF risk. This has been supported by policy settings and political commitment to support an effective process to develop and share an understanding of TF threats, vulnerabilities and consequences.

2.26. In addition to the NRA, the PST publishes a yearly threat assessment which includes various risks of extremism and politically motivated violence, threats to dignitaries, intelligence activity and proliferation of weapons of mass destruction. Each annual threat assessment includes consideration of financial aspects of these activities. In addition to the public document, PST produces classified assessments for government. The PST's confidential reports will not be discussed in this report.

2.27. The PST threat assessments and discussions with police indicate that TF risk arises chiefly from small scale domestic collection, provision and use of funds for radicalised persons in Norway or for the support of foreign groups operating outside of Norway. Foreign funding for terror groups or actors in Norway is not regarded as a significant risk at present. The threat assessment for 2014 highlighted that politically motivated violence in the form of extreme Islamism will continue to represent a serious problem, and that the PST's most important task in 2014 will be to prevent persons with close links to Norway from becoming involved in terrorist attacks. The emergence of an active Islamist extremist group will lead to greater polarisation between the various extremist groups in Norway, and could also increase the threat from right-wing extremist groups. There is also the risk that persons with extreme views acting alone, or with a loose connection to a group, could commit very serious crimes. Discussions with the PST confirmed the ongoing assessment of TF risks associated with these threats. The PST's threat assessments have identified risks from remittance,

in particular largely informal remittance systems which service immigrant populations in Norway. This is combined with vulnerabilities for TF arising from the absence of supervision of the passported MVTS sector, the lack of action in relation to the unauthorised remittance sector and weaknesses in the controls that relate to charitable collection of funds in Norway.

2.28. Norway has, to a large extent, co-ordinated domestically to institute and apply measures to mitigate many of these TF risks. The MFA collects and shares information on TF risk with the larger Norwegian NGOs operating in conflict zones and other areas with significant TF risks.

2.29. However, while Norway has demonstrated that its operational agencies possess a sound understanding of TF risks, this is not consistent across all competent authorities e.g., the FSA and SRBs did not demonstrate a good understanding of TF risks.

Policies and Coordination

Policies based on ML risks

2.30. Norway does not have overarching national AML policies and the policy objectives and activities for combating ML at the agency level are not clearly articulated. Those that exist do not reflect the identified ML risks and are not supported by prioritised actions by key stakeholders. The activities and objectives of competent authorities and SRBs are not configured to mitigate the ML/TF risks identified. In recent years Norway's AML policy priorities appear to have been legislative and institutional developments arising from the 3rd Round MER and, more recently, support for Norway's presidency of the FATF.

2.31. Norwegian authorities indicated that the national AML strategies are set out in the government's Action Plan to Combat Economic Crime which is issued jointly by the Ministries of Justice and Finance every few years and last for a number of years. The 2004-2007 Economic Crime Action Plan identified AML/CFT as a national priority but only set out actions to take to combat ML to a limited extent. The most recent version of the Action Plan has not been made available to the team in English and could not be assessed. From discussions with officials and the earlier versions of the plan available in English, it is apparent that broad consideration is given to the measures required for more targeted and effective action to detect and combat economic crime, including expertise required and knowledge gaps, enforcement and confiscation arrangements, as well as international engagements. Despite the existence of these Action Plans, Norway lacks a 'top down' approach to support and drive the implementation of national AML policies and activities to address the identified ML risks. This seems to reflect a lack of prioritisation of combating ML at the political level, although some agencies have themselves prioritised AML activities.

2.32. The DGPP sets policy priorities for police and prosecutors through an annual circular letter. For 2014, economic crime, including ML, is pointed out as a priority for investigation and prosecution. The DGPP has also emphasised the importance of active use of confiscation measures, especially in relation to ML. The MoJ and Police Directorate issued a policy performance requirement for 2013 which emphasises that the Police must conduct confiscation investigation in all cases of profit-motivated crime and that the numbers of confiscation requirements are expected to exceed the average for the last three years. The Police Directorate has also provided similar policy objectives to the police districts.

2.33. AML has not been sufficiently prioritised at the national level and as a result the activity based response is limited, lacks adequate cohesion across agencies and is generally reactive. The priority, resources and intensity of activities for AML of most competent authorities is not demonstrated to be consistent with the risks identified by the police, ØKOKRIM, and jointly in the NRA. As an example, the NRA highlights a number of vulnerable sectors; however few of these are subject to prioritised AML/CFT measures. Professional gatekeepers are identified as higher risk for ML, yet lawyers are subject to minimal oversight by a SRB, while TCSPs remain outside of AML/CFT regulation altogether.

2.34. Norwegian authorities indicated that they have delayed the development of a new Action Plan on Combating Economic Crime to take into account the outcomes of the FATF Mutual Evaluation and the EU issuing the 4th Anti-Money Laundering Directive.

2.35. Results of the assessments of risks are not properly used to justify exemptions and support the application of AML/CFT measures depending on risk. The activities and objectives of competent authorities and SRBs are not configured to mitigate the ML/TF risks identified.

Policies based on TF Risks

2.36. Implementation of policies and activities to combat TF risks demonstrate a substantial degree of effectiveness, although further steps remain to be taken. In a number of cases consideration is being given to make further reforms to respond to the identified risks. The MoJ issued an Action Plan to counter radicalisation and violent extremism covering the period 2010 - 2013 and focuses on four priority areas: increased knowledge and information; strengthened government cooperation; strengthened dialogue and involvement; and support for vulnerable and disadvantaged people. While CFT measures are not explicitly mentioned in the Plan, the PST, MFA and other ministries and agencies are pursuing policies which prioritise financial aspects of terrorism including developing and sharing financial intelligence, conducting financial investigations of terrorist groups and seeking to prevent the abuse of NPOs, hawala and other financial channels which may be vulnerable to TF. A new Action Plan was issued in June 2014, although this has not been provided to the assessment team.

2.37. However, while TF risks are generally well understood by the PST, they are not adequately integrated into Norway's policies relating to AML/CFT preventive measures, including policy and supervision priorities related to CDD of beneficial ownership and targeted financial sanctions. The only isolated example in the supervision of reporting entities when TF risks have been considered was in relation to the MVTS sector. Given the high risks identified by the PST, Norway introduced a licensing framework and took steps at that time to encourage remitters to become licensed and comply with AML/CFT regulatory controls in 2010. However, the level of supervision of MVTS since then has not been informed by TF risk. No on-site visits have taken place and little action is taken to identify unlicensed providers. A further challenge is that the policy for a relatively resource intensive licensing regime for these types of MVTS has not resulted in a significant number of remitters transferring from the informal to the formal sector. Interviews with remitters and the regulator suggest that compliance costs are an impediment to licensed players remaining in the formal system. At the same time, passported providers from other EEA countries are monitored for compliance with Norway's AML/CFT laws (see IO.4).

2.38. PST and the FIU have prioritised the development of TF-related financial intelligence and policies and activities to support financial investigations of terrorist groups and activities. This adds a significant degree of effectiveness. National AML/CFT policies to ensure the regulation and transparency of the collection of charitable funds have not been sufficient to address the identified risks. However the Ministry of Culture is leading work to review and amend the regulatory framework (see IO.10). The intensity of application of activities to apply UNSCR 1267 targeted financial sanctions does not reflect the risks identified by the PST. Implementation of targeted financial sanctions pursuant to UNSCR 1373, as required by Recommendation 6, is negatively affected by the absence of adequate policies and activities. The greatest challenge has been that the FSA, as the primary AML/CFT regulator and supervisor, has not prioritised CFT policies and activities in response to the risks identified by the PST. This is a significant gap for effectiveness.

Cooperation and coordination

2.39. Cooperation between competent authorities over the development and implementation of AML policies is not satisfactory. In particular, there has been limited coordination of supervisory activities within broader AML policies and there has been very limited engagement with SRBs. Cooperation in relation to CFT activities is more substantial, although this does not include supervisory activities. Nevertheless, a strong willingness to cooperate was noted. There are real opportunities to make significant improvements to policy and operational level cooperation and coordination on AML. The key obstacles to effectiveness are the lack of 'top down' support for coordination, a framework to do so, a lack of appropriate cooperation procedures and implementing measures.

2.40. Operational cooperation, and the transfer of information between AML stakeholders, is taking place within the framework, but on an informal and ad hoc basis, which on the whole is not effective. Coordination and cooperation on AML generally relies more upon working relationships at the operational level, rather

than a 'top down', national framework. The NRA confirms this and notes that parties further down the AML/CFT system are acting largely on their own initiative. Certain operational parts of the system are required to assume unrealistic levels of responsibility with insufficient guidance and support at the policy level. The NRA therefore provides a basis to address the problems.

2.41. The situation in relation to CFT is more effective. Operational cooperation and coordination, and the transfer of information between stakeholders at an operational level for CFT, generally displays a substantial level of effectiveness. Channels and mechanisms of cooperation and coordination are established and well supported. Certain agencies could be more closely involved, but overall the strength of the cooperation and coordination on CFT at an operational level is a model that Norway should consider for AML measures.

2.42. **MoF – MoJ***:* As the two lead ministries on AML/CFT, coordination between these two agencies exists but there was not a clear track record of policy level coordination on AML/CFT. This reflects the lack of a structured approach to coordination of AML/CFT policy making. While some coordination has taken place, for example during the development of the *MLA* which was enacted in 2009, this is limited and does not take place on a regular basis. Given the absence of a mechanism for the coordination of AML/CFT policy, the coordination that does take place is on an informal and ad hoc basis, and needs to be enhanced.

2.43. **FIU - FSA:** The FSA and the FIU are focal points for AML/CFT efforts in relation to preventive measures (including STR reporting) and supervision. Some cooperation does take place between the FIU and FSA but overall it is on an ad hoc and informal basis. Biannual high-level meetings are held at a senior level between OKOKRIM and the FSA. However, AML/CFT issues form only a small part of the agenda. At the operational levels ad hoc telephone contact or meetings take place on a case-by-case informal basis (including where the FIU has identified AML/CFT compliance failures with particular reporting parties). No information was available on parallel AML/CFT activities, what results are achieved in practice based on FIU and FSA dialogue and whether these are satisfactory. Increased engagement has been noted recently between FSA and the FIU on the topic of off-site inspections, in which the FIU is conducting a mini analysis of some banks' STR compliance, and providing feedback to the FSA. The FIU has a higher than expected level of engagement with reporting entities' compliance functions and as a result has a relatively detailed understanding of reporting parties' AML/CFT compliance, which is not being sufficiently utilised to help inform the FSA's supervisory risk analysis of financial sectors.

2.44. Cooperation and information sharing between the FIU and FSA on risk could be greatly improved. For example, although virtual currencies such as Bitcoin are noted in the NRA and the FIU has received STRs on this from entities under FSA supervision, no information exchange had taken place, in part because no regular forum or channel exists to discuss ML/TF risks. Additionally, there is no coordinated action to identify and take action against unlicensed MVTS providers and information exchange between the FIU and FSA on this is ad hoc.

2.45. **FIU – ØKOKRIM:** Authorities demonstrated a high level of cooperation between the FIU and ML team in ØKOKRIM.

2.46. **FIU - Police:** Norway has recognised that cooperation between the FIU and Police is frustrated to a large extent by the lack of a mechanism for national tasking over the dispatch of FIU referrals to police districts and other LEAs (see IO.6 below). Effective cooperation did take place with certain teams, such as with the Drugs Team, but decisions over the level of cooperation (or whether to cooperate with the FIU at all) remain mainly with individual police districts. Current arrangements are ad hoc, based around personal contacts and have no formal procedural basis unless the FIU files a police report. That cooperation relies to a great extent on the leverage obtained by the fact that most analysts in the FIU are serving Police Officers and prosecutors. When a Police District does not make use of the dissemination, the FIU uses alternative dissemination options, such as a referral to the Customs Authority, or does not pursue the case. The assessment team noted that this unsatisfactory arrangement may have resulted in the FIU ultimately making fewer disseminations. Norway has recognised this shortcoming, primarily in its review of the Norwegian Police Service (which should result in a smaller number of Districts and, in time, more standardised procedures) and as an objective of the *Round Norway* initiative. In general, communication was not taking place on how to address these issues. There has not been any consideration of alternatives that could complement the work of LEAs, such as referrals to the FSA of possible breaches of the *MLA*.

2.47. **DGPP – Police:** There is very good cooperation and coordination between the public prosecutors and the police, including specialist investigation agencies such as ØKOKRIM, KRIPOS and the PST. This includes aligned policies and priorities, as well as oversight of investigations by the DGPP.

2.48. **PST:** The PST takes a proactive and strategic approach to inter-agency cooperation. The PST is dependent on cooperation with different agencies and organisations in Norway, including the FIU, ØKOKRIM, the police districts, KRIPOS and the Ministry of Foreign Affairs. There is regular and effective cooperation with various stakeholders that is formalised and procedurally based with its more important partner agencies. The PST has personnel in all 27 police districts and in the 26 districts outside of Oslo is subordinate to the respective police chief. The PST cooperates with the Police over specific targets or persons of interest; with Norwegian Customs and Excise, primarily over the currency register (which also took place with other competent authorities); with the Norwegian Tax Administration and financial institutions over TF risks relating to hawala. However, it is a concern that the PST and FSA do not cooperate on a regular basis. There are no mechanisms through which the PST and FSA coordinate their activities with regards to CFT. The PST has established a good level of formalised cooperation with the FIU (regular meetings sharing information on TF indicators and TF related STRs for example) aided by two dedicated staff in the FIU, one of whom is from PST. These ex or embedded staff in the FIU (whether PST or Police) have promoted best practices for cooperation and coordination at the working level.

Coordination for combating proliferation financing

2.49. Norway has established mechanisms for the coordination of policies and activities to combat the financing of proliferation, though it is a concern that the FSA does not participate in these mechanisms. An operational working group meets weekly or bi-weekly to review applications for export licences and transfers of funds to and from Iran. Representatives from the PST, the customs authority, the export section of the MFA and the legal department of the MFA participate. The group also assesses export and financial exchanges with other states, including DPRK. The FIU and FSA do not participate in this or any other forum on combating proliferation financing, even on an 'as necessary' basis. This is a particular concern given the role of the FIU and the FSA's role in the implementation of the Iran and DPRK Regulations.

Engagement with the reporting entities

2.50. Norway has not taken sufficient action to ensure that financial institutions, DNFBPs and other sectors affected by the application of the FATF Standards are aware of the ML/TF risk profile in Norway. Norway has taken some important steps to ensure that financial institutions, DNFBPs and other sectors involved in implementing CFT controls are aware of the TF risks facing their sector. However, by contrast, not enough has been done to raise awareness of the ML risks facing those same sectors.

2.51. Some efforts have been made by LEAs, the FIU and the MFA to raise awareness of national ML/TF risks. The FIU takes a number of steps to reach out to the financial sector on issues of risk, directly through engagement with the reporting entities and through umbrella groups such as Finance Norway. The FIU has allocated resources and developed the expertise of staff and implemented specialist programs to engage with reporting financial institutions and DNFBPs on issues of AML/CFT compliance and STR reporting. However, the FSA is largely uninvolved in efforts to ensure that financial institutions and DNFBPs are aware of the ML/TF risks.

2.52. As noted above, a number of agency-level or issue-specific assessments have been produced that address ML/TF risk to varying degrees. These reports are publicly available and provide the private sector with some useful information regarding ML/TF risks in Norway, particularly the FIU's trend and annual reports, and the PST's annual public threat assessments. Some other studies have been done by private sector bodies, such as the 2009 report by the Security Council for Norwegian Businesses, and the 2013 Trend Report by Finance Norway, both of which have some information on ML issues.

2.53. Each year Finance Norway, the FIU and the FSA arrange a two day conference which focuses solely on ML/TF related trends, threats and risks, including STRs[4]. Private sector representatives found these conferences helpful and some of the provided material related to issues that were addressed in the NRA. Some information on risk is also published on the websites of the publishing authorities and also available on the government run web page *hvitvasking*. To some extent, the objective of sharing knowledge and strengthening cooperation between private and public sectors is being achieved through these forums. Nevertheless, Finance Norway has raised a concern that the Government and in particular the FSA have not been sufficiently proactive in sharing information on national ML/TF risks or shown an interest in receiving private sector views on potentially risk areas or factors[5]. During meetings with industry, the assessment team were informed that mechanisms or entry points to seek guidance from the FSA on risk are not sufficient. The FSA is regarded by industry as being passive rather than proactive, which does not effectively share information about its ML/TF risks at a sector or FI/Group level.

2.54. As the NRA was only published in March 2014, it has not yet been used to raise awareness of the relevant national ML/TF risks and it is uncertain how useful it would be given the limited focus of the NRA as described above.

2.55. The PST had also engaged the private sector on its views of TF risk, with its outreach program running three training courses in 2013. The assessment team received positive feedback during the on-site visit with regard to the mechanisms or entry points available to share information on TF risk with PST.

Conclusion on IO.1

2.56. The assessment team has serious concerns with the overall level of understanding of ML risk, and the cooperation and coordination of Norwegian authorities for AML policies and measures. The process and findings of the NRA are unsatisfactory. The team considers that this was not a comprehensive ML/TF risk assessment and that it is limited in its usefulness as a basis for setting a national AML/CFT policy. While LEAs have assessed the criminal threats in Norway, these are mainly focused on predicate crimes and not on ML risk. As a result, authorities do not possess a sufficient understanding of ML risks and AML priorities of LEAs are driven by their understanding of risks associated with predicate offences. The understanding of TF risks is stronger, as the PST in particular has assessed terrorism and its financing which informs their operational policies. The activities and objectives of the FSA are not configured to a satisfactory degree to mitigate the ML/TF risks, and Norway has not taken sufficient action to ensure that financial institutions, DNFBPs and other sectors are aware of the ML/TF risk profile in Norway. The sectors are not taking satisfactory risk-based mitigation measures. The lack of statistics in key areas increases the difficulty for Norway to assess ML/TF risks and implement evidence-based AML/CFT policies. Norway's high-level commitment to prepare an updated NRA is a welcome initiative, as is the intention to update policies based on the results of this assessment.

2.57. Norway does not have overarching national policies or strategies to combat ML/TF and there is no AML/CFT coordination mechanism at a national level. As a result, responsibilities are fragmented and there is no clear and consistent recognition of the importance of AML/CFT across competent authorities. Coordination is better with respect to CFT. At an operational level, considerable informal and ad hoc cooperation is taking place and has value. This is particularly the case for CFT activities, although concerns remain regarding operational AML cooperation, where the informal channels do not adequately replace the lack of formal coordination mechanisms. There is generally strong cooperation and coordination of activities to combat financing of proliferation, including between the PST, the customs authority, the export section of the MFA and the legal department of the MFA. However, it is a concern that the FIU and FSA do not participate in the cooperation mechanisms.

4 The target audience are financial institutions including Norway's largest banks and insurance companies, but smaller hawaladars and other groups, subject to the AML act, also attend.

5 The NRA acknowledges that Finance Norway has indicated that the requirements in the *MLA* are difficult for the banks to understand and comply with.

2.58. Norway has a **moderate level of effectiveness** for IO.1.

2.4 Recommendations on National AML/CFT Policies and Coordination

a. Norway should commence work as soon as possible on a more robust NRA (process, methodology and inputs) including by:

- Considering quantitative and qualitative data on the risks facing Norway and the operation of AML/CFT measures,
- Assessing and reflecting on the findings of various agency-level assessments on threat, vulnerability & consequence, and
- Consulting with all relevant stakeholders.

b. Norway should then develop national AML/CFT policies, including the use of financial intelligence, and identifying priority actions based on mitigating the identified ML/TF risks.

c. Norway should improve coordination, at the AML/CFT policy making level, including by:

- Establishing a strategic level national coordination / cooperation platform for regular inter-agency policy-level review of AML/CFT initiatives (preventive and criminal justice), and
- Strengthening feedback between agencies to judge the effectiveness of implementation in order to adjust strategies and their implementation (e.g., risk information, level or quality of STR reporting, information on unlicensed remitters or information that might lead to supervisory authorities to target specific institutions for review or support outreach efforts).

d. Norway should maintain comprehensive statistics on AML issues to inform the risk assessment and support evidence-based policy making, particularly for areas not currently covered including ML investigations and prosecutions, confiscations and international cooperation.

e. Norway should prioritise efforts to raise awareness of ML/TF risks among financial institutions and DNFBPs, including by:

- Providing regular and consistent guidance to the private sector on risk and their conduct of enterprise level risk assessments, and
- Feeding financial institutions' and DNFBPs' findings of risk into the NRA process.

f. Norway should use the findings of future ML/TF risk assessments to justify exemptions, and apply enhanced measures for higher risk scenarios and simplified measures for lower risk scenarios.

3. LEGAL SYSTEM AND OPERATIONAL ISSUES

Key Findings

- Norway has a well-functioning financial intelligence unit (FIU) which develops and disseminates good quality financial intelligence to a range of law enforcement agencies (LEAs) as well as to customs and tax authorities.
- The FIU produces its financial intelligence based on suspicious transaction reports (STRs) received and on information from a wide range of informative, public and restricted access databases, including police information. However, several factors negatively impact the FIU's ability and capacity to produce an increased amount of good intelligence products: the rather low quantity and quality of the STRs received; and the fact that the FIU did not undertake strategic analysis since 2011, undermines authorities' ability to identify emerging threats.
- Financial intelligence is used by some specialist agencies such as ØKOKRIM and the Norwegian Police Security Service (PST) to 'follow the money' associated with predicate offences and terrorist financing (TF), although money laundering (ML) offences are generally not pursued. The use of financial intelligence in the 27 police districts and in other specialised agencies such as the National Criminal Investigation Service (KRIPOS) is limited.
- Norway has in many ways a good legal foundation and sound institutional structure for combatting ML which could be applied to effectively mitigate ML risks. Norway has a broad ML offence that applies to all crimes in line with the FATF Standards, and the proposed new Penal Code with a separate ML offence (*cf.* "receiving") will help to show that ML is more than just an ancillary crime to the predicate offence. There are also designated LEAs with access to a generally broad range of powers.
- While economic crime is considered a priority, ML is not prioritised. Despite the absence of comprehensive and reliable statistics, information received from various authorities indicates that there are few ML cases, and that many of them are self-laundering cases. There are not many cases in relation to organised ML, third party laundering, or laundering the proceeds of foreign predicate offences.
- There are relatively few prosecutions and convictions for ML. ML cases are handled either by the 27 police districts or by specialised agencies such as ØKOKRIM. Police districts and specialised agencies often decide not to investigate or prosecute ML offences because they prioritise the investigation and prosecution of the predicate offence. In addition, the lack of expertise and resources in many police districts is also a factor.
- Confiscation powers are broad, and the confiscation of criminal proceeds is a policy priority. However, results to date are not satisfactory and significant improvements are necessary.
- The system for cross border cash and bearer negotiable instruments (BNI) declarations, while legally comprehensive, has produced limited outputs, relative to the risks in this area.

3.1 Background and Context

Legal System and Offences

3.1. Most criminal offences in Norway are contained in the *General Civil Penal Code 1902* (*PC*). The *PC* distinguishes between more serious offences "felonies" (mainly offences punishable by imprisonment for more than 3 months) and other less serious offences "misdemeanours". The PC also contains other relevant provisions such as those relating to ancillary offences, jurisdiction, corporate criminal liability, powers to order confiscation etc. The *PC* is complemented by the *Criminal Procedure Act 2006* (*CPA*) which sets out all the procedural powers and mechanisms including for the use of investigative powers and coercive measures (e.g., powers to freeze and seize property). Provisions in relation to the declaration of currency and BNI are contained in the *Customs Act 1966* (*CA*) and the *2009 Regulations to the Customs Act* (*RCA*). ML is criminalised in *PC*, s.317 & 318. The legal provisions concerning confiscation and provisional measures are set out in s.34-38 of the *PC* and in s.202d-g (Freezing of assets), s.203-216 (Seizure and surrender order), and s.217-222 (Charge on property). Administration of the property of the person charged) of the *CPA*.

3.2. ØKOKRIM is the national authority with responsibility for the investigation and prosecution of economic and environmental crime. In general, ØKOKRIM handles the most significant ML cases related to such criminality. The police districts also have responsibility for investigating ML. There are 27 police districts and all districts have specialised economic crime units which could handle ML cases. The KRIPOS and the National Authority for Prosecution of Organised and Other Serious Crime (NAST) are responsible for the investigation and prosecution of ML cases in relation to organised crime.

3.2 Technical Compliance (R.3, R.4, R.29-32)

Money Laundering and Confiscation:

Recommendation 3 – Money laundering offence

3.3. Norway is rated compliant (C) with Recommendation (R.) 3. ML is criminalised in s.317 of the *PC*, and s.318 makes ML conspiracy an offence. Section 317 also criminalises the receiving of stolen property. This provision makes it an offence to launder "the proceeds of a criminal act" and the offence covers all crimes as predicates (including a range of offences in all 21 categories of designated predicate offences including tax offences). The term "proceeds" covers all types of property, regardless of value, that directly or indirectly represent the proceeds of an offence. It is not necessary that someone be convicted of a predicate offence to prove that the property is the proceeds of crime. Third party and self-laundering are separately criminalised, laundering the proceeds of foreign predicate offences is covered, legal persons are subject to criminal liability and there is a range of ancillary offences. The ML offence is therefore a broad one.

3.4. Criminal sanctions for natural persons are proportionate to many other similar types of offences in Norway and although at the lower end of the range could be considered dissuasive. The penalty for ordinary ML is up to 3 years imprisonment. Aggravated ML has a penalty of up to 6 years imprisonment and is used based on factors such as the value of the property being laundered i.e., it can be aggravated if more than NOK 100 000 (EUR 13 000). More serious penalties apply to drug ML (21 years) and cases involving organised crime (up to 5 year increase). Unlimited fines can be imposed. Norway considers that the penalties for ordinary and aggravated ML are in line with other economic crimes, and are dissuasive. Overall the sanctions regime for s.317, while at the lower end of the international scale, is proportionate to most of the domestic penal regime, and can be considered dissuasive for technical compliance purposes.

Recommendation 4 – Confiscation and provisional measures

3.5. Norway is rated largely compliant (LC) with R.4. The legal provisions concerning confiscation (*PC* s.34-38) and provisional measures (*CPA* s.202-217) are generally comprehensive and have the potential to be

very effective. Confiscation of the proceeds of all criminal offences is mandatory, includes any profits derived, while confiscation of instrumentalities or intended instrumentalities is a discretionary penalty. Even if the prosecutor has not made a claim, the Court has a duty to confiscate if the preconditions are met. It is also possible to order equivalent value confiscation, and to confiscate proceeds held by third parties who knew that the property was criminally derived or was a gift. The amount of proceeds can be proven to the civil standard of proof. A potentially very effective additional power is the power to use extended confiscation in cases (a) which have a penalty of 6 or more years or the type of offence may result in a considerable gain, and (b) the offender was convicted within the previous five years of an offence resulting in a considerable gain. Under extended confiscation, the offender must prove on the balance of probabilities that the property was legally obtained, and can cover the property of their spouse, close relatives, or legal person(s) that they control. There is also a possibility for the prosecution authority to issue a writ of confiscation instead of an indictment (s.255, *CPA*). The writ can be used for confiscation of both goods and value.

3.6. The police and prosecution authorities, including ØKOKRIM, have investigative powers to identify and trace assets, and powers to freeze, seize and/or charge property. Freezing is restricted to terrorism and TF cases (see R.6), seizure is used to either seize or freeze property, while charging involves placing a charge on the property for a specific amount in order to secure payment of a possible confiscation order. There has not been any change to the legislation since Norway´s 4th follow up report. These powers are extensive but could be further strengthened if it became possible to seize all of a defendant's assets (even those not identified specifically). Another small practical enhancement would be to create the powers/mechanisms that would enable the authorities to actively manage seized or frozen property.

Operational and Law Enforcement

Recommendation 29 – Financial intelligence units

3.7. Norway is rated LC with R.29. Norway's FIU is a law enforcement/judicial type of FIU located within ØKOKRIM. It is responsible for receiving, analysing and disseminating information disclosed by reporting entities. The FIU has a well-developed operational analysis function with direct access to a wide range of databases and registers with administrative and law enforcement information to support its operational analysis. It uses an advanced IT-system *"Ask"* with analytical and data processing functions which allows it to directly link STRs to relevant public and police sources, and to information from other domestic authorities and foreign FIUs. The FIU is able to obtain additional financial information from the reporting entity which filed the STR. The scope of its strategic analysis is currently limited as no strategic analysis has been produced since 2011. Information can be disseminated to competent authorities both spontaneously and upon request. There are procedures in place for the handling, storage, protection of, and access to FIU information. For data protection reasons, the FIU is subject to the oversight of a Supervisory Board but the working methods of this Board could potentially interfere with the FIU's operational independence. The FIU has been a member of the Egmont Group since 1995 and frequently engages in information exchange with foreign counterparts.

Recommendation 30 – Responsibilities of law enforcement and investigative authorities

3.8. Norway is rated C with R.30. Norway has a comprehensive network of law enforcement and prosecution authorities that have designated responsibility for investigating ML, TF and associated predicate offences. In addition to the local police, Norway has seven special permanent units that are organised directly under the National Police Directorate (NPD). ØKOKRIM is one of these permanent units and specialises in the investigation of complicated economic crime, including ML, corruption and tax offences. As a general rule, ML and associated predicate offences are investigated by the local police under the instruction of the Prosecution Authority in the police district where the offence was committed. ØKOKRIM is in charge of the investigation of more complicated cases and also provides assistance to the local police. The PST is formally responsible for investigating covert TF cases. The police and ØKOKRIM are formally responsible for open cases, although in practice PST takes over all cases.

Recommendation 31 – Powers of law enforcement and investigative authorities

3.9. Norway is rated LC with R.31. Norwegian competent authorities that are responsible for investigating ML/TF and associated predicate offences have powers that give them access to documents and information for those investigations. Norway has legislative measures in place that provide law enforcement with a range of investigative techniques when conducting ML/TF or other criminal investigations. Most of these techniques can be used for serious offences (where the maximum penalty is five or ten years imprisonment). In the context of ML, they are available in cases of aggravated or organised crime/drug-related ML. It is also noted that witnesses bound by certain secrecy laws such as banking legislation, are also required to provide statements to police on matters covered by these laws. While authorities can identify accounts from the taxation register, this is only updated annually, which leaves a gap in the ability of authorities to identify whether natural or legal persons hold or control accounts.

Recommendation 32 – Cash Couriers

3.10. Norway is rated C with R.32. Norway has a sound legal framework in place for the declaration and identification of incoming and outgoing cross-border movements of funds by travellers. Customs authorities have comprehensive powers to collect further information from the carrier and to impose proportionate and dissuasive sanctions for failures to comply with the declaration requirement. Customs authorities can stop or restrain currency or BNI on a suspicion of ML/TF or predicate offences. For false declarations, customs can stop the currency or BNI immediately to withhold an administrative fine of 20% of the total amount not declared and to determine whether there is a suspicion of ML/TF. With the exception of the cases reported to the police/prosecutor, data regarding other cross-border declarations are registered by the customs authorities in the Currency Register. Norwegian competent authorities, including the FIU, have on-line access to this register. In addition, customs authorities work closely with other competent authorities in implementing cross-border declaration requirements and on related issues.

3.3 Effectiveness: Immediate Outcome 6 (Financial intelligence)

3.11. The FIU works with a wide range of informative, and in many respects unique, public and restricted access databases (see Chapter 1 for further details). These are available directly to law enforcement. For example, an agency can determine, online and in a timely way, the date of birth, addresses, employment status, domestic shareholdings and annual declared income of a subject. The breadth of readily accessible information gives LEAs significant assistance in the investigation of ML, associated predicate offences and TF. The FIU provides significant added value to this capacity, by producing bespoke analysis, working with this and the other data available to it, such as STRs (which are often the trigger for such work) and the information it can obtain from relevant reporting entities.

3.12. Typically, financial intelligence products are developed organically by the FIU, often following the initial receipt of an STR. This practice has evolved as a result of the focus of its statutory powers. That is, once an STR has been received from an entity with an obligation to report, the FIU can require that reporter to provide it with all necessary information concerning the transaction and the suspicion.

3.13. The FIU has a total of 18 staff, including 10 analysts, one of whom is a strategic analyst. This post has only recently been re-filled on a permanent basis, following the departure of the previous permanent strategic analyst 18 months ago. Thus, although the FIU now has the capability to conduct strategic analysis, the proactive generation of leads and other products for law enforcement agencies, compared to reactive operational work, is not a priority and no strategic analysis has been produced since 2011. The FIU's effectiveness in this regard is limited.

3.14. With respect to STRs being a trigger for much of the FIU's intelligence development, Norway drew attention to the connection between the analyses and products of the FIU and the quantity and quality of STRs. The FIU and ØKOKRIM have also expressed concern about the number of STRs and about their variable quality. A large number of STRs appear to follow from the reporting sectors' attention to smaller cash based transactions rather than larger, more complex, transactions which are connected to serious crime (see

Chapter 5 below). This in turn affects the FIU's ability to conduct larger and more complex analyses and thus its ability to disseminate information to the police in relation to such cases.

3.15. Despite this, on the basis of available material the output of the FIU is good in terms of operational analysis and cases are ready to be taken on by the police. This is demonstrated by the fact that the intelligence packages produced are in many instances at a sufficient level for the FIU to open an ML investigation on its own initiative, and for the FIU and prosecutors to move the case from the intelligence phase into the criminal law regime. However, as discussed below, a significant factor in this is the extent to which the police are willing and/or able to take on and follow up FIU cases.

3.16. Another significant positive is the degree to which the FIU is able to exchange information and collaborate with foreign partner FIUs, often through the Egmont Secure Web.

Box 3.1. Case example: FIU cooperation and analysis

In 2009, the FIU was contacted by an overseas sister unit in connection with an analysis of an assumed CO2 fraud case. The foreign unit discovered that considerable sums of money had passed through Norway. FIU investigations showed that STRs were not sent for these transactions. However, searches in the Registry of Cross Border Transactions and Currency Exchange revealed that NOK 8 billion (EUR 1.04 billion) had passed through a euro account in a Norwegian financial institution. These accounts had been established with the use of a poor copy of a foreign passport.

Use by competent authorities of financial intelligence and other related information

3.17. The FIU's intelligence products are disseminated to both LEAs and administrative agencies. Specifically, Intelligence Reports are distributed to police districts, the Intelligence Services and Administrative Agencies, including the Tax Administration and Customs. Intelligence placed by the FIU on *Indicia* will in practice be focused upon individuals that are 'known to police'. *Indicia* does not allow for the uploading of documents. Thus an *Indicia* user seeking additional information (e.g., bank statements) would need to contact the FIU. In practice, this makes for a two staged process because in many instances law enforcement users will only be able to see on *Indicia* that the FIU has information about a subject and, until they have applied to the FIU for that data, received and analysed it, they will have no idea how useful it may be. Thus, some agencies do not pursue every potential request for additional data. Some individual police users of *Indicia* indicated that they found the system "cumbersome" and often did not consult the FIU about further information. This limitation is exacerbated by the fact that law enforcement requests for data are the only tangible feedback to the FIU about the material it places on *Indicia* (see below). Accordingly, in light of the combination of: the lack of readily accessible useful data that can be placed on *Indicia*; the dampening effect upon follow up requests to the FIU; and the lack of feedback to the FIU about the quality of the material it has supplied and/or could supply, the use of *Indicia* for non-targeted disseminations is of limited effectiveness.

Table 3.1. Disseminations made by the FIU to law enforcement authorities

	2010	2011	2012	2013
Ongoing cases and charges	18	18	11	27
Intelligence reports - police	121	137	144	62
Information to Indicia	116	235	444	318
Intelligence reports – administrative authorities	90	81	68	28

Source: data provided by Norway

3.19. These limitations do not apply in relation to disseminations to ØKOKRIM and the PST which both appear to be effectively using financial intelligence and other relevant information in the investigation of predicate offences and TF, respectively. In the context of ØKOKRIM investigators and the FIU, this is perhaps to be expected, given that they are part of the same agency. The assessment team was given good examples of the follow up that takes place in the form of cases that have proceeded to trial.

Box 3.2. Case example: use of financial intelligence by ØKOKRIM

Cooperation between the FIU and ØKOKRIM led to the conviction of a former lawyer for economic crimes including embezzlement, with key information obtained by the FIU and provided to investigators. In another case, the conviction of a target for aggravated corruption was obtained, where the case was initiated by the FIU.

3.20. The PST receives detailed and effective disseminations from the FIU, in the form of detailed written intelligence reports. Disseminations from the FIU to the PST are based upon a high level agreement between them. The disseminations are enhanced by the PST's continuous link to the FIU, through regular weekly or bi-weekly meetings between analysts for the two agencies, which keep the FIU informed about areas of interest; and by the use of secondees, of which there are currently two, to read and assess FIU material. Indeed, the PST has confirmed that it sees all TF related STRs as soon as they are received by the FIU. The PST's investigations into terrorism and its financing make good use of the available financial intelligence and other relevant information.

Box 3.3. Case example: use of financial intelligence by PST

In one case the PST commenced an investigation after receiving an STR from the FIU. The PST carried out the investigation in cooperation with the FIU and led to convictions for offences related to terrorism in the District Court and Court of Appeal. This case has since been appealed.

3.21. Effective use of financial intelligence is evidenced by disseminations from the FIU to the Tax Administration. Although disseminations are made to the Tax Administration for civil tax recovery purposes, given the Administration's non-criminal remit, in many instances the intelligence or information involved concerns ML or activity related to a predicate offence. The Tax Administration holds FIU Intelligence Reports in high regard, with one official highlighting their added value by stating that 'it is considered gold'. They place particular emphasis upon not just the raw material, but also upon the analyses and hypotheses. The Tax Administration also confirmed that of 323 disseminations received in 2013, they were able to work on all but 50 of these cases for further inquiries and for tax recovery. Of these, 19 were remitted back to police forces for criminal investigation, as a result of the Administration's use of its accounting expertise in building a clearer picture and/or obtaining evidence of criminality.

Box 3.4. Case example: use of financial intelligence

In one case in the building and construction industry, by analysing FIU reports, the Tax Administration became aware that contractors were using fictitious invoices from sub-contractors to hide undeclared work. The sub-contractors were assessed to be largely ML entities and the Tax Administration assessed the extent of this type of evasion to be so widespread that it required notification to the Ministry of Finance (MoF) for additional funds to support extra efforts in that area.

3.22. It is worth noting that, as an agency without a law enforcement function, the Tax Administration does not have access to *Indicia* and accordingly receives its FIU Reports in written form, with relevant attachments, for example bank statements, included. The Tax Administration may therefore be in a better position than regular police forces, which can only access such additional material upon request to the FIU.

Areas where financial intelligence and other relevant information is not being used

3.23. While it is apparent that some competent authorities are using these financial intelligence packages, it is not clear to what extent they are being used or that they are being used consistently or effectively in ML investigations. Specifically, there has never been a detailed enquiry to see how many large and complex criminal cases that involve the proceeds of crime, have elements derived from STRs as part of the evidence used. Indeed a look at the larger criminal cases in Norway in recent years seems to suggest that there are only a limited number of cases where STRs have been involved. Moreover, given the number of ML prosecutions it appears that STRs do not lead to or play an important role in ML cases being prosecuted.

3.24. Recent Director General of Public Prosecutions (DGPP) annual circulars have stressed the importance of using FIU intelligence; however the police and KRIPOS do not in practice prioritise its use. While there has been good use of FIU financial intelligence by each of ØKOKRIM, the PST and the Tax Administration, this rarely appears to be the case for most of Norway's 27 police districts and KRIPOS. There is no strategy within the police districts for the assessment and progression of ML cases, whether as a result of a dissemination from the FIU or otherwise. Thus, it is not clear to what degree financial intelligence and all other relevant information is appropriately used by police districts or bodies such as KRIPOS for ML investigations.

3.25. Many of the intelligence products offered directly by the FIU are not taken up and some of the cases taken on are subsequently dropped. As a result of the lack of engagement from most districts, the FIU has been obliged to devote some of its limited resource to marketing its cases to investigating agencies. It is apparent that such marketing depends upon the personal contacts and powers of persuasion of the operational individuals concerned.

3.26. A number of factors may explain why FIU intelligence provided to police districts have only been used to a limited extent. These include a lack of resources and expertise, and lack of co-ordination within the designated law enforcement agency to follow through with targeted investigations and prosecutions. The Police Directorate has performed a short survey on this topic. However, with few respondents, the survey gives only an indication of the degree to which the financial intelligence and other relevant information are accessed and used in investigations. Police districts clearly regard FIU information as useful, and they value the co-operation with the FIU, although some smaller districts indicate that they have little contact with the FIU. Even in Oslo, the largest police district, contact is also limited. Oslo police district has guidelines concerning criminal cases, but these do not cover the dissemination of ML cases from the FIU to the district.

3.27. In seeking to deal with these issues, the Ministry of Justice (MoJ) supported the FIU's outreach function through the *Round Norway* project in late 2013. This followed the budget for 2013-14 which stated that the police districts must make better use of the information from the FIU; and that the FIU should visit all police districts from 2013-2014 to assist them on how to use information from the systems *ASK* and *Indicia*. As of mid-April 2014, the FIU had met with 18 of the 27 police districts to raise awareness of the FIU. It also successfully targeted a number of banks with a view to improving the quality and quantity of their STRs.

Use of material from sources other than the FIU

3.28. Norway has a range of public registers for shareholdings, companies, etc. which are a rich source of information for the FIU and investigators. The transactions recorded in the Currency Register are regarded as particularly useful. Law enforcement indicated that the data in this Register is useful for both predicate offences and ML investigations, not least because it contains details of every cross-border transaction or transfer, with a value of NOK 25 000 (EUR 3 250) or more. The FIU also has access to and makes effective use of this information in its analysis. The various registers in Norway and other available information on

legal persons are a valuable source of financial intelligence that is used effectively by specialised agencies including the FIU, PST and ØKOKRIM.

Conclusions on IO.6

3.29. The use of the FIU's financial intelligence differs significantly between competent authorities. ØKOKRIM and the PST use it to effectively 'follow the money' in criminal investigations, while its use in the 27 police districts and KRIPOS is limited, and the FIU experiences challenges in getting police to use FIU disseminations. Norway has a well-functioning FIU which develops and disseminates good quality financial intelligence based on a wide range of sources including STRs, various government registries, police information and the currency database. However, the FIU's strong analytical capability is undermined by the low quality of STRs received. In addition, KRIPOS does not emphasise the use of financial intelligence in investigations which is a concern given the risk of drug trafficking in Norway, and there is a lack of expertise among some police districts to use financial intelligence effectively. The uneven uptake by LEAs of FIU disseminations undermines the effectiveness of cooperation. However, the recent *Round Norway* project is a good initiative to improve this situation.

3.30. Norway has a **moderate level of effectiveness** for IO.6.

3.4 Effectiveness: Immediate Outcome 7 (ML investigation and prosecution)

3.31. Norway has a generally sound legal and institutional framework for combating ML. However, a significant concern is that competent authorities do not prioritise the investigation and prosecution of ML. Rather, authorities focus on predicate offences which has led to few ML cases being prosecuted. ML threats have only to a limited extent been assessed by Norwegian authorities as part of the National Risk Assessment (NRA) or the broader criminal threat assessments undertaken. However, the criminal threat assessments by KRIPOS and ØKOKRIM suggest that profit-generated crime in Norway stems from a range of domestic and foreign predicate offences including illicit drugs, fraud and tax evasion. It is not clear that law enforcement and prosecutorial authorities systematically target these ML risks.

3.32. Norway has sound legal provisions and a designated institutional framework that has the capacity to investigate and prosecute ML. However the investigation and prosecution agencies in Norway concentrate on predicate offences rather than on ML offences. In part, this is due to a widely held view that ML is an ancillary crime to the predicate offence. Indeed in s.317 the basic third party ML offence is referred to as "aiding and abetting" the predicate offence, and is part of the same sentence as the offence of receiving stolen goods (*heleri*). This view and approach is reflected in the low number of ML investigations and prosecutions. In addition, statistics regarding ML investigations and prosecutions are incomplete and unreliable (see also R.33), thus making it more difficult to assess the effectiveness of the investigative and prosecutorial regime for ML.

3.33. The Norwegian ML offence is a catch-all offence and, in theory, the offence could be a part of all investigations involving predicate offences generating proceeds. To support and give direction to ML investigations and prosecutions at an operational level, the DGPP sets out in an annual circular letter the types of criminal acts which should be prioritised by the Police and the Public Prosecutors. For 2014, economic crime, including ML, is one of several types of crime that is pointed out as a priority for investigation and prosecution. In this context, the DGPP has also emphasised the importance of active use of confiscation measures, especially in relation to ML. Competent authorities describe the DGPP's circular letters as being important for investigation and prosecution prioritisation. However, as explained below, this is not reflected in the approach taken in practice by investigators and prosecutors.

3.34. Apart from these annual circular letters, the DGPP has also issued more specific guidelines in relation to investigating and prosecuting self-laundering. However, it is understood that while it is clearly stated in the guidelines that the self-laundering offence shall be prosecuted when the ML act could be regarded as a stand-alone offence separate from the predicate offence, the DGPP states that investigating and prosecuting both a predicate offence and self-laundering should be restricted. The guidelines contain several practical

examples of when a prosecution for a predicate offence and self-laundering could be pursued. However, at the same time, the DGPP points to the fact that prosecution should be restrictive about the use of concurrent penal provisions. As a result, it is concluded that prosecution for self-laundering shall be reserved for obvious cases, thus having a dampening effect on self-laundering prosecutions.

3.35. ØKOKRIM has a specialised ML unit which deals with more complicated ML or economic crime cases. The ML Unit consists of prosecutors, police investigators and other specialists such as, tax auditors. The ML team has clearly excellent knowledge, experience and capacity to identify ML and many examples were presented to the team that showed that complex financial investigations are being pursued. However, the focus was often on the predicate offence and confiscation rather than on an ML offence.

3.36. Prosecutors at ØKOKRIM and KRIPOS / NAST clearly prioritise predicate offences rather than ML. It was indicated that often a case starts with a suspicion of ML but in the investigation and prosecution stages the predicate offences are then pursued because they are easier to prove. This approach was confirmed by the examples of important economic crime cases which were investigated and prosecuted and were presented to the assessment team. On a practical level, ØKOKRIM handles serious cases of economic crime. These cases quite often include suspicions of ML.

3.37. Most ordinary criminal cases and sometimes serious cases of economic crime and associated ML are investigated and prosecuted by the 27 police districts in Norway. As indicated in IO.6 above, very few ML cases originate from information from the FIU, and there is a concern that quite a number of the police districts, especially the many small ones, do not have enough capacity and/or experience to handle ML cases. This is reflected in the approach that many of the intelligence products offered directly by the FIU are not taken up or dropped, as mentioned above.

3.38. In this regard the functioning and structure of the Norwegian Police Service has recently been reviewed by a Commission following the Anders Breivik terrorist attack of 22 July 2011. Among the main findings is the conclusion that "the current structure, with its 27 police districts, does not provide the necessary conditions for developing specialist functions or to deal with large-scale serious cases and incidents". The Commission also notes that only the few large police districts have the necessary framework to provide good services and the capacity to develop and maintain robust specialist functions. The Commission therefore recommends, among other things, a reduction in the number of police districts. This finding, if implemented, would be useful to ensure critical mass to build specialist AML investigation capacity to ensure ML and parallel predicate investigations are pursued more effectively.

3.39. As noted in Chapter 2, the limited coordination means that resources in these areas are spread among the involved agencies without there being a national coordination mechanism that should be informed at relevant times about the trends, experiences and resources that exist.

3.40. Investigative techniques like joint or cooperative investigations are used in major proceeds generating offences. Secret coercive measures are not extensively used. Secret communications surveillance can only be used in drug related ML cases or if an act of aggravated ML has been committed as part of the activity of an organized criminal group. Norway provided some limited examples of the use of more sophisticated investigative methods, but the net result is that although financial investigations are pursued, they generally do not appear to use a wide range of sophisticated powers and techniques as part of those investigations.

3.41. Given its responsibilities, ØKOKRIM focuses on a small number of serious economic and environmental crime cases. In the period 2010-2013, ØKOKRIM had cases which resulted in 125 individual convictions, of which 15 persons were convicted of ML in 10 different cases. There were also 3 ML prosecutions in this period which resulted in acquittals. In addition, 8 cases started as ML investigations but in the end were prosecuted as other offences, in line with the preference to prosecute the predicate offence, rather than ML. ØKOKRIM is the most active law enforcement agency in terms of pursuit of ML, but despite this it is a concern that the number of the ML cases remains low. This is a result of the focus of all Norwegian LEAs on the predicate offence rather than ML offence for investigations and prosecutions.

Table 3.2. ML cases by ØKOKRIM

	2010	2011	2012	2013
ML Prosecutions	6	1	4	7
ML Convictions	6	1	4	4
Cases started as ML but prosecuted predicate offence	3	2	3	0

Source: data provided by Norway

3.42. Norway was only able to provide reliable statistics on ML prosecutions or convictions handled by ØKOKRIM. Norway provided summaries of 24 ML cases adjudicated in 2013-2014 through the Supreme Court and Appeals Courts, although these do not represent all ML cases adjudicated in that period. Norway did provide statistics on the ML cases in the police districts as registered in the police case management system STRASAK. However, these have not been included in this report as there are significant concerns regarding their reliability (see below). The registration codes under the STRASAK system are flawed and difficult to interpret and the data for s.317 that has been entered is not reliable, which makes it complicated to identify ML cases. Another complication is that judicial and prosecution decisions usually do not make a distinction between receiving the proceeds of a predicate offence (including receiving of stolen goods) and ML. This is due to the fact that s.317 first paragraph covers both ML and the traditional offence of receiving, and the statistics therefore do not make a clear separation between them.

3.43. On the initiative of the Police Directorate, an analysis of all cases involving violations of s.317 of the Penal Code in the Oslo Police District that were concluded in 2012 has been made. The total number of cases was 1 247, compared to 4 528 cases of violation of s.317 of the Penal Code for the whole of Norway, i.e., approximately 27% of registered cases that year. The analysis showed that the large majority of cases consisted of receiving criminal proceeds, and that the majority of recorded ML cases were incorrectly classified. There were 22 cases recorded as ML by the Oslo Police District in 2012, but of these only five actually involved ML. The analysis also found that of the 34 ML cases concluded by the Police District in 2012, there were 25 ML cases that were incorrectly classified. Of these 34 ML cases, 21 went to court, prosecution was dropped in 3 cases and 10 were discontinued. It is not known how many convictions were obtained. This analysis of these cases demonstrates the unreliability of the statistics provided by Norway.

3.44. As regards other authorities such as KRIPOS and NAST, which pursue organised crime and drug trafficking cases, only a limited number of case summaries (for the period 2013-14) were provided with limited information available on the cases. Based on qualitative information obtained during the on-site visit and the limited number of cases provided, the assessment team concludes that little use is made of the ML offence. Norway provided the assessment team with a small number of significant ML cases that were ØKOKRIM economic crime cases, which were discussed in detail. Immediately prior to the face to face meeting Norway provided short summaries of 24 case examples of aggravated ML cases in 2013 and 2014 which included both successful and unsuccessful prosecutions. In addition, information was provided on another five ongoing cases (post on-site). However, it was not possible at this point to clarify further details about these cases. Most of the predicates were drug trafficking or tax related, and many were self-laundering cases. The conviction rate for the ML offences in the examples provided was over 80%. Given the very late provision of the information and inability to obtain more detail it is difficult to make firm conclusions based on this new material. It does show that the ML offence is used on occasion, including by KRIPOS and police districts, however in most cases it appears that the ML acts are closely associated to the predicate offence, and have been added as an extension of that offence.

3.45. As noted above, the criminal sanctions for natural persons are proportionate to many other similar types of offences in Norway. No comprehensive statistics are available on sentencing, and the only material made available were the cases referred to above. As many of the cases were self-laundering, it is not possible to separate the sentence for the predicate offence from the laundering aspect. It is clear that if it is drug trafficking and associated ML then a noticeably heavier sentence is imposed. In other cases the sentences were in the range of 2-4 years, which includes the sentence for the predicate. Several cases were only for aggravated ML and the sentences ranged from five months to 3.5 years. One case involving a lawyer (see

below) suggests that the sentences for ML may not be significant, even in cases of very serious criminality and it is not clear that they are dissuasive in practice.

Box 3.5. Case example: investigation of ML by a lawyer

In 2013, a lawyer was convicted of several counts of ML under s317 of the Penal Code. The ML took place over a period of eight years with funds coming from different sources and one company, which were the result of fraud offences in the United States, Italy and Norway. ML was conducted through the collection of debts (NOK 1.5 million), purchase of real estate in Spain (NOK 335 000) and transactions to and from the lawyer's client account (NOK 3.4 million and EUR 42 000). The defendant was found guilty in the court of appeal and sentenced to 3 years and 6 months imprisonment and NOK 113 000 (EUR 14 700) was confiscated.

Conclusions on IO.7

3.46. In many respects Norway has a good legal foundation and sound institutional structure for combatting ML which could be applied to effectively mitigate ML risks. However, while financial investigations are being undertaken for predicate offences, a fundamental concern is that the investigation and prosecution of ML is not prioritised by competent authorities. Decisions not to investigate or prosecute ML in the 27 Police Districts often result from a lack of expertise and resources. The specialised agencies such as ØKOKRIM and KRIPOS often decide to investigate and prosecute the predicate offence rather than ML. These factors undermine Norway's ability to effectively investigate and prosecute ML. The authorities could not provide comprehensive and reliable statistics for the investigation and prosecution of ML, there were a limited number of case examples, and information provided by prosecutors and law enforcement did not provide a clearer picture. As a result, there are few ML prosecutions and convictions, many of which appear to be self-laundering, and it is not clear that the sentences applied in practice are dissuasive.

3.47. Norway has a **moderate level of effectiveness** for IO.7.

3.5 Effectiveness: Immediate Outcome 8 (Confiscation)

3.48. Norway has a good legal framework for freezing, seizing and confiscation measures. Criminal proceeds can be confiscated without establishing the precise criminal offence from which the proceeds are derived, and extended confiscation is a valuable power. However, the lack of consistent, reliable and comprehensive statistics regarding confiscation, and seizing and freezing, in combination with a lack of any substantive qualitative information (including case examples), presents a major challenge in assessing effectiveness

3.49. Norway has set clear policy objectives focusing on improving the use of confiscation measures and competent authorities are aware of the need for an increased focus. This is especially true given the general perception that the results of confiscation are not satisfactory. For instance, the policy performance requirement for 2013 from the MoJ to the Police Directorate emphasises that the Police must conduct confiscation investigation in all cases of profit-motivated crime and that the numbers of confiscation requirements are expected to exceed the average for the last three years. The Police Directorate has also provided similar policy objectives to the police districts and special investigative agencies. The Police Directorate has established several initiatives to help improve results. Moreover, in his annual Circular letter (2014) the DGPP also calls attention to the importance of the active use of confiscation measures whenever it is applicable. The Norwegian authorities, including Prosecution, Police, ØKOKRIM and Customs have acknowledged that the policy objective to focus on confiscation has not been successful to date and confirmed during the meetings with the assessment team that the results with respect to confiscation are not satisfactory.

3.50. To support the use of the quite comprehensive confiscation provisions in an effective and coordinated manner, ØKOKRIM produced a handbook on confiscation. It emphasises the importance of confiscation to disrupt and prevent crime and contains explanations and instructive examples of how to secure confiscation, and what to particularly consider about prosecution, trial and confiscation abroad. While this handbook is highly regarded and used by practitioners, it has not yet produced the required results pointing to an effective confiscation regime. Moreover, ØKOKRIM and the Police College have also organised seminars and courses on the subject but again, without clear visible results so far.

3.51. The Police Directorate is in charge of keeping statistics regarding confiscation, and the statistics for 2009-2013 are included in the table 3.3 below. These centrally registered statistics give a nationwide picture and show the number of enforceable confiscation requirements (orders) and the amounts and value to be confiscated. It is the number of confiscation orders that are counted, not the number of criminal cases (there may be several confiscation orders in each case or sentence). This includes both ordinary confiscation (*PC* ss.34 and 35) and extended confiscation (*PC* s.34a). It should be noted though that such confiscation statistics include both court orders for confiscation and cases where the police have confiscated property and this was not contested by the defendant. There is no data on the number of cases or the value of property that has been seized, charged or frozen.

3.52. The Police Directorate highlighted that the number of confiscation orders fluctuate significantly between police districts and from year to year as can be deduced from the table. This is likely linked to the lack of resources and expertise the local police districts are confronted with (see also IO.7 above). However, there is a clear downward trend in the value of the confiscation orders made (see proceeds of crime – amounts), with the amount in 2013 being one third of the 2009 figure. Table 3.3 represent value of confiscation orders made by the courts rather than actual amount of confiscations collected.

Table 3.3. Police districts: Confiscation orders

	2009	2010	2011	2012	2013
Number of confiscation orders					
Confiscation of proceeds, s.34	972	1 011	1 761	1 061	991
Extended confiscation of proceeds, s.34a	94	155	61	359	37
Total	1 066	1 166	1 822	1 420	1 028
Number of objects/goods confiscated					
Number of objects – Confiscated goods, s.35	4 622	4 842	5 442	5 342	5 558
Amount of confiscation orders					
Value confiscation orders (NOK million)	234.5	187.4	135	108	81
Value confiscation orders (EUR million)	30.5	24.4	17.6	14	10.5

Source: data provided by Norway

3.53. ØKOKRIM also maintains statistics on the enforceable orders for confiscation and compensation. The statistics for 2009-2013 are included in Table 3.4 below. Given that ØKOKRIM focuses on a limited number of serious cases, the amounts confiscated can fluctuate from year to year depending on the conclusion of cases that involve significant proceeds. However, it can be deduced from the statistics that there is a significant

upward trend in the value of confiscation orders made for ØKOKRIM cases. The table below represent the value of confiscation orders made in ØKOKRIM cases rather than the value of money actually realised pursuant to confiscation orders and paid into government revenue (see below for further detail). As with the Police Districts, there is no data on the number of cases or the value of property that has been seized, charged or frozen. It contains some information on the amount and number of confiscations made by KRIPOS/NAST, although these are very small amounts.

Table 3.4. ØKOKRIM and KRIPOS: Confiscation and compensation orders

	2009	2010	2011	2012	2013	Average
ØKOKRIM - No. of orders	16	15	12	9	16	13.6
Value (NOK million)	7.5	31.3	61	12.3	34.3	29.3
Value (EUR million)	1	4.1	7.9	1.6	4.4	3.8
KRIPOS/NAST No. of orders			9	18	6	11
Value (NOK million)			1.5	2.2	0.1	1.3
Value (EUR million)			0.2	0.3	0.01	0.2

Source: data provided by Norway

3.54. In practice, seized property is normally taken care of by the Police. However, as soon as there is an enforceable confiscation order the Public Prosecutor, or in some cases the Police, makes an administrative decision on execution of the confiscation, and can sell property or goods that are specifically ordered to be confiscated e.g., cash that is the proceeds of a drug deal. All orders to pay a pecuniary amount (rather than an order confiscating a specific item of property or goods) are pursued as a civil debt by the National Collection Agency (NCA) which is responsible for the actual enforcement of the order and recovery of the assets. As a result, confiscation statistics kept by Norway's Police Directorate and ØKOKRIM (see above) do not show how much money is actually collected but instead, give an overview of the amounts of money ordered to be confiscated.

Chart 3.1 Value of Confiscation orders

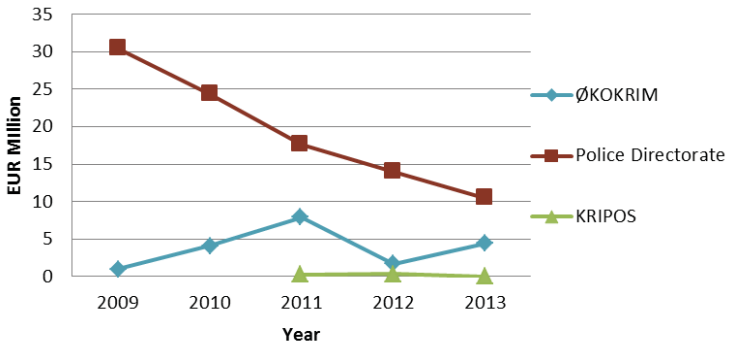


Table 3.5. Amounts recovered from confiscation orders

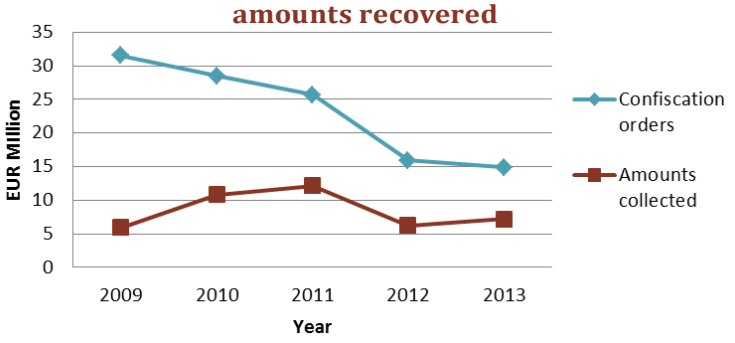
Amounts recovered by the NCA1	2009	2010	2011	2012	2013	Average
NOK million	45.6	83.1	93.4	43.3	55.8	64.2
EUR million	5.9	10.8	12.1	6.2	7.2	8.3

Table note 1: Value of confiscated goods not included.
Source: data provided by Norway

3.55. The NCA is an agency of the MoF and is used by 32 government authorities; not only by the police and prosecution authorities. There is a disconnect between the property seized by LEAs, the confiscation orders that are made and the actual recovery of the proceeds. There do not appear to be any coordination mechanisms between LEAs on the one hand and the NCA on the other hand.

3.56. The value of assets recovered by the NCA is significantly less than the value of assets subject to confiscation orders. Norway indicated that the discrepancy between the amounts in the confiscation orders and amounts collected by the NCA is partly due to the time taken for collection (which may take place in stages) and partly due to unsuccessful collections as proceeds may have dissipated or are hidden. However, the overall picture is difficult to determine as Norway was unable to provide any data on the number and value of assets seized or frozen, and there were only a limited number of case examples provided by authorities which contained limited information. The discrepancy implies that authorities in Norway are not adequately taking action, through the seizure, freezing, or charging of assets, to secure assets and thus deprive criminals of their proceeds of crime. Rather, based on the assessment team's interviews with competent authorities, where there is focus, it is on obtaining confiscation orders at the end of a case.

Chart 3.2 Value of Confiscation orders and amounts recovered



3.57. The value of property (movable or immoveable property) confiscated is not reflected in the confiscation statistics in Tables 3.3-3.5. In practice, when property is confiscated, it is sold without the money being transferred to the NCA. The result of this is that the value of confiscated property, which may be considerable, is not reflected in the court decisions, nor in the police confiscation statistics, or in the statistics of confiscation orders enforced by the NCA. Norway provided information (Table 3.6) on the value of confiscated property realised by all LEAs through the sale. No further information was provided as to the number of assets that were sold. Further, no breakdown on the type of assets was provided. Authorities did advise that a large portion of the value relates to real estate, motor vehicles and luxury items.

Table 3.6. Value of confiscation property realised by all LEAs[1]

Amounts of property sold by police[2]	2009	2010	2011	2012	2013	Average
NOK million	24.5	25.1	26.2	23.8	41.3	28.2
EUR million	3.2	3.3	3.4	3.1	5.4	3.7

Table notes:

1. The relation between these figures and Tables 3.3-3.5 are unclear given that these were provided late in the assessment process and the assessment team did not have the opportunity to discuss with the Norwegian authorities.
2. Values are estimated as the statistics provided included non-recovered property. Norwegian authorities estimate that less than 1% relates to non-recovered property so the figures were reduced by 1%.

Source: data provided by Norway

3.58. It is clear that the results in terms of amounts confiscated vary considerably both from year to year and between agencies. Given that the level of confiscation orders and the value of confiscated assets realised is relatively low, the levels and fluctuate significantly based on individual cases in any one year. For example, the increase in 2013 of realised confiscated assets is largely a result of an ØKOKRIM case in which an expensive real estate property was realised. It is a concern that confiscation orders in police cases are declining considerably and that orders made for KRIPOS/NAST, responsible for serious drugs and organised crime cases are negligible. There are some good qualitative examples of successful confiscation; but these are isolated cases.

Box 3.6. Case example: the Tordenskjold case

The Tordenskjold case, handled by ØKOKRIM, concerned fraud and breach of trust by the chairman and CEO against a publicly listed Norwegian shipping company (Tordenskjold ASA). Funds were stolen through the purchase and sale of vessels, and unauthorised commissions. Dividends went through various accounts in tax havens and other jurisdictions to the accounts of foundations abroad. ØKOKRIM made significant use of international cooperation, including informal contact with their counterparts and formal mutual legal assistance, to determine the ownership and control of the identified accounts. Evidence was gathered from a range of jurisdictions including Guernsey, Switzerland, Denmark, Spain and Belgium. In October 2013, the Supreme Court upheld the confiscation of the proceeds of crime abroad, despite the fact that the formal account holders were not made party to the case. Nearly NOK 30 million (EUR 3.9 million) was confiscated and is expected to be returned through asset sharing arrangements.

3.59. In general however, the available data suggests, and this is confirmed by the representatives from all LEAs and prosecution services, that the actions taken and the results achieved regarding the confiscation of criminal proceeds is not adequate and needs to be improved in Norway. It is difficult to make precise judgments given that there is virtually no information on the risks and the possible value of criminal proceeds in Norway (whether domestic or foreign), and that there is only partial data on the value of property seized, confiscated and recovered. However it is concerning that the value of confiscation orders in Police Directorate cases had, by 2013, declined to about EUR 10 million, one third of the 2009 figure. Furthermore, it is not clear how much of this is actually recovered. Also, the amount confiscated by KRIPOS/NAST, which is responsible for serious drug trafficking and organised crime cases, is negligible. Importantly, and despite clear policy objectives, strong legislation and areas of expertise, the universal view of authorities is that the confiscation system is not effective.

Cross-border declaration and seizures

3.60. The NRA finds that Norway has significant currency smuggling risks. A study by Customs in 2007 estimated that approximately 1.5 billion NOK (EUR 195 million) was smuggled out of Norway in that year. The FIU also noted that there is a large volume of NOK exchanged in Baltic countries and a widespread involvement of Baltic organised crime groups in Norway as a contributing factor for this trend. Norway has a sound legal framework in place for the declaration and identification of cross-border movements of funds. There is evidence that the system is implemented in practice but has only produced limited outputs when contrasted with the risks of cross border movement of cash and BNI. The cross border declaration system has produced some results, including through cooperation with foreign partners, as shown by the outcome of the Atlas and Athena operations set out below. Norway provided the following examples of currency seized through international cooperation (see also IO.2 below):

Box 3.7. Case examples: currency seizures

September 2008 – NOK 880 000 (EUR 114 400): The seizure was made from a passenger travelling by plane from Oslo to Sri Lanka. Money was detected in the person's hand luggage and clothes.

October 2009 – NOK 303 000 (EUR 39 390): The seizure was made from a bus passenger travelling from Oslo, Norway via Sweden to Lithuania. Money detected was hidden in lining of suitcase.

April 2010 – NOK 415 000 (EUR 53 950): The seizure was made from the driver of a car leaving from Larvik, Norway to Denmark on a ferry. Money was detected in lining of a holdall.

October 2012 – NOK 692 900 (EUR 90 077): The seizure was made from a passenger travelling by plane from Bergen, Norway to Poland. Money was detected among clothes in checked baggage.

3.61. Norway also provided the following figures regarding the total number of declared cross border movements of cash and BNI and seizures of cash:

Table 3.7. Cross- border declarations (cash and BNIs)

	2011[1]	2012	2013	Average
Total number (In)	1 338	1 214	1 213	1 225
Total amount (In) (NOK million)	190	137	101	428
Total amount (In) (EUR million)	24.7	17.8	13.4	55.6
Total number (Out)	6 893	7 825	9 321	6 010
Total amount (Out) (NOK million)	467	517	559	385.8
Total amount (Out) (EUR million)	60.7	67.2	72.7	20.2

Table note 1: From March 2011, Customs was given the legal basis to issue an administrative fine for minor cash smuggling. Therefore, the figures for 2011 represent a partial estimate of the cases that would have been given a fine.
Source: data provided by Norway

3.62. One point that is very noticeable from the data is that a lot more cash and BNI are being taken out of Norway than are coming into the country. This is increasing both in terms of number of declarations and value. It is also striking that the number of cases where money was seized remains relatively stable over the period 2009-2013, and the value of such seizures even appears to be declining. One would expect that more experience regarding implementation would also lead to an increased detection of the breaches of the legislation, especially given the sharp increase in the number of declarations made. This finding points to a serious issue regarding the effective implementation of the declaration regime.

Table 3.8. Cross-border seizures of cash and BNIs

		2009	2010	2011	2012	2013
Police reports	Number	136	139	96	91	73
	Value (NOK million)	16.7	19	16.4	8.8	7.4
	Value (EUR million)	2.2	2.5	2.1	1.1	1
Admin. fines	Number			794	801	903
	Value (NOK million)			39.7	37.4	43.1
	Value (EUR million)			5.2	4.9	5.6
Total cash seized	Number	627	967	890	892	976
	Value (NOK million)	42.7	58	56.1	46.2	50.5
	Value (EUR million)	5.6	7.5	4.3	6.0	6.6

Source: data provided by Norway

3.63. Both Customs and Police authorities have acknowledged, during meetings with the assessment team, that there is further room for improvement in implementing the legal framework. Customs authorities are currently working on developing new guidelines for customs officers, including on administrative fines which can be imposed since 2011.

3.64. If customs authorities suspect that any amount of currency or BNI carried by a person is associated with a crime punishable by imprisonment for more than six months, then regardless of whether a declaration has been made, Customs must report the case to the police/prosecutor for further investigation. In addition, as a general rule, all declarations of cross border movements of funds of NOK 500 000 (EUR 65 000) or more are handed over from the customs authorities to the police. Referrals are however not systematically picked

up by the police because of a lack of resources or other priorities. As a result, many opportunities to seize and confiscate, or to follow up on cross border ML or other criminality are not taken up.

Conclusions on IO.8

3.65. Norway has a strong legal framework for the freezing, seizing and confiscation of criminal proceeds. However, despite authorities making confiscation a policy priority, results are not satisfactory. There is a lack of statistics regarding freezing and seizing. The data that is available for confiscation shows a steady decline in the amounts confiscated. Despite the fact that there are some good confiscation case examples, and that the authorities seek to confiscate all types of property, using extensive powers, the key objective of depriving criminals of their proceeds is not adequately met. The level of confiscation varies considerably from year to year, and change significantly year to year based on single cases. It is a concern that confiscation orders in police cases are declining considerably and that orders made for KRIPOS/NAST, responsible for serious drugs and organised crime cases are negligible. In addition, the value of assets actually confiscated is considerably less than the value of the confiscation orders. Further, authorities only provided a limited number of case examples where assets were frozen or seized, and subsequently confiscated. It is difficult to determine why the system is less effective than it should be, and further analysis should be done to examine this issue in more detail. From the available information, and as confirmed by the authorities, it is clear that the confiscation results achieved are less than expected and significant improvements are necessary.

3.66. Norway has a **moderate level of effectiveness** for IO.8.

3.6 Recommendations on legal system and operational issues

FIU and financial intelligence

a. The FIU should enhance its strategic analysis function.

b. The Police Districts and KRIPOS should enhance their use of financial intelligence, particularly the disseminations by the FIU.

c. Norwegian authorities should more clearly delineate the powers of the Supervisory Board in relation to data which the FIU receives and processes, including the extent to which the Board can require access to live operational data.

ML investigations and prosecutions

d. Law enforcement agencies should prioritise and give investigative focus to further utilising financial intelligence and the ML offence to target organised crime, tax offences, foreign proceeds of crime and other high threat areas.

e. The MoJ and the National Police Directorate should ensure that police districts have appropriate expertise and resources to use financial intelligence, to target and progress ML cases and parallel predicate investigations and make more effective use of confiscation powers and tools.

f. ML should be clearly made a stand-alone offence.

g. Norway should use the DGPP's statutory authority to improve the effectiveness of the use of the ML offence, for example, through issuing guidelines or instructions.

Confiscation

h. Norwegian police and prosecution authorities should continue to prioritise the confiscation of proceeds of crime and examine the complete chain of action to determine why actions to confiscate and recover criminal proceeds are not effective, including any legislative or institutional framework issues.

i. Norway should establish and implement procedures and processes for the management of frozen or charged property before and/or after confiscation.

4 TERRORIST FINANCING AND FINANCING OF PROLIFERATION

Note this chapter sets out the assessment of the Recommendations and Immediate Outcomes which are specific to terrorist financing and the financing of proliferation. The legal and operational measures set out in the previous chapter are relevant to countering both money laundering and the financing of terrorism.

Key Findings

- Norway has a sound legal framework for criminalising terrorist financing (TF), with the exception of the technical gaps in the offence. However, they do not appear to have undermined effectiveness.
- Norway is focusing its investigative resources and international cooperation efforts into conducting a small number of investigations related to terrorism and potential TF charges, based on its understanding of TF risks. The use of financial intelligence is integrated into all of the Norwegian Police Security Service's (PST) investigations. Given the context of terrorist risks in Norway and the security and law enforcement roles of PST, the objective of the outcome is achieved, at least in part, by employing other criminal justice measures to disrupt TF activities where it is not practicable to secure a TF conviction.
- Norway has only had one TF prosecution which did not lead to a conviction. However, this appears to be generally in line with TF risks.
- Norway has a sound legal framework for the freezing of terrorist assets under the UN sanctions regime (UNSCR 1267), though technical deficiencies exist. Banks have a good awareness of the freezing obligations, though implementation outside the banking sector is varied and limited. Effective implementation is undermined by the poor implementation of customer due diligence (CDD) requirements relating to beneficial ownership (see Immediate Outcome (IO) 4). Norway has implemented only certain aspects of targeted financial sanctions pursuant to UNSCR 1373, as required by Recommendation 6. The terrorist asset freezing mechanism under s202d of the *Criminal Procedure Act* (*CPA)* can only be used as part of an ongoing criminal investigation and does not establish a prohibition from making funds available to persons subject to a freezing action under this mechanism. As a result, Norway is unable to use targeted financial sanctions as an effective tool to combat TF.
- Norway has taken other action to prevent terrorists from moving funds using other asset freezing and confiscation measures. However, at the time of the on-site visit, the mechanism under s202d of the CPA had only been used in one instance. When terrorist and TF cases are made public, Norway has instead taken action to secure funds using asset confiscation and charging provisions.
- Norway has recognised the TF risk profile for non-profit organisations (NPOs) and has taken steps to effectively implement a targeted approach to the part of the sector responsible for the bulk of overseas NPO activity.
- Norway has taken measures to implement targeted financial sanctions for proliferation financing (PF) and financial institutions have frozen bank accounts of designated persons under this framework. However, the delays in transposing designations made by the UN into Norwegian law are a concern as targeted financial sanctions for PF are not implemented without delay. In addition, implementation outside the banking sector is varied and limited, and the lack of supervision of all reporting entities for these obligations is a concern.

4.1 Background and Context

4.1. **The PST's** main objective is to prevent and disrupt criminal activities threatening the security of the state of Norway, and PST is also the agency responsible for the law enforcement/criminal investigation of TF offences. The PST is a security service with police and prosecutorial capacities. Counter-terrorism and CFT are highly prioritised. In theory cases about terrorism and counter-terrorist financing (CFT) could be handled by any Police District. In practice such cases are dealt with only by the PST during both investigation and prosecution. Therefore, the PST generally has responsibility for investigations and certain prosecutorial decisions relating to the TF offence in s147b and s147d of the *Penal Code*. Court cases are normally prosecuted by NAST, but could also be prosecuted by PST. Cooperation with the regular Police, Customs, other authorities and the Foreign Ministry is highly developed. Also the cooperation with Services of other countries, especially the other Nordic countries and the members of the Bern Club is frequent and well- functioning. Budget money is allocated in relation to threat anticipated in the PST's annual assessment. The legal provisions for the regular Police and Prosecution concerning investigation and prosecution also apply to the PST. The PST has the possibility to use, before a formal investigation has been initiated, coercive measures to prevent TF. These measures include secret search, concealed video surveillance and technological tracking, audio surveillance and communication control and covert audio surveillance.

4.2. **The Ministry of Foreign Affairs (MFA)** is responsible for ensuring implementation of the targeted financial sanctions relating to TF and PF, and **the Financial Supervisory Authority *(Kredittilsynet)* (FSA)** is responsible for monitoring the compliance of the requirements by reporting entities. The targeted financial sanctions pursuant to UNSCR 1267/1989 and 1988 are implemented by an enabling statute, and the *Regulation on sanctions against Al-Qaida* of 22 December 1999 and the *Regulation on sanctions against Taliban* of 8 November 2013. Norway has a mechanism under s202d of the CPA which allows authorities to freeze terrorist assets as part of an ongoing criminal investigation.

4.3. The targeted financial sanctions relating to proliferation are implemented by the *Regulation on Sanctions against Iran of 9 February 2007* (the *Iran Regulations*) and *Regulation No. 1405 relating to sanctions and restrictive measures against North Korea of 15 December 2006* (the *DPRK Regulations*). The approach to the two regulations differs as the *DPRK Regulations* adopt the EU framework in the *European Council Regulation (EC) No. 329/2007*. The Iran Regulations do not rely on the EU framework, although they reflect the EU regulations.

4.4. Norway has a very active NPO sector with a large range of domestic NPOs supported by well organised umbrella organisations. Norway also has a strong network of larger NPOs active in charitable and human rights activities outside of Norway, including in conflict zones with significant security and potential terrorism risks. This latter sector is largely funded from public sector sources, reflecting the active role of domestic donors and the government of Norway to assist humanitarian causes. The levels of licensing or registering NPOs vary in Norway, and all such registrations are voluntary. Only 108 NPOs are licensed with the Foundation Collection Control under the *Act on the Registration of Charitable Fundraising*. This includes almost all of the largest NPOs which conduct collection of funds and operate in foreign jurisdictions. In addition, these NPOs may have a network of partner NPOs under them. There are 363 NPOs registered with the tax authorities for tax free status. These are all nationally based NPOs and may have a lot of regional/local branches under them. 31 000 NPOs are registered with the Register of NPOs, which is a register initiated by the NPO sector in 2010 to simplify cooperation between the sector and the state. Associations and organisations must register to participate in grant schemes and all such entities must also be registered with the Central Coordinating Register for Legal Entities. NPO sector umbrella organisations estimate that approximately 50 000 mostly small NPOs are not registered at all.

4.2 Technical Compliance (R.5-8)

Recommendation 5 – Terrorist financing offence

4.5. Norway is rated largely compliant (LC) with R.5. While Norway has a generally sound legal framework for the criminalisation of TF on the basis of the TF convention and R.5, there is a technical deficiency. There

are two TF offences in s147b of the *Penal Code*. Firstly, it is an offence to obtain or collect funds or other assets with the intention that they should be used (in full or in part) to finance terrorist acts: *s147b, first paragraph*. However, the provision of funds with the intention that they be used to carry out terrorist acts is not clearly criminalised, although this could be covered under the second paragraph. Secondly, it is an offence to make funds or other assets, bank services or other financial services available to terrorists or terrorist organisations, or person or enterprise acting on behalf of a terrorist or terrorist organisation: *s147b, second paragraph*. However, Norway has not criminalised as a stand-alone offence the collection of funds in the knowledge that they are to be used for any purpose by a terrorist individual or organisation. Norway noted that this conduct is criminalised as an attempt to make funds available to terrorists or terrorist organisations: *s.147b, cf s.49, PC*, though this has never been considered by the courts. It is noted that such conduct could also be criminalised as aiding and abetting a terrorist act, even though this is not sufficient to meet the requirements of R.5. Criminal sanctions for the TF offence are up to 10 years imprisonment for natural persons. Criminal liability applies to legal persons who are punishable by a fine or restrictions on the right to carry on a business. In addition, the act of establishing, joining, recruiting members or providing financial or material support to terrorism is an offence: *s149d, PC*.

Recommendation 6 – Targeted financial sanctions related to terrorism and terrorist financing

4.6. Norway is rated partially compliant (PC) with R.6. The *Al-Qaida Regulations* and *Taliban Regulations* establish a sound legal framework to implement targeted financial sanctions pursuant to UNSCR 1267/1988 and 1989 (the UN Taliban/Al Qaida sanctions). The regulations require all persons to freeze the assets of designated persons without delay and prohibit anyone from making funds available to or for the benefit of designated individuals and entities. The designation lists are automatically updated in Norwegian law. Therefore the freezing obligation and prohibition of making funds available occur without delay. The FSA has issued guidelines to assist financial institutions (FIs) and designated non-financial businesses and professions (DNFBPs) to implement these requirements.

4.7. Norway has sought to implement targeted financial sanctions through a mechanism in the *CPA* (s202d). However, it implements only certain aspects of the targeted financial sanctions pursuant to UNSCR 1373 as required by Recommendation 6, and serious deficiencies remain. This mechanism allows the PST or prosecutor to freeze terrorist assets on the basis of suspicion without going to court, and it must then be brought before the court within 7 days. The freezing order can either list the identified funds or assets that are known or can include any assets owned by the person. This can include present or future assets. The order must be renewed every four weeks by the court, but the court may set a longer time limit if it deems that a new consideration in four weeks is not required. The decisions of the court are made public. However, this mechanism does not establish a designation mechanism and can only be used as part of an ongoing criminal investigation. Importantly, it does not establish a prohibition from making funds available to persons subject to a freezing action under this mechanism, though the provision of funds to a terrorist or terrorist organisation would be considered a TF offence: *PC* s147b *second paragraph*. These are serious deficiencies.

Recommendation 7 – Targeted financial sanctions related to proliferation

4.8. Norway is rated PC compliant with R.7. While Norway has established mechanisms to implement targeted financing sanctions relating to proliferation that are generally in line with requirements of R.7, delays in transposing designations into Norwegian law are a concern. Both the *Iran Regulations* and the *DPRK Regulations* require all natural and legal persons to freeze the assets of designated persons without delay and prohibit anyone from making funds available to designated persons. Failure to comply with the regulations is subject to fine and/or imprisonment of up to three years. The most significant deficiency is the delay in transposing designations into Norwegian law. The designation lists are contained in annexes to the regulations and are required to be updated when changes are made. For the *Iran Regulations*, this process takes 1-4 weeks. For the *DPRK Regulations*, it is a two-step process as they rely on the EU framework. At the EU level it can take up to 4 weeks to update the EU framework and then there is an additional delay of 1-4 weeks to update the annex of the *DPRK Regulations*. However, the EU regime for proliferation-related sanctions mitigates this problem to a limited extent. Nevertheless, the delays mean that the targeted financial sanctions for proliferation are not implemented without delay which is a serious technical deficiency.

4.9. The FSA has issued guidelines relating to these regulations and anyone who freezes funds under these mechanisms is required to immediately inform the MFA. The FSA is responsible for monitoring compliance by financial institutions and DNFBPs. However, the FSA has not focused on targeted financial sanctions and has only been considered on one occasion as part of a questionnaire to the banking sector in 2013, which included some specific questions on how they implement targeted financial sanctions. The FSA has not undertaken any monitoring of other types of reporting entities outside of the banking sector. Compliance with the regulations has not been reviewed during on-site visits.

Recommendation 8 – Non-profit organisations

4.10. Norway is rated LC with R.8. Norway has taken steps to enhance the transparency of the NPO sector and mitigate the risk of NPOs being misused for TF. The PST considers NPO sectors' TF risks in the PST annual threat assessments. The MFA considers the risks of the network of larger NPOs which account for (i) a significant portion of the financial resources under the control of the sector; and (ii) a substantial share of the sector's international activities. These NPOs are predominantly funded by the Norwegian government through the MFA. Authorities have engaged with the NPO sector including the Ministry of Culture when reviewing the adequacy of the operation of the legal framework, the MFA with those larger NPOs operating internationally, and the Ministry of Justice (MoJ) which published the *"Guide on how to avoid terrorist funding: Your contribution can be misused"* in 2012. The PST has an ongoing and targeted outreach to NPOs and relevant organizations, in collaboration with some selected police districts.

4.11. Norway has pursued policies to promote transparency, integrity and public confidence in the administration of NPOs through mostly voluntary measures. There are no mandatory requirements for NPOs to register, however policies support NPOs registering on a voluntary basis due to incentives, including favourable taxation treatment. Also, any NPO opening a bank account needs to be registered in the Brønnøysund Register, which ensures registration of some basic information. The MFA requires a number of controls for the NPOs it funds, including registration, reporting on the use of funds, providing statements of income and expenditure, and 'know their beneficiaries and associated NPOs'. Given the largely voluntary nature of registration of NPOs in Norway, sanctions appear to be limited to the removal of benefits accruable to NPOs (e.g., public funding and tax-exempt status).

4.3 Effectiveness: Immediate Outcome 9 (TF investigation and prosecution)

4.12. As outlined in Chapter 2 at Section 3, the authorities demonstrated a good understanding of the risk and context of TF based on the PST´s work on annual threat assessments and the work of the MFA on TF risks, and undertake their work on the basis of the TF risks identified. The TF risks include small scale domestic collection, provision and use of funds for radicalised persons at risk of being involved in politically motivated violence in the form of Islamist extremism both in Norway and abroad.

4.13. The Commission of the 22 July 2011 has in its report (NOU, 2012) analysed what was done before, during and after the terrorist attacks perpetrated by Anders Behring Breivik. The Commission's constructive criticism has among other things resulted in a review of the Norwegian police organisation. On the part of the PST the Commission´s findings about how tips and certain kinds of information were dealt with has led the PST to introduce new and more adequate methods in this area. The reorganization of the PST was completed on 1 March 2014. The new organization includes a new function which shall deal with tips and certain kinds of information from other services and the public immediately after receiving it.

4.14. Norway is focusing its investigative resources and international cooperation efforts into conducting a smaller number of financial investigations related to terrorism and potential TF charges, based on its understanding of TF risks. The PST indicates that investigations often identify roles played by terrorist financiers, but in the majority of cases investigations do not result in prosecutions for TF. Some cases have been dropped due to the limited chances of prosecution given the lack of evidence, while other investigations have involved early intervention as a preventive measure by the PST before gathering sufficient evidence for prosecution. It is apparent that financial investigations of terrorist groups and terrorist financiers are conducted by the PST making use of a wide range of investigative techniques and sources of financial

intelligence including cooperation with the financial intelligence unit (FIU) and other domestic authorities and international partners. The degree to which the PST uses the legal provisions and other methods is classified. It is worth noting that anyone can read on the PST official website that, for instance, s.222, CPA is used and what coercive measures this section makes available.

4.15. The PST has a close working relationship with the FIU and the National Authority for Investigaton and Prosecution of Economic and Environmental Crime (ØKOKRIM), and makes use of suspicious transaction reports (STRs) in its investigations into terrorism and TF. The PST has had one successful prosecution for terrorism offences in the NEPTUN case. The District Court found the defendant guilty of terrorism offences and the Court of Appeal upheld this decision. This case is ongoing as the decision of the Court of Appeal is appealed. In this case, the investigation was started by an STR which was reported to the PST from the FIU. Investigators from ØKOKRIM assisted the PST in their investigation, particularly for their financial investigation expertise.

4.16. Norway has only had one TF prosecution, which did not result in a conviction. The summary of this case is outlined below.

Box 4.1. Box 8 – TF prosecution

In 2009, a suspect was charged with TF under s147b PC based on sending funds through his illegal hawala operation to the Somali terrorist organization al-Shabaab. This was an extensive investigation which demonstrated the PST's use of a range of investigation techniques in TF investigations including secret communications surveillance, communications control, and electronic seizures. In the trial (Sentence 6 December 2010 by the Oslo District Court), a considerable part of the evidence consisted of a great number of telephone conversations from secret communications surveillance and communications control of the accused persons. In another trial for an offence of planning and preparation for a terrorist offence (Sentence 30 January 2012 by the Oslo District Court) important evidence was presented in the shape of several conversations on both telephone and e-mail from secret communications surveillance, covert audio surveillance, from both house and car, and communications control. In the TF case Norway also had fruitful cooperation with two countries in the European Union.

In this case, the accused was acquitted of TF in both the district court and the court of appeal as it was not demonstrated that Al-Shabaab, the organisation to which the funds were sent, was a terrorist organisation. Norwegian authorities undertook a significant effort to document the ideology and activity of Al-Shabaab. However, the accused was acquitted as the evidentiary burden was not met based on the facts of the case.

4.17. The PST also uses other legal measures to prevent and disrupt TF activities when the outcome of an investigation is doubtful. In the TF case, while there was no TF conviction, the accused was convicted of breaching the Somalia embargo and his funds were confiscated upon conviction. In another case in 2013, the leader of an NPO was suspected of TF offences and arrested on the suspicion that he was going to send his son and friend to Syria to join a terrorist organisation. In this instance, the PST considered that a TF conviction was not possible at the time the accused proposed to send them to Syria. The accused was arrested and charged with violations of s147d (recruiting a member for a terrorist organisation) and s224 (slavery offences). The asset freezing and confiscation in these two cases are considered further in IO.10.

4.18. As noted above, TF has been an aspect of several investigations of terrorism, some of which have been dropped, while others are on-going. The PST could not provide further information about the dropped or ongoing cases as the information is classified.

4.19. In the course of TF investigations, the PST is able to quickly and extensively access police data and obtain information from the FIU through well-developed channels. The PST is also able to quickly obtain information held by the FSA, NPO sector regulators, and Customs on the Currency Register. However there

have been some impediments with the pace and breadth of access to information from Customs and Tax due to secrecy obligations. PST reports that the government is working to support closer harmonisation between PST, Tax and Customs. Specifically, a proposal is under consideration where the secrecy provisions will be modified so that information to law enforcemenet agencies (LEAs) (including PST) can be provided by request or at the customs authorities own initiative, when there is "reasonable grounds to examine" whether someone prepares, commits or has committed serious crimes. This will be changed from the current provision, which demands "reasonable grounds to suspect…criminal acts". While this is a positive step, the PST does not consider the current legislation to be a significant obstacle.

4.20. The technical deficiencies with the TF offence identified above have not had an impact on effectiveness, as they have not undermined investigations or prosecutions for TF. No concerns or difficulties regarding the TF offence were raised in the TF prosecution described above.

4.21. Taken into account the obvious evidential challenges in TF cases, the methods available for the PST to prevent and disrupt TF and the risk for terrorist activities Norway faces, it is not remarkable that only one case of TF has been prosecuted. In this context it should also be noted that there have been comparatively few prosecutions for TF within the EU.

4.22. The impression of transparency that the PST´s website brings about, in conjunction with the open and comprehensive report by the 22 July Commission, does supplement the overall efforts to counter terrorism and extremist behaviour.

Conclusion on IO.9

4.23. The overall impression is that TF is investigated and prosecuted in an effective way and that no major improvements are needed. The Immediate Outcome is achieved to a large extent. Norway is focusing its investigative resources and international cooperation efforts into a small number of investigations related to terrorism and potential TF charges. The PST demonstrated a strong understanding of TF risk and targets its investigations and resources based on these risks. Norway has only had one TF prosecution, which did not lead to a conviction as there was insufficient evidence. However, this seems to be generally in line with the TF risks in the country and the legal framework for the investigation and prosecution of TF is generally sound. The FIU and PST work closely together, and use of financial intelligence is integrated into all of PST's investigations. The PST has also used other criminal justice measures to disrupt TF activities where it was not practicable to secure a TF conviction.

4.24. Norway has a **substantial level of effectiveness** for IO.9.

4.4 Effectiveness: Immediate Outcome 10 (TF preventive measures and financial sanctions)

Targeted financial sanctions for TF

4.25. While the legislative framework and mechanisms exist to freeze the assets without delay, and prohibit the provision of assets to, terrorists and terrorist groups designated by the UN under the UN Taliban/Al Qaida sanctions, there are important technical gaps which undermine effectiveness. Given that the obligation on parties to understand if their customers or parties to transactions have any relationship of ownership or control with a UN-designated entity is indirect, it is not clear that guidance supports the implementation of controls to check if a customer or transaction is an entity acting on behalf of or at the direction of a designated entity.

4.26. The FSA has taken some steps to support effective implementation of freezing without delay by providing guidelines to indicate the sources of up-to-date UN designation lists and the need to check for matches through electronic monitoring systems. The FSA also publishes the designation lists on its website. In its guidance, the FSA encourages financial institutions and DNFBPs to monitor the lists published by UN

Sanctions Committees to ensure that they are aware of de-listings as soon as they occur. Norway does not have a mechanism to alert financial institutions, DNFBPs and others to changes to the designation lists and there are no specific measures to communicate de-listings and unfreezing actions.

4.27. The PST has conducted outreach to a number of financial sector entities on a targeted basis to raise awareness of TF risks and the need for mitigation, including the potential risk of assets related to the UN Taliban/Al Qaida sanctions being present in the Norwegian economy. This supports more effective application of controls by the financial sector. The FSA, as the regulator of financial institutions and most of the DNFBPs present in Norway, has not conducted any outreach related to TF sanctions to support more effective implementation.

4.28. From discussions with representatives of various financial institutions, it is evident that the banking sector in particular has a high-level of awareness of the requirements related to UN Taliban/Al Qaida sanctions and is taking action to implement measures. Implementation by other reporting entities is varied and limited. A challenge for effective implementation of sanction screening in Norway is the limited implementation of requirements related to the identification and verification of ultimate beneficial ownership. As set out under IO 4, there are low levels of effectiveness relating to the conduct of CDD which limit the availability of beneficial ownership information to support effective sanctions screening of accounts and transactions.

4.29. Banks and some other reporting entities take a systems-led approach to real-time screening of accounts and transactions for matches with UN-listed entities. This includes screening both customers and beneficial owners, when known, against the lists. To achieve this they rely solely on external service providers for sanctions screening. However it is not clear if the reporting entities or the FSA take any steps to be assured that those private providers are applying the most up-to-date UN designations. It is also not clear that entities outside of the prudentially regulated sectors are applying screening programs or taking many other steps to check customers and parties to transactions against the UNSCR 1267 lists.

4.30. Norway's assessment of TF risk indicates challenges with individuals in Norway affiliated with UN-designated entities. The single case of Norway having frozen property related to UN Taliban/Al Qaida sanctions occurred in February 2003 when the property of a person related to a designated entity (Ansar al-Islam) was frozen (a single bank account containing USD 1 000). In that case, Norway was notified that the entity was being designated and was able to investigate if any related property was held in Norway in order to take action to freeze the property.

4.31. The PST 2013 Threat Assessment highlighted that extremist Islamist groups are small, but support militant Islamist groups in their former home regions, primarily through the collection of funds and several individuals from these groupings have travelled abroad to join these groups and to participate in armed battles. Further to the PST assessment of this trend, press reports in early 2014 indicated that Al-Shabaab issued a statement claiming that a Norwegian national of Somali origin was a suicide bomber killed in an attack on African Union troops in Bulo-Burte, central Somalia in early 2014.

4.32. Norway has never proposed a designation to the UN Sanctions Committees. The MFA indicated that Norway gave active consideration to proposing a designation in one instance, however no information was provided on how the process for identifying possible targets for designation was undertaken.

4.33. As noted above, there are serious technical deficiencies with Norway's implementation of targeted financial sanctions pursuant to UNSCR 1373 as required by Recommendation 6, as the asset freezing mechanism under s202d of the *CPA* can only be used as part of an ongoing investigation and does not establish a prohibition from provided funds to persons subject to a freezing action under this mechanism. These deficiencies mean that competent authorities are unable to target terrorist assets using these measures, which are intended to compliment asset tracing, financial investigations and provisional measures in a criminal context. As a result, Norway is unable to use these targeted financial sanctions as a tool to effectively combat TF. At the time of the onsite visit Norway did not have concrete plans to implement such a mechanism pursuant to UNSCR 1373 as required by Recommendation 6.

Terrorist asset freezing and confiscation, and TF risks

4.34. Through assessments conducted by the PST, the TF risk profile for Norway is, in a large part, well understood by the authorities and clearly articulated in public documents. It is not evident, however, that the measures to deprive terrorists and terrorist financiers of assets have been applied in a way that is consistent with the risk profile.

4.35. The assessment team sought to understand the extent to which implementation of the asset freezing mechanism that is available in the context of a terrorism investigation (s202d *CPA*) may support the effectiveness of Norway's efforts to prevent terrorists from raising, moving and using their funds. The PST or a prosecutor can take freezing action on an *ex parte* basis as part of a terrorism or TF investigation the person whose assets are to be frozen. This mechanism has the potential to freeze terrorist assets in a swift manner on a case-by-case basis, and the PST has procedures to immediately notify the financial institution to ensure that the assets are frozen immediately. At the time of the on-site visit, this mechanism has been used once to freeze terrorist assets. In this instance, the PST, who was aware of the bank account of the suspect, made the freezing order and informed the financial institution which froze funds immediately. The freezing order was first confirmed by the district court (as is required within 7 days), but dismissed by the court of appeal. The court of appeal found no proof of the funds belonging to a terrorist or terrorist organization and considered that they belonged to the individual donors because the funds were in an illegal hawala account used for ordinary transfers of funds. On 23 October 2014, Norway advised that the mechanism had been used in two other cases on 17 October 2014 and 20 October 2014. Given the late stage of the assessment process, the effectiveness of this mechanism in these cases could not be assessed. The Norwegian authorities indicated that this mechanism is only considered when a terrorism investigation has been made public by a prosecutor, of which there have only been a few instances. While there have been other covert terrorism investigations, this mechanism was not considered so as to not alert the suspect and disrupt the investigation.

4.36. Norwegian authorities have frozen and confiscated funds of suspected terrorists using ordinary criminal confiscation measures on three occasions (a description of these measures is in Chapter 3).

Box 4.2. Case examples: other confiscation of terrorist assets

Case 1: The first case was in the TF case outlined in IO.9. While there was no TF conviction, the accused was convicted of breaching the Somalia embargo and funds of NOK 144 000 (EUR 18 720) were confiscated under s3 of the *Act of 7 June 1968 number 4 to carry out the commitment from the United Nations Security Council*.

Case 2: The second case was in the NEPTUN case, Norway's only successful prosecution for terrorism offences, as the authorities confiscated NOK 954 930 (EUR 124 141) from the convicted terrorist under s34, 35 and 37d of the *PC*.

Case 3: The third case was in the case of the arrest of the NPO leader arrested on the suspicion that he was going to send his son and friend to Syria to join a terrorist organisation (as outlined in IO.9). The NPO leader was arrested with NOK 350 000 (EUR 45 500) in cash which was due to be sent to Syria with his son. The PST placed an immediate charge on these funds under s.217 of the CPA which allows the prosecutor to secure specific property by placing a charge against that property in order to secure payment of a fine or confiscation. This is an ongoing case and the accused has agreed for these funds subject to a charge to be used by the Norwegian authorities for charitable purposes.

4.37. These three cases demonstrate that Norway has taken steps to confiscate terrorist assets. In particular, the case of the NPO leader demonstrates the PST's effective and innovative use of asset freezing measures to disrupt the movement of funds suspected of being used for terrorism. Beyond the few cases outlined above, there have not been cases of significant assets being frozen in the context of terrorist investigations. However,

this is largely consistent with the risk profile for TF in Norway and the focus of the PST on a small number of terrorism and TF cases per year.

Non-Profit Organisations (NPOs)

4.38. Norway, in seeking to support the operation of NPOs, takes a number of approaches to avoid disrupting legitimate NPOs by assessing the TF risk profile for Norwegian NPOs. The PST yearly threat assessments consider aspects of the NPO sector's vulnerability to terrorism and TF, particularly risks for NPOs to be used domestically for small-scale collection of funds and material support for terrorism. The PST identifies that these higher risk groups do not control many resource or a significant share of the sector's international activities.

4.39. The MFA periodically identifies vulnerabilities of the network of larger NPOs which are active in charitable and human rights activities outside of Norway, including TF risks in conflict zones and terrorism-prone areas. The MFA works with international partners to assess TF risks in those conflict zones.

Internationally focused NPOs

4.40. The MFA periodically conducts outreach on risk, transparency and compliance to the network of larger NPOs which are active in charitable and human rights activities outside of Norway. These larger NPOs are predominantly funded by the Norwegian government through the MFA and are required to report on the use of the received funds, and subject themselves to control measures. The experience of the regulator and NPOs met by the team indicate that these large NPOs are complying with auditing and accounting legislation. Those which are registered for tax-free status are subject to controls from the tax authority. The MFA, through the Foreign Service Internal Control Unit (FSCU), controls the use of bilateral international development assistance by requiring public information, financial statements of income and expenditure, financial accountability, licensing or registration, "know your beneficiaries and associated NPOs" and record keeping. The FSCU has intensified its efforts to monitor and follow up on misuse of funds by publicly funded programs by NPOs. This has included allocating additional resources conducting risk assessments and on-site inspections which considered elements of TF risk where relevant. There is a concern that effective implementation of controls for those entities which may not be receiving public funding are generally not required to implement all of the controls and standards required by the FATF.

4.41. The FSCU provided data on the financial irregularities cases during the period 2007-12 and outlined findings and sanctions undertaken. The FSCU has identified a significant number of fraud, instances of corruption and other abuses of NPOs and indicated that criminal charges and other sanctions had been pursued in these cases. The FSCU has also detected a small number of instances possibly involving TF, which were referred to PST and international partners.

Domestically focused NPOs

4.42. There has been outreach to the more domestically focused NPO sector; however, this has varied across the sector. In 2012, the MoJ published the "Guide on how to avoid terrorist funding: Your contribution can be misused" and circulated it in Norwegian and several other languages spoken by minority groups in Norway. This Guide was circulated to NPO regulators, self-regulatory and umbrella organisations.

4.43. Reflecting concerns with risks from unregulated collection of funds by NPOs, Norway amended its legal framework in 2007 through the *Act on the Registration of Charitable Fundraising*. The Act established a voluntary licensing regime for the charitable collection of funds by NPOs. The Foundation Collection Control in Norway (established in 1991) was appointed by the Ministry of Culture to administer the voluntary licensing regime. NPOs licensed by the Foundation Collection Control to undertake the collection of charitable funds are required to submit statements of program and financial statements of accounts including fundraising and expenditure. These accounts are available on the Foundation Collection Control website. The Foundation

Collection Control supports transparency and compliance by its 108 licensed NPOs with the required standards.

4.44. The purely voluntary licensing regime for collection of charitable funds has not been effective in providing tools to prevent illegitimate actors misusing charitable fundraising, including possible abuse for TF. Norwegian authorities and the NPO sector have raised concerns that, while the purpose of the *Act on the Registration of Charitable Fundraising* remains valid, its implementation has been inadequate to effectively address the various risks. Following discussion with the NPO sector, the Ministry of Culture commenced a review of the adequacy of the operation of the new Act through an external evaluation involving the NPO sector.

4.45. In the context of domestic NPOs, Norway was unable to provide examples of cases of interventions and confiscation related to abuse of NPOs for TF. The voluntary nature of registration of NPOs in Norway means that available sanctions appear to be limited and the available evidence shows that measures to sanction cases of non-compliance have been very limited. Norway has taken steps to remove incentives and to publish a list of untrustworthy fundraisers (even those not registered with it) on the website of the Collection Control Office www.innsamlingskontrollen.no.

Conclusion on IO.10

4.46. Norwegian authorities have taken some action to prevent terrorists from raising, moving and using funds, however, the effectiveness of targeted financial sanctions is undermined by limitations in the criminal justice mechanism used to implement UNSCR 1373 as required by Recommendation 6. Norway has a generally sound legal framework for targeted financial sanctions pursuant to the UN Taliban/Al Qaida sanctions. Banks have a good awareness of the freezing obligations and implement measures. However, implementation is undermined by the limited implementation of beneficial ownership requirements, and implementation outside the banking sector is varied and limited. Norway's mechanism to implement targeted financial sanctions pursuant to UNSCR 1373 as required by Recommendation 6 has serious deficiencies as it can only be used as part of an ongoing criminal investigation and does not prohibit the provision of funds to persons subject to a freezing action under this mechanism. These deficiencies are important factors, since they undermine the ability of Norway to use targeted financial sanctions as an effective tool to combat TF. Despite this, Norway has taken alternative action to secure terrorist funds using confiscation and charging provisions in several cases. Finally, Norway has taken a targeted approach and effectively prevents misuse of Norwegian NPOs that are responsible for the bulk of overseas NPO activity.

4.47. Norway has a **moderate level of effectiveness** for IO.10.

4.5 Effectiveness: Immediate Outcome 11 (PF financial sanctions)

4.48. Norway has taken measures to prevent persons and entities involved in the proliferation of weapons of mass destruction from raising, moving and using funds. The *Iran Regulations* and *DPRK Regulations* implement the list-based freezing obligations and activity-based financial prohibitions related to the financial aspects of the supply, sale, transfer, manufacture, maintenance, or use of the items, materials, equipment, goods and technology prohibited by the relevant resolutions UNSCRs due to their association with proliferation of WMD. The most significant deficiency in the Norwegian framework is the delay in transposing new designations made by the UN into Norwegian law. As noted above, there are delays of 1-4 weeks for the *Iran Regulations*, and up to 8 weeks for the *DPRK Regulations* to update the annexes to the regulations. Norway is required to adopt an amended regulation to implement new designations and as a result, the freezing obligations and prohibitions do not commence until well after a UN designation is made. After being adopted by the MFA, the amended document is sent to Lovdata (the entity in charge of publishing laws and regulations) for inclusion in the regulation. This long delay has an adverse effect on the effectiveness of the regime as efforts to freeze the assets of designated persons are undermined by the person having advanced notice of their designation in Norway. However, this adverse effect is mitigated to some extent by the FSA including information on new designations on their website immediately after being informed by the UNSC rather than waiting for the designations to be transposed into Norwegian law. In addition, Norwegian banks rely on third party systems

that monitor several lists of designated persons, including UNSC-lists. Banks have not informed Norwegian authorities of any instances where they have identified the assets of designated persons upon designation by the UNSC and before the designations were transposed into Norwegian law.

4.49. These delays are due to governmental processes involved in revising regulations. However, at the EU level, Norway has established a dialogue with relevant committees in the EU to seek quicker implementation of designations at the EU level. In practice, financial institutions have frozen funds at the time of designation by the UN and prior to transposition into Norwegian law. This is considered further below.

4.50. The *Iran Regulations* and *DPRK Regulations* cover the funds controlled by a designated person, which covers instances of funds owned by third party where the designated person exercises control. This has been effectively demonstrated in one example in Norway. In this instance, funds were frozen under the *Iran Regulations* by a Norwegian maritime insurance company which were not owned by a designated entity, but they were frozen because the foreign shipping company involved acted on behalf of a designated entity.

Implementation by reporting entities

4.51. FIs have frozen assets related to proliferation pursuant to the *Iran Regulations*. Norway reports that there have been 17 instances of funds frozen in bank accounts, with a total amount of almost EUR 5.5 million relating to 13 designated entities. These funds were frozen by two banks which held accounts which held bank accounts and guarantees owned or controlled by designated persons. The frozen funds are related to entities designated by both the UN and EU as the *Iran Regulations* implement both sanctions regimes. The values over the past 5 years are set out below:

Table 4.1. Funds Frozen under the *Iran Regulations*

	2009	2010	2011	2012	2013
Value of funds frozen (approx. EUR)	0	70 000	13 000	5 097 000	254 000
Number of freezing actions	0	2	1	12	1

Source: data provided by Norway

4.52. The number and value of Iran sanctions related freezing actions taken has increased significantly since 2007. The majority of instances of freezing and the amount of funds frozen were in 2012 (12 accounts with a total of over EUR 5 million). The significant increase in 2012 is likely a result of new designations made by the EU. No funds have been frozen pursuant to the *DPRK Regulations*. The difference between funds frozen under the Iran Regulations and the DPRK Regulations is in line with the fact that the size of Iranian-Norwegian bilateral trade is significantly larger than Norwegian-North Korean bilateral trade._

4.53. In most instances, the financial institution informed the MFA immediately of the freezing of funds under the *Iran Regulations*, in line with the regulations and guidance for financial institutions. In one instance the financial institution notified ØKOKRIM. However, this is considered to be an isolated incident.

4.54. The MFA may authorise access to funds for certain circumstances such as basic needs or professional fees. The mechanism for accessing funds has proved to be effective in practice. The MFA has approved two applications for access to frozen funds for legal fees, while one application is still pending decision by the MFA. Of these applications under the *Iran Regulations*, both were related to entities designated by the EU. All funds frozen in Norway are owned by larger entities and therefore the fact that there have been no applications for access to funds for basic needs is expected. The MFA is also the responsible authority to proposing designations to the UN Committees. However, no such proposals have been made so the effectiveness of this mechanism is difficult to determine. There have not been any reports by FIs or DNFBPs of a refusal to provide funds or other assets to designated persons in line with the prohibition requirements in the regulations.

4.55. The banking sector generally demonstrated a good awareness and understanding of their obligations under the *Iran and DPRK Regulations*. This was particularly the case for large, multinational banks. This is

due to both steps taken by the Norwegian authorities to inform reporting entities of their obligations and international pressure. Banks and some other reporting entities take a systems-led approach to real-time screening of accounts and transactions for matches with designated persons and entities. This includes screening both their customers and beneficial owners, when known, against the lists. These entities rely solely on external service providers for sanctions screening. However, it is not clear if the reporting entities or the FSA take any steps to assure themselves that those private providers are applying the most up-to-date designations and that the contents of their databases are accurate.

4.56. Despite the delays in transposing designations, in practice, large FIs in the banking sector may monitor the UN lists directly, if this is included by their service provider, rather than waiting for the lists to be transposed into Norwegian law. All reporting entities are encouraged to do so by the FSA in the guidance. The FSA receives information on new designations immediately from the Permanent Mission of Norway to the UN and places this information on their website by the next day. There have been examples of FIs in Norway identifying funds of persons designated by the UN before the designations are transposed into Norwegian law. In such instances, FIs have frozen the funds at the time of designation by the UN and prior to transposition into Norwegian law. This is, to some extent, due to other sanctions regimes and international pressure, in addition to the guidance provided by the FSA, The impact of the transposition delays on effectiveness is further mitigated by the fact that in some instances, designated entities added by the relevant UN Sanctions Committees were already designated by the EU sanctions which Norway has implemented.

4.57. The poor implementation of requirements related to the identification and verification of ultimate beneficial ownership has a negative impact on the implementation of the asset freezing obligations for proliferation. As set out under IO.4, there are low levels of effectiveness relating to the depth of CDD such that ultimate beneficial ownership information is available to support effective sanctions screening of accounts and transactions.

4.58. Implementation is varied and limited outside the banking sector. In the insurance sector, FIs were aware of the obligations and took some limited measures. These institutions used private service providers to monitor foreign customers but not Norwegian customers due to the cost of the service. DNFBPs did not take any measures to implement targeted financial sanctions relating to proliferation.

4.59. While only two banks have frozen funds in Norway, this may be explained by the fact that these large institutions hold a dominant market share in the banking sector and have a significant exposure to the oil and gas and related sectors in Norway. In addition, one Norwegian insurance company and one other Norwegian company have frozen funds or other assets pursuant to the *Iran Regulations*. The limited implementation in other parts of the financial sector and DNFBPs may be a contributing factor to the number of entities that have frozen funds.

4.60. There is a lower level of understanding and awareness for the *DPRK Regulations* than for the *Iran Regulations*. This may be due to the differing risk exposure of Norway to the economies of Iran and DPRK. The *DPRK Regulations* were only recently revised on 28 March 2014 after having initially been made in 2006. This represented a change in approach by Norwegian authorities as it adopted the EU framework. This means that the targeted financial sanctions in Norway also apply to persons designated by the EU under this mechanism. However, FIs were not aware of the change in approach and the guidance produced by the FSA and MFA has not been updated to reflect the revised regulations. All funds frozen by institutions have related to designated entities pursuant to the *Iran Regulations*.

Supervision of reporting entities

4.61. The lack of supervision of reporting entities for these obligations is a significant concern. The FSA is responsible for monitoring compliance by reporting entities; however, it has undertaken limited supervision. The only instance where the FSA considered this specifically was as part of a questionnaire to the banking sector in 2013, which included some specific questions on how the banking sector implements targeted financial sanctions. However, prior to this questionnaire, the FSA had not conducted any supervision regarding the targeted financial sanctions for proliferation financing. It is a concern that compliance with the

Iran and DPRK Regulations has not been reviewed or discussed as part of their on-site visits. The proliferation financing sanctions have not formed a part of any AML/CFT supervisory work outside the banking sector.

4.62. The FSA is aware that FIs rely solely on private service providers to carry out their obligations. However, it has not considered whether these measures are sufficient to meet the requirements. It has not taken any steps to test the robustness of the measures or engage in discussions with these FIs to obtain a detailed understanding of the operation of these measures. There is no supervision of DNFBPs relating to the implementation of the sanctions regimes.

4.63. The PST and FSA do not adequately coordinate in carrying the supervisory activity for the *Iran Regulations* and *DPRK Regulations*. As noted above in Chapter 2, the PST generally has sound mechanisms to coordinate activities domestically on financing of proliferation issues. However, the FSA does not participate in these forums. The lack of coordination increases the difficulty for the FSA to monitor reporting entities. This includes the ability to apply supervisory resources to areas of most importance and to ensure that supervisors understand the obligations and are able to identify deficiencies in a FI's measures.

Other measures

4.64. The *Iran and DPRK Regulations* include a range of measures that extend beyond the technical requirements of Recommendation 7, but which support efforts to counter the financing of proliferation.

4.65. The *Iran Regulations* also prohibit all transfers of funds exceeding certain thresholds to or from a FI located in Iran or an Iranian person, without prior approval from the MFA: Art.30, 30a, 31. The thresholds for transfers involving FIs that require approval are: NOK 800 000 (EUR 104 000) when regarding foodstuffs, healthcare, medical equipment, or for agricultural or humanitarian purposes; NOK 320 000 (EUR 41 600) when regarding personal remittances and NOK 80 000 (EUR 10 400) for any other transfer. For transfers involving Iranian persons, there are no thresholds for transfers regarding foodstuffs, healthcare, medical equipment, or for agricultural or humanitarian purposes, while the threshold of NOK 320 000 (EUR 41 600) applies to all other transfers. Before a transaction is approved, the MFA consults with the PST with the aim to obtain information on the beneficial owner of the account the funds. Since 2011, the MFA has received 81 applications for transfer of funds to Iran (17 in 2011, 23 in 2012 and 41 in 2013). Four applications have been denied, two in 2012 relating to one UN designated entity and one EU designated entity, and two in 2013 relating to UN designated entities. All denials were due to the fact that sanctioned Iranian banks were involved in the transaction. This additional mechanism enhances the effectiveness of the regime to prevent persons involved in proliferation financing by reducing risk and ensuring that FIs review transactions with Iranian FIs and persons.

4.66. Norway's export control regime is overseen by the export section of the MFA which considers applications for the export of dual-use materials. Requests are only approved to end-users where there is no risk of such exports being diverted to military use or use in the manufacture of weapons of mass destruction. Norway also participates in multilateral export control arrangements. As noted above at IO.1, Norway has established coordination mechanisms to combat exports of goods and technologies relevant for the development of weapons of mass destruction and the financing of proliferation, though it is a concern that the FIU and FSA do not participate. In particular, the lack of coordination with the PST would negatively impact on the effectiveness of any future monitoring of the *Iran and DPRK Regulations* as it would make it difficult to take a risk-based approach to monitoring.

Conclusion on IO.11

4.67. Norway has taken significant measures to prevent persons and entities designated by the UN from raising, using and moving funds, however, the delays in transposition and the lack of supervision have an adverse impact on the effectiveness of the measures. There is strong coordination and cooperation between competent authorities on PF, although this does not include engagement with the FSA. Financial institutions have frozen the funds of designated entities, and of entities acting on behalf of designated entities, under the Iran sanctions, which demonstrate the effectiveness of the measures. While some of these cases relate to EU designations, this demonstrates the functioning of the system as Norway implements the EU and

UN measures using the same regulations. Banks understand their obligations relating to targeted financial sanctions for PF and have frozen bank accounts of designated persons, although implementation outside of the banking sector is varied and limited. Furthermore, the lack of supervision for all reporting entities is a concern as the measures being taken by financial institutions have never been tested and their adequacy has not been considered.

4.68. The delays in transposing designations into Norwegian law negatively impact the effective use of targeted financial sanctions to combat PF. The delays are mitigated to some extent by financial institutions which monitor UN lists (as encouraged to do so by the FSA's guidance) and have frozen funds prior to transposition into Norwegian law. Norway also implements EU sanctions, which means that it has already implemented targeted financial sanctions for new UN designations which are previously on EU lists. However, this is not considered sufficient to overcome the deficiencies in the legal framework.

4.69. Norway has a **moderate level of effectiveness** for IO.11.

4.6 Recommendations on Terrorist Financing and Financing of Proliferation

Terrorist financing

a. Norway should clearly criminalise as a stand-alone offence the provision of funds for terrorist acts and the collection of funds in the knowledge that they are to be used for any purpose by a terrorist organisation or an individual terrorist (s.147b, *PC*).

b. Norway should support effective implementation of targeted financial sanctions for TF by:

- implementing all aspects of targeted financial sanctions pursuant to UNSCR 1373 as required by Recommendation 6
- establishing effective supervision of FIs and DNFBPs for targeted financial sanctions

c. Norway should enhance targeted outreach to the NPO sector on issues of risk, transparency and the standards set out in R8 and continue to support the government/NPO sector consultation in the formulation of regulatory controls for the collection of funds to address the risks posed by unregulated collection.

d. Norway should enhance the coverage and implementation of regulatory frameworks and oversight for those NPOs which may be at risk. This should be done taking into account risks, while balancing the need to ensure that such measures do not disrupt legitimate NPO activities.

Proliferation financing

e. Norway should ensure that designations are transposed quickly into Norwegian law under the Iran and DPRK Regulations to ensure that targeted financial sanctions for PF are implemented without delay. .

f. The FSA should undertake effective monitoring for compliance with the Iran and DPRK Regulations, taking into account the reliance of financial institutions on private service providers.

- The FSA and PST, with FIU engagement, should establish a mechanism to communicate and coordinate on PF issues to assist in establishing risk-based targeted supervision.

Bibliography

NOU (2012), *Report of the 22 July Commission: 2012-2014*, www.regjeringen.no

5. PREVENTIVE MEASURES

Key Findings

- Significant enhancements were made to the preventive measures regime in 2009 to better align with the 2003 FATF Recommendations. However, Norway has not updated the regime since then, despite the shortcomings that exist in several key areas.
- Some sectors, such as banking, understand the criminal threats to which they are exposed, but the requirement for a money laundering / terrorist financing (ML/TF) risk assessment is not clearly understood and is not widespread. Financial institutions and designated non-financial businesses and professions (DNFBPs) do not have a well-developed understanding of risk or the scope and depth of measures required to mitigate varying ML/TF risks.
- Although anti-money laundering and counter-terrorist financing (AML/CFT) obligations are generally well understood in certain sectors; such as banking, audit and accounting, and real estate; significant compliance gaps have been identified by the authorities across a number of sectors and implementation of some key preventive measures has not been effective in mitigating ML/TF risks.
- Weaknesses exist over the necessary customer due diligence (CDD) measures required to understand beneficial owners, particularly where foreign ownership is involved, which undermines effectiveness.
- Concerns exist over the application of preventive measures in some key areas such as politically exposed persons (PEPs), wire transfers and correspondent banking.
- Ongoing monitoring and periodic review requirements have not been effectively implemented.
- Concerns exist over the quantity and quality of suspicious transaction reports (STRs).

5.1 Background and Context

(a) Financial Sector and DNFBPs

5.1. Norway has a relatively small financial sector, which is generally domestically orientated, employing around 40 000-50 000 people. Exposure to ML/TF risk factors could arise from the open nature of the Norwegian economy, in which oil, gas and shipping play a major role. Most sectors are relatively small and concentrated by the standards of other European countries:

a. **The banking sector** in Norway is small relative to total GDP in comparison to some other European countries. Banks in Norway are often part of wider financial groups that also include mortgage companies, finance companies, securities funds, insurance companies and real estate brokers. Although there are a large number of banks in Norway, there is also a relatively high level of concentration. The five largest financial groups control over 70% of the market while two banks, DNB Bank and Nordea, dominate the domestic banking sector. DNB Bank is 34% government owned and plays a particularly important role in Norway's AML/CFT regime since it is the settlement bank for many smaller savings banks (which in Norway cooperate extensively, have formed alliances with varying degrees of integration and are characterised by small scale, local operations). As in most countries the banking sector is important from an ML/TF risk perspective.

b. **The MVTS sector** consists of a significant number of money or value transfer service (MVTS) providers and agents and has been identified as high risk in the National Risk Assessment (NRA). There are 21 payment institutions (including hawala) authorised in Norway and a large number of branches or agents of payment institutions authorised in other European Economic Areas (EEA) countries according to the *EU Payment Services Directive (PSD).* Money exchange services are only provided by banks and finance companies, with one bank FOREX, being more prominent in providing this service. In recent years it has taken a number of steps to tighten its AML/CFT controls.

c. **The insurance sector** is small in terms of the number of insurance companies and premium collection values compared with other developed countries. Notably Norway's AML/CFT obligations apply to both life and non-life insurance. There is very limited use of products or services that are considered to be more risky, such as single premium insurance or viatical arrangements, and thus the sector generally appears to be lower risk.

d. **The securities sector** is also relatively small. Trading in securities takes place via securities departments in banks and through 30 management companies for securities funds and 130 investment firms. The Financial Supervisory Authority (FSA) is of the view that the vulnerability of the securities market for ML activities is moderate. This is in contrast with some trend reports which indicate that the ML risk in the securities sector has significantly increased recently.

e. **Other types of financial institutions** – In addition to the banking sector, some banking activities such as lending, including financial leasing; issuing and managing means of payments; as well as money exchange services are offered by 52 finance companies.

f. **Auditors and accountants** are subject to full AML/CFT obligations. There are 6 704 auditors in 600 audit firms and 11 218 accountants in 2 862 accounting firms. While the five biggest audit firms account for over 60% of the work, the pattern for external accountants is somewhat different; there are a few large entities and a substantial number of small and medium sized entities, 95% of which have less than 10 full time employees.

g. **The real estate sector** is important to the Norwegian economy and features in the NRA as an area

of higher risk. Home prices have seen significant rises over the past decade[1] and international buyers are common in the commercial sector. The sector includes firms licensed to practice estate agency and lawyers whose estate agency is ancillary to their law business. Estate agents who form part of large bank groups account for approximately 70% of the sector.

h. **Lawyers and independent legal professionals** – There are around 7 000 lawyers in Norway and 90% of them are a member of the Norwegian Bar Association. 2 000 of these lawyers work as in-house lawyers for private companies/organisations and government institutions while the remaining 5 000 private practicing lawyers are split between large law firms (around 5 300) and sole practitioners (around 1 500). Almost half of the private practicing lawyers work in Oslo. The legal profession is considered to be higher risk by the authorities. Notaries do not operate in Norway and the services often associated with notaries are generally carried out by lawyers in Norway.

i. **TSCPs** became subject to AML/CFT requirements when the *MLA* was amended in 2009. However there is no clearly defined sector, and Norway was not able to provide any indication of the number of professionals offering these services. This is due to the fact that this category of DNFBPs is neither licenced nor supervised for AML/CFT purposes as TCSPs. However, it is believed that the majority of work done in this area is by practising lawyers rather than independent businesses.

j. **There are between 500 and 550 dealers in precious metals and stones** in Norway. These are all subject to preventive measures in the AML/CFT legislation and regulations when they perform transactions in cash exceeding NOK 40 000 (EUR 5 200), as the *MLA* applies to all dealers of movable property above this threshold. Even though AML/CFT preventive measures have applied to this category of DNFBPs since 2004, they are still not regulated nor supervised by any agency for AML/CFT purposes.

k. **Casinos** – are not classified as a reporting DNFBP in Norway. Offering gaming activities in Norway is a criminal offence unless they are permitted by a specific law. There are no laws permitting land-based casinos in Norway and therefore they are prohibited. However, under certain conditions and licencing requirements, entities can provide services for ship-based and, since January 2014, Internet-based casinos. One entity has been granted a licence to provide casino-style gaming on the Internet, and one entity has been granted a licence to operate a casino on Norwegian ship transfers between Norway and foreign ports. Although subject to a number of controls which help mitigate the risks, these entities are not subject to Norway's AML/CFT laws. In addition, competent authorities have not taken any measures to prevent foreign registered cruise ships providing gaming activities in Norwegian waters or to control the activities of foreign internet casino gaming providers.

1 Measures introduced by regulators to cool demand have had an effect and some deflation of prices has taken place in recent months.

Table 5.1. Number of reporting entities

Industry sector	Number
Banks	126
EEA branches of credit institutions in Norway	42
MVTS (authorised in Norway)	22 (with 5 agents)
MVTS (authorised in other EEA countries offering services in Norway through agents/branches located in Norway)[1]	16 (with 402 agents & 6 branches)
MVTS (authorised in other EEA countries offering services in Norway but with no agents/branches in Norway)[2]	211
Insurance entities (companies and intermediaries)	182
Securities entities	160
Other types of financial institutions (finance companies, e-money institutions)	54
Auditors	600
Accountants	2862
Real estate agencies	517
Lawyers and legal professionals	7000
TCSPs	Unknown
Dealers of precious metals and stones	500-550
Casinos	2

Table Notes:

1 The three largest MVTS providers (having international operations) with passported agents operating in Norway are based in the United Kingdom and Ireland.

2 The majority of, and largest, MVTS providers offering cross-border services in Norway are based in the United Kingdom.

Source: data provided by Norway

(b) Preventive Measures

5.2. Norway's current AML/CFT preventive measures are based on the 2003 FATF Standards and the third EU Money Laundering directive. The principal legislation is the *Act Relating to Measures to Combat Money Laundering and the Financing of Terrorism 2009* (*MLA*) and the *Regulations concerning Measures to Combat Money Laundering and the Financing of Terrorism 2009* (MLR). The FSA has also issued guidelines on AML/CFT issues, the most important being those issued in 2009. The *MLA* imposes requirements that are consistent with the 2003 FATF recommendations, but which have not been updated to take into account the changes introduced through the 2012 FATF Recommendations, most notably the risk-based approach in R.1.

(c) Risk-Based Exemptions or extensions of preventive measures

5.3. Norway has exempted certain types of customers and transactions from preventive measures. However, this has not been done on the basis of proven lower risk but rather on the basis of policy or perceived risk. There has been little extension of AML/CFT measures on the basis of risk.

5.2 Technical Compliance (R.9-23)

Recommendation 9 – Financial institution secrecy laws

5.4. Norway is rated largely compliant (LC) with Recommendation (R.) 9. There is a duty on financial institutions and their employees to maintain the confidentiality of any information concerning the customer which comes to their knowledge, but disclosure is permitted if this specifically required by law e.g., reporting STRs is specifically permitted: s.11 *MLA.* It also allows financial institutions and insurance companies to exchange customer data if this is necessary to investigate suspicious transactions. Competent authorities are able to access and share (both domestically and internationally) information held by reporting entities, but there are limitations on the ability of reporting entities to share information internationally within a group.

Recommendation 10 – Customer due diligence

5.5. Norway is rated partially compliant (PC) with R.10. The requirements in the *MLA/MLR*, which were enacted in 2009, are based on the 2003 FATF Recommendations Actions have not yet been taken to bring the requirements into line with the new Standards, in particular concerning risk-based approach (RBA). Moreover the FSA guidance has not been updated to take into account the more recent international developments.

5.6. The most important CDD requirements such as when CDD must be carried out, and the obligations for customer and beneficial owner identification and verification and ongoing due diligence, are generally in line with the FATF Standards: see *MLA chapter 2*. When taken together with the extensive system of national registers of Norwegian citizens and residents, along with the different types of legal persons created in Norway, these measures create the foundation for a solid set of CDD measures.

5.7. However there are a range of areas where AML/CFT requirements are lacking. As noted above, RBA is not properly incorporated into the framework, with low risk exemptions being based on assumptions and the measures set out in the EU's 3rd Anti-Money Laundering Directive (3AMLD). Furthermore, there is insufficient elaboration regarding risk and the measures to take commensurate to those risks. There are no measures for life insurance beneficiaries, and there are a number of other less serious deficiencies, such as those relating to: beneficial owner identification for occasional wire transfers between EUR 1 000 and 15 000, ensuring that FIs have a broad understanding of the ownership and control structure of legal persons/arrangements, the timing of CDD etc. This series of weaknesses undermines the otherwise solid implementation of fundamental measures.

Recommendation 11 – Record-keeping

5.8. Norway is rated LC with R.11. The requirements in *the MLA* to keep CDD data are generally sound - such records must be retained for five years after termination of the customer relationship or after an occasional transaction is carried out. Reporting FIs must also have systems that enable them to provide rapid and complete responses to enquiries from the National Authority for Investigation and Prosecution of Economic and Environmental Crime (ØKOKRIM) or supervisory authorities concerning customers, and data should be stored in an easily accessible location. Obligations concerning the keeping of transaction records are set out in the *Bookkeeping Act 2004 and Regulations* (which apply to all types of businesses). Sections 4-6 of the Act, read with the Regulations, appears to impose requirements to keep complete transactions records, Although generally worded, the preparatory works and other documents showed that transactional records need to be kept in sufficient detail so that individual transactions can be reconstructed. Such records are available in practice to competent authorities.

Additional Measures for specific customers and activities

Recommendation 12 – Politically exposed persons

5.9. Norway is rated PC with R.12. The *MLA* establishes measures concerning the establishment of customer relationships with foreign PEPs: s15. A PEP is defined as a natural person who holds or held a high

public office or post in a state other than Norway during the last year. The *Money Laundering Regulations* (*MLR)* further describes what is meant by 'holder of high public office or post' and lists a range of high-ranking positions: s.11. Family members and close associates are covered in the PEPs requirements. However, they are included in the definition of PEPs which creates a confusing and circular definition. Reporting entities are required to conduct 'appropriate CDD measures' to establish whether customers are PEPs and then take additional measures for PEPs including senior management approval, determining source of funds and enhanced on-going monitoring: s15 *MLA*.

5.10. The definition of a PEP includes a holder of an office or post in an international organisation which corresponds to the high-ranking positions outlined in the *MLR* and the same requirements apply. However, this approach has limitations as the government positions in the list do not correspond well to the concept of senior management positions in an international organisation. There are no requirements relating to domestic PEPs.

5.11. The requirements only apply to foreign PEPs who have held a high public office or post during the previous year, which is too prescriptive, not in line with an RBA and insufficient to meet the FATF definition of a PEP. Moreover, the PEPs requirements do not cover beneficial owners of natural persons, as is expressly stated in the FSA Guidance. The definition of close associate in relation to the PEPs requirements includes beneficial owners of legal persons and legal arrangements: s11 *MLR*. However, there are no measures in place in relation to life insurance policies and PEPs.

Recommendation 13 – Correspondent banking

5.12. Norway is rated PC with R.13. Although the requirements regarding correspondent banking and shell banks introduced in the 2009 *MLA* mirror those of R.13, they only apply to credit institutions and not to any other type of FIs, although it is not clear what types of correspondent relationships are envisaged. Importantly, the requirements only apply when entering into an agreement with correspondent banks outside the EEA, which creates an important technical deficiency given that the vast majority of relationships are within the EEA.

Recommendation 14 – Money or value transfer services

5.13. Norway is rated LC with R.14. Norway has comprehensive authorisation requirements for Norwegian MVTS providers. MVTS providers are required to have authorisation from the FSA, which conducts fit and proper person tests. The FSA may also grant a limited authorisation which waives some of the general rules for payment institutions and creates limits on total transaction amounts per month. The limited authorisation also includes an assessment of the provider's AML/CFT policies and procedures. In accordance with the *EU Payment Services Directive* (*PSD*), Norway also allows payment institutions with their head office in another EEA country to establish and carry on business through a branch or agent, or carry on cross-border activities in Norway without authorisation from the FSA. This is on condition that the entity is authorised to carry on business in its home country and is registered with the FSA. Carrying out unauthorised MVTS is a breach of the FIA, punishable by a fine or imprisonment of up to 1 year. The police are the competent authority for the identification and sanction of unauthorised MVTS providers. Norway produced two examples of these cases as well as indicating that other cases are ongoing, although this action has only been taken on an ad hoc basis.

5.14. The FSA is responsible for monitoring the compliance of MVTS providers with AML/CFT obligations. Authorised MVTS providers are subject to comprehensive off-site supervision through an assessment of AML/CFT procedures and requirements to report to the FSA on a semi-annual basis on their monitoring and reporting obligations. Providers with limited authorisation are also required to renew their authorisation every two years, which include a review of their AML/CFT procedures. However, the FSA has not undertaken any on-site inspections of authorised providers. The branches and agents in Norway of MVTS providers authorised by other EEA countries that operate in Norway are not subject to monitoring for AML/CFT compliance. This is a significant concern given the large portion of market share held by the multinational providers. These branches and agents are subject to the *MLA*, yet the FSA (with reference to the PSD) considers that this is the responsibility of the home country supervisor.

Recommendation 15 – New technologies

5.15. Norway is rated PC with R.15. Norway has only taken limited steps to identify and assess the risks that may arise in relation to the development of new products and new business practices, including new delivery mechanisms, and the use of new or developing technologies for both new and pre-existing products. Recently, Norway undertook its first NRA which included consideration of some of the risks posed by new technologies, such virtual currencies and new payment systems. However, the deficiencies with the NRA as noted above also apply here. There is no specific requirement for all REs to identify and assess the risks posed by new technologies. There are also general requirements for institutions to conduct risk assessments and mitigate risks before the launch of new products, practices and new technologies. Norway considers that this applies to ML/TF risk. However, neither the regulations nor the associated guidance refer to ML/TF risks, and it remains unclear whether there are requirements for REs to undertake ML/TF risk assessments prior to the launch or use of new products, practices and technologies, nor to take appropriate measures to manage and mitigate the risks.

Recommendation 16 – Wire transfers

5.16. Norway is rated PC with R.16. Norway implements the requirements relating to wire transfer through s.20 of the *MLR* which transposes into Norwegian law the *EU Regulation on wire transfers (1781/2006/EC)* (the EU Regulation). The EU Regulation places obligations on ordering FIs to ensure that transfers of funds are accompanied by complete information on the payer. For transfers of EUR 1 000 or more, the ordering FI is also required to verify the complete payer information. In line with R.16, the EU Regulation does not require verification for transfers under EUR 1 000. However, under the *MLA*, verification is required if there is a suspicion of ML/TF. Intermediary FIs are required to maintain all information with the wire transfer and beneficiary FIs are required to detect and take action when there is missing information. A significant deficiency is that there are no requirements to include and maintain the required beneficiary information in cross-border and domestic transfers. In addition, intermediary FIs are not required to identify cross-border wire transfers that lack information, or to have risk-based policies and procedures on when to execute, reject or suspend a wire transfer with missing information.

5.17. For the purposes of R.16, wire transfers entirely within the EEA are considered to be domestic wire transfers, and the EU Regulation makes this distinction in line with R.16. However, the definition of transfers within the EEA in the EU Regulation is wider than that permitted as a domestic wire transfer. A domestic wire transfer is defined to include a chain of wire transfers that takes place entirely within the EEA. However, the EU Regulation only refers to the situation where the payment service provider of the payer and payee are situated in the EEA. This means that where an intermediary institution is situated outside the EEA, this may be considered a transfer within the EEA under the Regulation, but not a domestic transfer under R.16.

Reliance, Controls and Financial Groups

Recommendation 17 – Reliance on third parties

5.18. Norway is rated PC with R.17. The 2009 *MLA* introduced provisions that allow reporting entities to rely on third parties to perform certain CDD measures: s11 *MLA*. Such reliance does not absolve reporting FIs from their obligations to ensure that CDD measures are applied in accordance with the *MLA*. Third parties in other countries must be subject to CDD and record keeping requirements that are equivalent to those in the *MLA*, and subject to supervision: *MLA* s11(1)(11).The *MLA* places the obligation to make CDD information available to reporting entity on the third party upon request which, in the case of a third party located outside Norway would be difficult to enforce. Moreover, there are no requirements on FIs to ensure that domestic third parties have measures in place to comply with CDD and record-keeping requirements. Norway does not have regard to information available on the level of country risk when determining in which countries a third party can be based.

Recommendation 18 – Internal controls, and foreign branches and subsidiaries

5.19. Norway is rated PC with R.18. Reporting entities are required to have satisfactory internal control and communication procedures in place to ensure compliance with their AML/CFT obligations, including compliance management arrangements and on-going employee training. However, these measures are silent with regard to screening of employees and the implementation of group-wide AML/CFT programmes. The *MLA* does not contain a requirement for all FIs to have an independent audit function to test compliance; however, the FIA places such an obligation on a range of FIs[2]. The obligation to ensure that FIs' foreign branches and subsidiaries are familiar with the internal control requirements are limited to branches and subsidiaries established in states outside the EEA while a large majority of branches and subsidiaries of Norwegian FIs are located within the EEA.

Recommendation 19 – Higher risk countries

5.20. Norway is rated LC with R.19. There is no requirement for reporting entities to apply enhanced CDD, proportionate to the risk, to business relationships or transactions from countries for which the FATF calls to do so, which is a new and important component of the revised standards. However, Norway has the power to apply counter-measures against higher risk jurisdictions both in situations called upon to do so by the FATF and independently of any call by the FATF. Norway also has measures in place to advise FIs about weaknesses in the AML/CFT systems of countries which are publicly identified by the FATF, and FSA guidance refers reporting entities to FATF and FSRB websites which contain assessments and other reports that contain information on other countries, and any weaknesses in their AML/CFT systems.

Reporting of Suspicious Transactions

Recommendations 20 & 21– Reporting of suspicious transactions, tipping-off and confidentiality

5.21. Norway is rated compliant (C) with R.20 and LC with R.21. Overall, Norway has an adequate legal framework requiring the reporting of suspicious transactions. The *MLA* provides that reporting FIs and their employees are protected from both criminal and civil liability when they communicate information in good faith to the FIU. The *MLA* contains a tipping-off prohibition designed to ensure the confidentiality of the information reported, however there is no sanction for breaching this provision other than the application of general supervisory sanctions that can be applied to reporting entities. In particular, there is no sanction applicable to individuals breaching this provision. For example, no sanctions would apply to a bank employee that tipped off that an STR had been made.

Designated non-financial businesses and professions

Recommendation 22 – DNFBPs: Customer due diligence

5.22. Norway is rated PC with R.22. The majority of DNFBPs are covered by Norway's AML/CFT regime and are subject to the requirements in the *MLA*. However, there is a minor scope issue in that certain internet and ship-based casino gaming activities are not covered by the AML/CFT legislation. Given that DNFBPs are subject to the same requirements, the deficiencies identified in relation to R.10-12, R.15 & R.17 equally apply here.

2 Public credit institutions, public trustee's offices and foundations, management companies, investment firms, certain finance companies, payment institutions and electronic money institutions.

Recommendation 23 – DNFBPs: Other measures

5.23. Norway is rated LC with R.23. Given that DNFBPs are subject to the AML/CFT requirements, the deficiencies identified in relation to R.18, 19 and 21 equally apply here, as does the minor scope issue.

5.3 Effectiveness: Immediate Outcome 4 (Preventive Measures)

5.24. **Banking sector:** The requirement for FIs to undertake a ML/TF risk assessment is not clearly articulated in the *MLA* and is not well understood or implemented. In 2010, testing by the FSA on 13 banks established that few had risk assessments in place or understood the requirement to identify, assess and understand their ML/TF risks. In its more recent supervision of banks the FSA has focused on ML/TF risk assessments and commented on failures in follow up supervisory letters, but the requirement has not been examined outside of the banking sector. Based on analysis of the off-site examinations conducted in 2013 (in which 35 out of 140 banks had no or very limited customers placed under enhanced CDD and demonstrated a lack of awareness of ML/TF risks and the measures that are required to mitigate them) the NRA notes the banking sector's view was that the RBA requirements still remain difficult to understand and concludes that many small and medium sized banks have not carried out risk assessments of their operations nor developed risk based routines and procedures. Similar concerns exist within other sectors, in particular the MVTS sector.

5.25. During interviews with a range of different sized banks it was apparent that the sector possessed a considerable understanding of the main criminal threats or ML/TF risks to which it might be exposed. For example, a savings bank with branches near the border with Russia indicated that significant cash deposits by Russian nationals were a concern. Threats presented by the larger institutions were more consistent with complex operations and included trade finance and private equity funds. There is no information on how banks assess fiscal or tax evasion risk, or what risk mitigation measures, if any, have been taken. All banks spoken to had identified ML/TF risks associated with the form of business organisation known as 'Norwegian-registered foreign business enterprise' (NUF) which grants reduced public disclosure and more lenient requirements for share capital[3].

5.26. Norway acknowledges that the application of AML/CFT measures differ to a substantial degree among different banks[4]. The thematic reports conducted in 2010 identified that most banks had not established measures to ensure compliance with the *MLA*, in particular the requirement to apply enhanced CDD. Most large commercial banks understand the requirements as set out in the law, regulations and guidance, but for others the picture is more mixed, with some banks demonstrating a serious lack of understanding of the requirements and compliance with them. The FSA has also noted significant shortcomings in banks training programs and have issued advice over the frequency and scope of training.

5.27. Simplified due diligence is not undertaken on the basis of ML/TF risk. While the *MLA* contains aspects of RBA (i.e., discretion on the level of CDD above a baseline for normal risk) the *MLA* does not allow institutions the discretion to classify customers as lower risk and conduct simplified due diligence (SDD) on this basis. This is only permissible in certain standard low-risk situations.

5.28. **Money or value transfer services:** The MVTS sector has a low level of understanding of ML/TF risks and of implementation of AML/CFT measures. This is a significant concern given the high level of risk in this sector. In terms of MVTS companies authorised in Norway, the FSA has identified that compliance with AML/CFT obligations is not satisfactory. Information from the FIU also suggests unlicensed MVTS activity

3 The NRA notes that the number of STRs from auditors has fallen from 54 in 2012 to 39 in 2013. It is assumed that this may be linked to the introduction of the audit exemption for this group of limited liability companies.

4 These observations are based on the 13 AML/CFT thematic examinations in 2010, as well as 40 on-site examinations in 2013 which contained elements of AML/CFT and 140 desk-based reviews conducted in 2013.

carried out by agents not known to the authorities may be significant, while the obligation to report to the currency register (which is a very useful and well used source of information for competent authorities) is fulfilled only by a minority of MVTS providers. The FSA has also expressed serious concerns over lack of AML/CFT compliance by the agents of EEA payment institutions operating in Norway, amongst which STR reporting levels are very low.

5.29. *Securities sector:* The FSA carries out on-site inspections in the securities sector and while these cover aspects of firms' AML/CFT guidelines and routines, it is not the main focus and there have been very few remarks on AML/CFT in subsequent FSA examination reports[5]. Most firms are known to have basic routines in place, and from discussions with the industry bodies and the limited sample of firms met by the assessment team, there was a reasonable degree of awareness over the AML/CFT obligations and the requirement to have routines. There was much less awareness over the risk based approach, what might constitute higher risk in the securities sector and what measures might be required to deal with higher (and lower, where relevant) risk customers, products and countries. It is not clear whether screening against UN designations is well implemented in the sector.

5.30. *Insurance sector:* Understanding and awareness in the insurance sector was not well-developed. Given that there has been no supervision or monitoring, making an assessment is challenging, but it appears that at best there are only basic routines or obligations and no risk based preventive controls.

5.31. *Accountants and Auditors:* AML/CFT obligations are reasonably well understood by most auditors and accountants. Knowledge and awareness was high in the auditor sector, especially in large firms, who during the on-site visit demonstrated a strong grasp of the AML/CFT obligations and the challenges they present for the industry, such as the risk based approach, and some awareness of ML/TF risks. Knowledge amongst smaller firms of accountants was considered more variable. Most audit and accounting firms have implemented routines that satisfy AML/CFT obligations and these have been subject to testing. Accountants use standard routines developed by the Association of Authorized Accountants (NARF).

5.32. *Real Estate agents:* There is a reasonable awareness of AML/CFT obligations and some understanding of ML/TF risk by agents operating as part of larger financial groups in this highly regulated sector. Some basic testing has been undertaken by the FSA over compliance with AML/CFT obligations, such as the requirement to have routines. However, despite apparent ML risks STR reporting levels remain low and doubts exist over the effective implementation of preventive measures in this sector, although the Norwegian Association of Real Estate Agents[6] has been active in promoting awareness of AML/CFT issues amongst its members.

5.33. *Lawyers:* Although lawyers are regulated and supervised for AML/CFT by the Supervisory Council for Legal Practice, in practice they are audited annually by an external auditor for bookkeeping and auditing obligations. As with some other sectors, certainly amongst bigger firms there was awareness of the obligations and the requirement to have systems and routines. Beyond this accurate assessment is challenging other than to say that oversight of the implementation of AML/CFT obligations consists of a high level audit and is not effective. The assessment team was told that while the controls of large firms was better and risk tolerance lower, the opposite was true of smaller firms.

5.34. *Dealers in Precious Metals and Stones* exhibited a very low awareness of ML/TF risk or the AML/CFT obligations which applied, an observation supported by very low STR reporting levels.

5 The FSA considers that this is because ML/TF risk is low or moderate but have not provided supporting evidence of an assessment, and the issue it not addressed in the NRA

6 80% of all private real estate in Norway is done through an real estate agent who is a member of NEF.

Enhanced or Specific Measures

Beneficial Owners ('BO')

5.35. Financial institutions and DNFBPs have a good general understanding of the concept of BO but do not, as a general rule, implement measures that will allow them to understand and verify the ownership and control structure since there is no clear requirement for them to do so. The main focus is on identification ('registering and retaining BO information') on the basis of information provided by the customer and cross-checked with information provided by private service providers, which is mainly sourced from the various Norwegian registries (although very useful, these do not contain information on foreign ownership). There is not sufficient guidance on the regulatory expectation concerning the actions that might constitute *reasonable measures*[7] to verify the accuracy of BO information based on an assessment of the ML/TF risks. Therefore, while the law itself is consistent with the obligations regarding BOs, implementation is not effective, and understanding of BO obligations was not sufficiently widespread or at the depth of understanding required, for example, in relation to reasonable measures to verify identity where foreign ownership is involved. Although the financial system is generally domestically orientated, foreign (especially Nordic) ownership is important in the banking system, having increased significantly in recent years and is relatively high by regional standards. It was noted for example that compliance failures over the identification and verification of beneficial owners were highlighted in an FSA inspection of a Norwegian subsidiary of a Nordic banking group in 2012 (see box 6.1 below).

5.36. Interviews with financial institutions indicate that despite the complexities of identifying BOs, financial institutions and DNFBPs have not raised concerns with regulators regarding the extent of their obligations or challenges with identifying the UBO.

Politically Exposed Persons

5.37. Technical compliance shortcomings are highlighted in section 5.2 which significantly undermine effectiveness. The requirements that are in place are not applied effectively. During desk based reviews in 2013 many banks misinterpreted the definition of PEP to include domestic PEPs (which it does not). This resulted in significant over calculation of the PEP population identified by certain banks. The FSA subsequently instructed banks to remove high level domestic PEPs from this classification in supervisory letters but had not provided banks with any guidance on how the risk of domestic PEPs could be managed. Within most sectors, there was an over reliance on commercial PEP screening tools to meet this obligation.

Correspondent banking

5.38. The technical deficiencies regarding the scope of application of the high level requirements in s. 16 *MLA*, taken together with the lack of substantive guidance on correspondent banking impact effectiveness significantly. The FSA has not examined how banks apply these obligations in practice. During the on-site visit, banks were unsure whether the obligations of the *MLA* applied to correspondent relationships which pre-exist the *MLA.* Taken together with concerns over the ineffective implementation of periodic reviews, the enhanced specific measures applied by banks in this area are inadequately applied, despite the higher risks.

Wire transfers and New Technologies

5.39. Technical deficiencies aside, there is little evidence on which to base any objective assessment of banks' compliance with wire transfer rules since the area has not been tested by the FSA. There are no specific obligations over risks presented by new technologies and financial institutions practices in this area are untested. In relation to wire transfers, as noted above (R16), there are significant deficiencies in the EU

7 This potential shortcoming was highlighted to Norway after enactment of the *MLA*, in the fourth follow up report dated 11 June 2009, when it was observed 'this is an area that would greatly benefit from further guidance from the FSA, particularly with regard to what constitutes 'reasonable measures'. No such guidance has been provided to date.

legal framework which applies in Norway as it does not require the details of beneficiaries to be included in transfers. This limits the ability of Norwegian LEAs to follow the money in criminal investigations when funds are transferred domestically or internationally. While, it is understood that some payment systems have updated their messaging systems to allow sending financial institutions to enter beneficiary information, this is not mandatory.

Preventive Measures associated with targeted financial sanctions

5.40. Based on qualitative information received onsite, and desk based reviews conducted by the FSA, compliance with targeted financial sanctions obligations is mixed. While the greatest risk lies with large commercial banks, which generally understand the obligations and have systems and controls in place (which may be due to international focus on sanctions), desk based reviews conducted in 2013 found 36 banks had no systems or controls to initiate freezing obligations, while approximately 65 banks did not take any action to check or screen beneficial owners against designation lists. The FSA considered that a number of banks had given this area a rather low priority. Assessment of compliance in other sectors is more challenging, though from the interviews conducted by the assessment team, awareness is low with over reliance on the notion that most customers are Norwegian, and that there are few designations linked to Norway. In the MVTS sector, which represents the biggest risk after banks, outside of the large payment institutions from EEA countries and their agents, there is no evidence that screening is widespread or effective as there has been no on-site testing by the FSA.

Ongoing monitoring and Suspicious Transaction Reporting

5.41. Pursuant to *MLA* s.14, reporting FIs are required to conduct ongoing monitoring, while *MLR* s.18 introduces a requirement for all financial institutions to establish electronic surveillance systems, regardless of their size or risk profile. The robustness of systems for ongoing monitoring to detect unusual or suspicious transactions or patterns of activity has not been tested by the FSA and effectiveness is low. Effectiveness is impacted by the quality of CDD and the lack of awareness and formal assessment of ML.TF risk. During the on-site visit banks raised a number of concerns, such as how the objectives and key performance indicators should be defined to recognise when automated transaction monitoring systems were underperforming and in the absence of clear guidance on the FSA's regulatory expectations. The assessment team was not provided with any validation, by any party, that these systems are effective in mitigating ML/TF risks.

5.42. The obligation on reporting FIs to update documents and information on customers under MLA s.14 is also not effectively implemented. How and when this should occur is not clear. Given that beneficial ownership requirements were only introduced in 2009, whether customer information that is held for customers pre-existing 2009 is useful or appropriate to determine the level of monitoring could not be ascertained, either from reporting FIs or the FSA.

5.43. The level and quality of reporting to the FIU by reporting entities has long been a concern for Norway and is highlighted in the NRA, particularly for the banking and MVTS sectors. Overall reporting levels for MVTS dropped significantly in 2010-2012 (see table 5.2) and have been reasonably constant for the last 3 years.

5.44. While some large banks consider that the quality of reports has increased, this view was not necessarily shared by the FIU, which has been quite active in outreach to the banking sector over STRs. The FSA has assessed that the decrease between 2010 and 2011 was a result of a change in reporting practice on the part of one major bank which accounted for a large percentage of reports to the FIU. The FSA also observed that desk based reviews conducted in 2013 revealed a considerable and inexplicable decrease in the number of STRs from some major banks.

5.45. Outside of the banking sector, which accounts for around 75% of all reports, the MVTS sector is the second biggest provider of reports (807 in 2013 and 882 in 2012) although concern has been expressed over the relative lack of STRs from payment institutions from EEA countries and their agents, given the considerable volume of funds remitted through this sector. The FIU considers that a cause of the decrease in reporting from the MVTS sector from 2009-2013 was an increase in the understanding of the ML/TF risks and less defensive reporting triggered by back office alerts. In particular, FOREX Bank (an MVTS)

changed its policies so as to report multiple transactions in a single STR and enhanced its CDD and analysis process, thus reducing significantly the number of reports it made, which were a major part of the total. This has coincided with an increase in quality in STRs from the MVTS sector. In terms of volume next are auditors and accountants (95 in 2013) and then insurance companies (67 in 2013). Reports by securities firms and lawyers indicate very low levels of awareness. There are no clear reasons for the decrease in STRs from other sectors over this period including accountants, auditors and dealers in expensive objects.

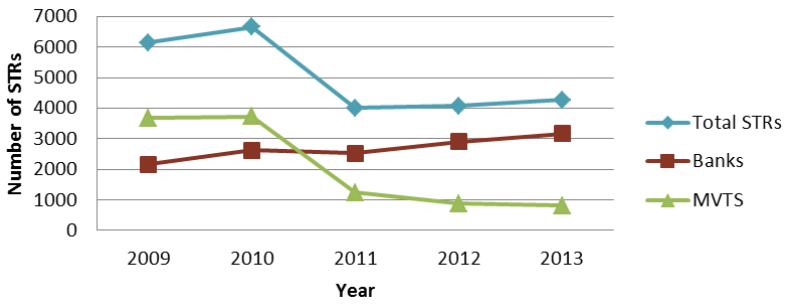
Table 5.2. Number of Reporting Entities

Type of reporting entity	2009	2010	2011	2012	2013
Banks	2 176	2 618	2 529	2 903	3 170
Insurance companies	31	42	33	55	67
Securities firms	1	7	5	1	4
Lawyers	12	6	11	12	10
Money transfer entities	3 681	3 734	1 234	882	807
e-money firms	0	0	1	1	1
Accountants	58	59	46	47	56
Real estate agents	21	15	6	17	19
Auditors	97	86	65	54	39
Dealers in expensive objects	82	78	62	59	50
Others cf. Money Laundering Act §4	2	15	26	38	49
Total	6 161	6 660	4 018	4 069	4 272

Source: data provided by Norway

5.46. The quality of reports is also highly variable. According to analysis of STRs conducted by the FIU in 2011 (the trend report on ML) a significant volume of STRs still relate to cash transactions, often involving either foreign citizenship or origin, or the building and construction industry. These do not necessarily correlate with the potential ML/TF risks facing Norway today, and the NRA notes that reporting entities may be excessively focused on certain groups or methods.

Chart 5.1 Number of STRs filed



5.47. The NRA also highlights the fact that the majority of STRs are triggered by events and analysis that may be carried out after the event, rather than reports based on risk profiling of the customer, ongoing monitoring and a good understanding of the ownership and control structure.

5.48. The FSA has expressed concern over low reporting levels and has issued findings to address some of these shortcomings in banks' systems. The FIU considers that the varying quality of STRs is due to the lack of resources allocated to AML/CFT functions by reporting entities. Although there has been a recent increase there are still some MVTS companies that have a very low reporting rate in comparison to other MVTS providers in Norway.

5.49. The FSA make good use of the currency register in detecting transactions that should have been reported to the FIU; for example, situations where structuring takes place. The FIU also reported that STRs from some regional banks represented a higher level of quality than some very large commercial banks.

5.50. While the lack of feedback on STRs, both case and sector specific (including trends and typologies) is a topic that was raised by all sectors, the FIU has engaged the banking and MVTS sectors regularly. Furthermore, it has provided guidance in the annual AML conferences, through the FIU annual report and when meeting reporting institutions. Engagement with reporting entities during the '*Round Norway*' project was very well received and improvement in quality of reports was reported. As the primary objective of '*Round Norway*' was to raise levels of awareness in police districts, the FSA did not participate. Otherwise, general coordination between the FIU and the FSA on STRs over both quantity and quality and the closely correlated issue of the effectiveness of banks ongoing monitoring systems, has been somewhat limited.

5.51. The power under section 19 of the *MLA*[8], which provides the FIU with a temporary power to order that a transaction should not be carried out, was not well understood by banks. Although the FIU reported that it talked to banks at least several times a month on this issue, statistics are not maintained and there is no internal guidance on this topic. Lack of awareness, particularly in those banks processing large volumes of payments on a daily basis, support a general lack of awareness or regular use, despite this being an important provision, albeit temporary in nature.

Conclusions on IO.4

5.52. While significant enhancements were made to the preventive measures regime in 2009, Norway has taken limited steps to update the regime since. The AML/CFT legislation remains out of step with the 2012 FATF Recommendations. These technical deficiencies limit the effectiveness of the preventive measures to some degree. The requirements for ML/TF risk assessments are not clearly understood and reporting entities do not have a well-developed understanding of risk. Some sectors, such as the banking sector have a better understanding of the criminal threats, but understanding of risk in other parts of the financial sector is weak and very limited amongst DNFBPs. Concerns exist over the quantity and quality of STRs which are predominately related to cash-based transactions. While some sectors have implemented AML/CFT measures, significant weaknesses exist regarding the implementation of key preventive measures such as beneficial ownership, PEPs, wire transfers, correspondent banking and ongoing monitoring.

5.53. Norway has a **moderate level of effectiveness** for IO.4.

5.4 Recommendations on Preventive Measures[9]

a. Norway should prioritise the implementation of CDD on a risk sensitive basis (in particular beneficial ownership information and ongoing monitoring) by financial institutions and DNFBPs and support them to apply the enhanced or specific measures for: (a) PEPs, (b) correspondent banking, (c) new technologies, (d) wire transfer rules, (e) targeted financial sanctions relating to TF, and (f) higher-risk countries identified by the FATF:

- Supervisors should prioritise support for passported MVTS, the banking sector and other sectors based on their risk profile.

8 *MLA* s.19 states 'The entity with a reporting obligation shall not carry out transactions entailing an obligation to report as referred to in s.18 before ØKOKRIM has been notified. In special cases, ØKOKRIM may order that such transactions shall not be carried out'. Further guidance is then provided regarding the circumstances in which a transaction may nevertheless be carried out before notifying ØKOKRIM.

9 These recommendations should be read in conjunction with the recommendations on supervision in chapter 6.

- Effective implementation of these and other preventive measures should be supported by risk-sensitive supervisory engagement (such as in the banking sector) (see also Chapter 6).

b. Norway should ensure that there is adequate assessment, understanding and mitigation of ML/TF risks, including appropriate mechanisms being put in place by financial institutions to document and provide risk assessment information to competent authorities, including the FSA:

- Norway should ensure that there are effective channels that will allow information on risk to be shared between the FSA/FIU/Police and financial institutions/DNFBPs.

c. Financial institutions should regularly evaluate (e.g., through internal audit), the robustness and adequacy of ongoing monitoring systems and review of accounts and transactions.

d. Norway should address the issues regarding volume and quality of STRs through a multi-disciplinary approach (FIU and supervisors):

- To ensure that FI/DNFBPs' internal policies and controls enable their timely review of: (i) complex or unusual transactions, (ii) potential STRs for reporting to the FIU, and (iii) potential false-positives.

- To ensure that STRs contain complete, accurate and adequate information relating to the suspicious transaction.

e. On the basis of ML/TF risk assessments, supervisors should ensure that financial institutions and DNFBPs adequately apply mitigating measures commensurate with the risks identified. This should include supporting the implementation of a risk-based approach whereby financial institutions have the discretion to classify customers as lower risk and conduct SDD on that basis.

f. Norway should update the MLA to ensure CDD and other requirements (including foreign and domestic PEPs, wire transfers and new technologies) are consistent with the FATF 2012 Recommendations. This should include adding a requirement that will ensure that reporting entities understand the ownership and control structure of customers.

6. SUPERVISION

Key Findings

- The Financial Supervisory Authority (FSA) is in charge of the supervision and oversight of financial institutions and has established licensing regimes. Real estate agents, auditors and accountants, also come under FSA supervision while lawyers come under the purview of a self-regulatory body (SRB).
- Money laundering / terrorist financing (ML/TF) risks have not been adequately identified and or understood by the FSA and SRBs.
- The FSA uses a combination of off-site and on-site supervision, based mostly on prudential and other industry specific risks. The frequency, scope and intensity of anti-money laundering / counter-terrorist financing (AML/CFT) supervision are not sufficiently ML/TF-risk based and requires enhancement, particularly for large complex institutions.
- The SRBs only undertake limited supervision for AML/CFT compliance.
- While some feedback and guidance on compliance with AML/CFT requirements has been provided, this has generally been insufficient to address significant knowledge gaps on some core issues.
- The FSA is aware that compliance is not at a level it should be, and in some cases serious breaches have been identified.
- There is not a wide enough range of powers to sanction, nor are they sufficiently dissuasive, and even the sanctions that are available to authorities, such as coercive fines and prosecutions, have not been imposed. No sanctions other than written warnings have been applied to financial institutions.
- There are particular concerns with the significant gaps in the supervision of the money valute transfer services (MVTS) sector. Although Norway has identified the MVTS sector as high risk in the National Risk Assessment (NRA), the FSA has not carried out any on-site inspections of MVTS providers, and there is no supervision of the extensive network of agents notified to the FSA under the *EU Payment Services Directive* which make up a large portion of the sector. In addition, despite a robust licensing system, enforcement activities to address the risk posed by unauthorised remitters are inadequate.

6.1 Background and Context

6.1. Norway's financial sector is regulated through comprehensive licensing and prudential requirements contained in sector specific legislation such as the financial institutions Act (FIA), Commercial Banks Act (CBA), Savings Banks Act (SBA), Securities Funds Act (SFA), Securities Trading Act (STA) and Insurance Act (IA). The responsibility for supervising FIs, both for prudential and AML/CFT purposes, is assigned to Norway's Financial Supervisory Authority (FSA), the functions and powers of which are set out in the Financial Services Act (FS Act).

6.2. **The Norwegian FSA** is an independent governmental agency that operates on the basis of on laws and decisions emanating from the Parliament, the Government and the MoF and on international standards for financial supervision and regulation. The FSA is headed by a non-executive board of five members appointed by the MoF upon delegation from the King. The FSA's Director General is appointed by the King in Council for a six year term. The FSA has approximately 280 employees for the prudential and AML/CFT supervision of a wide range of entities. For AML/CFT, the FSA is responsible for the supervision of FIs, estate agencies, and external accountants and auditors. The FSA is also the competent authority for supervising MVTS. Regarding EEA authorised payment institutions and their agents see below. Sanctions for non-compliance with AML/CFT obligations can be imposed based on provisions in the *Money Laundering Act* (*MLA)* and FS Act.

6.3. **Supervisory Council for Legal Practice** (Supervisory Council) is an independent governmental body financed by lawyers and responsible for AML/CFT supervision of lawyers and assistant attorneys. The governing body is a three person Supervisory Board which is appointed by the Ministry of Justice (MoJ). The Chairman must be a practicing lawyer and one member must be a chartered accountant. The secretariat of the Supervisory Council has 13 employees.

6.4. Norway has no designated supervisors for dealers in precious metals and stones and TCSPs. However, the Police Authority is responsible for the licensing and monitoring of second-hand shops to prevent the sale of stolen goods, though this does not constitute AML/CFT supervision. In addition, to the extent that trust and company services are provided by lawyers and accountants, they would be supervised by the respective supervisors for AML/CFT. In relation to casinos, although there are no land-based casinos, some internet gambling activities are licensed in Norway but are not covered by the *MLA* and therefore not supervised for compliance with AML/CFT requirements.

6.5. **DnR and NARF** – The Norwegian Institute of Public Accountants (DnR), the professional body for auditors in Norway, and the Norwegian Association of Authorised Accountants (NARF), national body for authorised external accountants, carry out quality control of their members including with regard to the implementation of AML/CFT measures. Neither the DnR nor the NARF are self-regulatory bodies for AML/CFT purposes, although they undertake supervision of their members for broader requirements. However, in determining the frequency and intensity of supervision, the FSA has decided to give less priority to those entities which are already subject to control by their respective organisations. Neither organisation has any powers, including sanctioning powers, to enforce compliance of their members with the *MLA*.

6.2 Technical Compliance (R.26-28, R.34, R.35)

Recommendation 26 – Regulation and supervision of financial institutions

6.6. Norway is rated partially compliant (PC) with Recommendation (R.) 26. The licensing function for reporting financial institutions (FIs) is divided between the MoF and the FSA. Licensing covers both core principles and other reporting FIs, including MVTS and money currency exchange providers. As the financial sector supervisor, the FSA conducts fit and proper tests when a reporting FI is granted a license. Investments firms, management companies for securities funds, securities register, regulated market, debt-collecting businesses, real estate agents, foreign branches of Norwegian insurance and pensions companies and savings banks are obliged to notify the FSA of any changes in key functionaries. However, there is no similar requirement for commercial banks, savings banks, and all insurance and finance companies.

6.7. The FSA's supervision of core principles FIs is said to be founded on a risk-based approach but the assessment to determine which reporting FIs are subject to on-site inspections is largely based on prudential information. There is insufficient evidence to conclude that ML/TF risks are adequately taken into account when determining priorities for AML/CFT supervision. In addition, AML/CFT supervision of securities has only formed a minor part of the broader on-site inspections. Before recent on-site visits, no AML/CFT inspections were carried out in the insurance sector. For authorised MVTS providers, the FSA only monitors AML/CFT compliance via off-site or document based supervision. The FSA does not conduct any monitoring for AML/CFT compliance of MVTS providers from the European Economic Area (EEA) which have agents or branches providing services in Norway.

6.8. The FSA has only limited written documentation to support institution specific ML/TF risk assessments and there is no reliable formal risk assessment which could provide a basis for the classification of reporting FIs based on ML/TF risks. As a result, the FSA has no sound basis to decide on the frequency and intensity of on-site and off-site AML/CFT supervision of financial institutions and groups.

Recommendation 27 – Powers of supervisors

6.9. Norway is rated largely compliant (LC) with R.27. The FSA has comprehensive inspection and monitoring powers, including the power to conduct on-site inspections and off-site reviews. The FSA also has the power to compel the production of or obtain access to reporting FIs' records without the need for a court order. However the sanctions powers are inadequate (see R.35).

Recommendation 28 – Regulation and supervision of DNFBPs

6.10. Norway is rated PC with R.28. Casinos are not classified as a reporting designated non-financial business or profession (DNFBP) in Norway, although casinos are prohibited without a licence. Only two entities are currently licenced, one ship-based casino and an entity which offers casino-style gaming on the Internet. For more details see section 5.1 above. The FSA is the competent AML/CFT supervisor for real estate agents, accountants and auditors while the Supervisory Council for Legal Practice is responsible for ensuring compliance by lawyers and other independent legal professionals with AML/CFT requirements. Norway has no designated competent authority for AML/CFT monitoring and supervision of trust and company service providers (TCSPs) and dealers in precious metals and stones. While both the FSA and the Supervisory Council have adequate powers to perform their functions and conduct fit and proper tests, the sanctions at their disposal for non-compliance with AML/CFT obligations are not proportionate and dissuasive, as explained in relation to R.35 below.

6.11. The FSA and the Supervisory Council have no specific ML/TF risk assessments for the categories of DNFBPs that they supervise nor is there a reliable formal risk assessment which could provide a basis for the classification of reporting DNFBPs based on ML/TF risks. AML/CFT supervision of DNFBPs is conducted as part of a more general supervision to ensure compliance with licensing provisions and to monitor professional conduct. As a result, the frequency and intensity of the AML/CFT supervision of DNFBPs is not based on the supervisor's understanding of the ML/TF risks that these professions face.

Recommendation 34 – Guidance and feedback

6.12. Norway is rated LC with R.34. In cooperation with the private sector, Norway's FSA and FIU have set up some formal guidance mechanisms for both the private and public sectors through the creation of a dedicated AML/CFT website and the holding of an annual AML/CFT conference. Information is made available on the legislation, typologies and trends, and on the FATF and the Egmont Group. This information provides relevant background and contributes to a better understanding by the private sector of general AML/CFT issues. The guidance is comparatively high-level and does not provide sufficient assistance to reporting entities regarding the implementation of AML/CFT requirements on a day-to-day basis.

6.13. The FIU has assigned a full-time position dedicated to ensuring compliance by FIs and DNFBPs with the reporting obligation. Concrete feedback and guidance is provided both upon request and spontaneously, including through face-to-face meetings with individual entities. In addition, the FIU also delivers presentations on how to improve compliance with reporting obligations during seminars which specifically focus on certain

categories of reporting entities. The FIU produces annual reports with information on typologies, case examples and statistics and contributes to ØKOKRIM's report on trends in financial crime.

6.14. In June 2009, the FSA issued Circular 8/2009 which contains general AML/CFT guidelines for the implementation of 2009 *MLA* and *MLR* provisions. This guidance paper does not adequately support the effective implementation of the key building blocks of Norway's AML/CFT regime. While the FSA has provided some training and feedback, this has not been proactive or sufficient.

6.15. The PST is well engaged in providing feedback on CFT, including typologies, to both public and private sector entities, often in cooperation with the FIU. This feedback is provided both on a case-by-case basis and through participation in training sessions and seminars. Norway was unable to provide the assessment team with concrete examples of feedback from other LEAs to the reporting entities.

Recommendation 35 – Sanctions

6.16. Norway is rated PC with R.35. The *MLA* contains specific sanction provisions for failures to comply with AML/CFT obligations, although there are no administrative penalties available. Supervisory authorities are empowered to issue orders and coercive fines against reporting entities as a sanction for non-compliance with those orders. The *MLA* is silent with regard to the level of coercive fines but the MoF does have regulation-making authority regarding coercive fines. So far, the Ministry has not yet issued such implementing regulations. The *MLA* also provides for criminal proceedings, which could result in fines being imposed on both reporting entities and their directors and senior management for non-compliance with s5 (risk-based approach (RBA) to customer due diligence (CDD)), s6-8 (timing of, and requirements when performing, CDD and record keeping of information obtained through CDD), s.15 (enhanced CDD), s.17-18 (STR-reporting) and s.22 (record keeping – suspicious transaction reports (STRs)). In particularly serious cases penalties of up to one year's imprisonment can apply. However, these eight sections do not cover some of the fundamental building blocks of Norway's AML/CFT regime, including certain CDD requirements (e.g., timing, third parties and reliance), the obligation to apply on-going monitoring, corresponding banking relationship requirements, internal control requirements, and the tipping-off provisions. Moreover the need to prove the failings to the criminal standard of proof would be more difficult than the civil standard for administrative fines.

6.17. The sanction provisions of the *MLA* are complemented by the FSA's sanctioning powers included in the FS Act. These include withdrawing, restricting or suspending the licence of the reporting entities, fines and orders to rectify deficiencies. In addition, any person, including officers, employees, senior management and directors of reporting entities supervised by the FSA, can be liable to fines and/or imprisonment when they wilfully or through negligence contravene an order issued by the FSA. As with the *MLA*, these non-coercive fines can only be imposed if criminal proceedings are brought.

6.18. The *MLA*, in combination with the *FS Act*, provides the FSA with a limited range of sanctions for failures to comply with the AML/CFT requirements. These sanctions cannot be considered to be proportionate and dissuasive, especially for directors and senior management. The major shortcomings are that the fines provided for in the *MLA* are not available for the breach of a number of core requirements. Furthermore, non-coercive fines are only available as a result of criminal proceedings, and that the range of sanctions available should be broader.

6.3 Effectiveness: Immediate Outcome 3 (Supervision)

Licensing and other Controls

6.19. Institutional arrangements for the supervision and oversight of financial institutions, as well as real estate agents, auditors and accountants, are well developed, as are the respective licensing regimes. For other DNFBPs there are no such regimes. A pillar of Norway's approach to supervision has been its comprehensive and robust licensing and regulation of financial institutions; Norway maintains that it is easier to refuse a licence than assess an institution for compliance. Notwithstanding such an approach, only limited sanctions

for those engaged in financial activities outside of the relevant licensing regime have been applied, although such unlicensed activity does appear to take place in some sectors, notably MVTS.

6.20. The FSA assesses the fitness and properness of board members and persons directly in charge of the reporting entity. A license must not be granted if persons possessing key functions cannot live up to the fit and proper requirements. Although the FSA, as part of its supervisory objective, examines any changes in key functions, there are no obligations on commercial banks, insurance and finance companies to notify the FSA of any changes in key functions or of information which formed the basis for assessing a person as fit and proper. However, these entities are also required to ensure that the fit and proper requirements are met at all time and the FSA considers this issue in its supervision. Nevertheless, this is a significant technical deficiency which could undermine the FSA's ability to prevent criminals from controlling and holding a management function in financial institutions.

6.21. Norway also permits the operation of branches of credit institutions authorised in other EEA countries. The decision to issue an authorisation valid for the EU is the responsibility of the competent authority of the home Member State. Such a financial institution may then provide services or perform activities throughout the EU, either through the establishment of a branch or through the free provision of services, without the need to obtain additional authorisations in each host Member State. However, these branches in Norway are subject to Norwegian AML/CFT laws, and the FSA is the supervisor for the 42 branches which currently operate in Norway and they are subject to the same level of AML/CFT supervision as Norwegian financial institutions. For a financial institution providing services without a physical presence in Norway, supervision is carried out by the home supervisor for AML/CFT.

Supervisors' understanding of ML/TF risks

6.22. The measures used by the FSA to understand and assess ML/TF risks of the sectors and entities they supervise do not facilitate a clear understanding of all ML/TF risks. No specific tools have been developed to collect information that is needed for identifying and maintaining an understanding of ML/TF risk. The FSA does not assign an ML/TF risk classification to any reporting entity.

6.23. The FSA has not undertaken sufficient AML/CFT supervision across all sectors. Supervisors have a varied knowledge of ML/TF risks that are primarily based on the inspections, but have too little knowledge of the risks associated with products, services, customers, geographic locations etc., to assist them in evaluating the financial institution's own ML/TF risks. Very limited sharing of knowledge has occurred across the different sections until recently. Supervisors have therefore not been in a position to compare risk factors and procedures as used by peer financial institutions. It was notable that in the NRA, in which the FSA participated a number of risks that were largely assumed and could not be supported by information and analysis, while a number of risks that were consistently raised by different banks were not included at all. ML/TF risk is considered by the FSA to be an integral part of operational risk, which is a concern given its narrow focus.

6.24. Based on the vulnerabilities identified in the NRA, efforts are being made to address shortcomings and recently the FSA has established a working group with participants from across the different sections with the purpose of sharing knowledge in the AML/CFT area.

6.25. The Supervisory Council has neither identified nor assessed, to any extent, ML/TF threats and vulnerabilities for lawyers and subsequently displays a very limited appreciation of ML/TF risks. There is a limited understanding of situations where lawyers are misusing their office for criminal activities and laundering the proceeds of such activities, or where customers are misusing lawyers for ML.

Risk-based approach to AML/CFT supervision – by sector

6.26. The focus, depth and frequency of FSA supervision is primarily driven by prudential and other concerns and is not sufficiently ML/TF risk sensitive. The FSA maintains its AML/CFT supervision of REs is founded on a risk-based approach, based on the "module for the assessment of operational risk". The module is a tool that is used to identify and assess the quality of risk management and operational risk in

institutions. It consists respectively of guidance and information, and poses questions related to institutions' risk management and loss event categories. ML/TF is mentioned as examples in the category "external fraud". The questions are further designed to be used for purposes of institutional self-assessment. The document contains (in an annex) a template of AML/CFT questions, but the framework does not provide a sufficient focus on ML/TF risks for AML/CFT supervisory activity, particularly given that ML/TF risk is defined narrowly under 'external fraud'. ML/TF risk is very different to operational risk, which is focused on potential losses for the institution. The FSA has in its supervision focused on the 18 (now 17) large commercial banks (which due to the concentrated nature of the Norwegian banking sector have the most significant ML/TF risks in the sector), but even for these banks the frequency, intensity and scope of the AML/CFT supervisory activities has been in adequate.

6.27. The focus on AML/CFT supervision of auditors and audit firms is based on a statutory and cyclical scheme. In addition the FSA carries out risk-based supervision, although ML/TF risk is not a central selection criterion. With regard to external accountants, the FSA's selection of entities for inspection is primarily based on reports from other authorities and bodies, i.e., tax with focus on violations of tax and accounting regulations. Supervision in the securities sector is focused on market abuse, but ML/TF risk is considered to a limited extent.

6.28. Within the FSA, AML/CFT inspections are carried out by sectoral supervisors primarily as a part of their prudential supervision, although some targeted AML/CFT inspections has been carried out. They undertake AML/CFT inspections using standard templates containing basic questions regarding compliance with the *MLA*: risk classification of customers, CDD of non-face-to-face customers and internal controls. In addition, sample testing of the reporting entities' due diligence of the five newest retail and corporate customer relationships is usually carried out.

6.29. In general, the inspections are focused on technical compliance with the AML/CFT regulations and not on the effectiveness and robustness of the preventive measures implemented by the reporting entities. For example, FIs are required to have an electronic monitoring system, which is routinely met by FIs using an external service provider. During the inspections the FSA will audit the fact that the FI has such a system but no examination would be performed to validate whether the system was effective and whether the FI understood the objectives or key performance indicators. No sample testing is conducted. When the FSA has focused on STRs in its monitoring activity, it has focused largely on the quantity, although recently quality has also become an issue. Some key *MLA* requirements relating to high risk activities, such as correspondent banking, have not been subject to any examination or inspection. This stems from the fact that the FSA has not developed any formal policies that specifically ensure that AML/CFT inspections identify and target higher risk activities of the FI.

6.30. As can be seen from Table 6.1 below, the FSA has not undertaken sufficient AML/CFT supervision across the sectors – no inspections in either the MVTS sector which is considered as a high risk sector both by the FSA and in the NRA, or in the life insurance sector.

Table 6.1. On-site inspections with an AML/CFT component

Industry sector	2009	2010	2011	2012	2013
Banks	13	16	32	29	30
Insurance	0	0	0	0	0
Securities	16	24	18	19	12
MVTS	0	0	0	0	0
Other financial institutions	0	0	0	0	0
Real estate agents	29	48	93	43	50
Auditors, Audit firms and External Accountants	159	141	103	108	102
Lawyers	33	48	23	19	20

Source: data provided by Norway

6.31. Banks In 2010, the FSA conducted 16 AML/CFT on-site inspections of bank and finance companies for the purpose of obtaining an overview of compliance with the *MLA* that had entered into force in April 2009. The inspections comprised reporting entities from the most significant financial groups operating in Norway, including the private banking and shipping departments of Norway's two largest banks. The inspections generally covered basic obligations such as risk classification of customers, BO information, purpose and intended nature of the customer relationship, ongoing monitoring, internal controls, training of employees, and sample testing of CDD of retail and corporate customers. Although some pre-onsite fieldwork was undertaken, these examinations were very short and high level in nature. The banks concerned described these as akin to audits rather than in depth examinations. FSA findings regarding compliance with the *MLA* revealed considerable room for improvement.

6.32. In 2013, the FSA carried out 30 on-site inspections of bank and finance companies driven by prudential considerations, but which included a small AML/CFT component, The AML/CFT component was carried out on a time interval of between 2-4 hours depending on the size of the bank. Concerns with regard to *MLA* compliance were raised in 30 preliminary inspection reports to 28 banks and 2 finance companies. The concerns were followed up with critical remarks in 19 final reports to 17 banks and 2 finance companies. By April 2014 five of the 30 inspections remained ongoing. Although the FSA found deficiencies, no other sanctions had been imposed in any case at the time of the on-site visit. In addition, the FSA carried out one inspection of one of the largest banks in Norway focusing solely on AML/CFT issues in 2013. During this inspection the FSA not only focused on basic *MLA* obligations but included issues such as the bank's risk assessment and management engagement.

6.33. In 2013, the FSA also conducted a document based off-site inspection of all 140 banks conducting business in Norway (including branches of EEA credit institutions). The questionnaire that the banks had to fill in included questions regarding internal controls, reports from internal audit, procedures regarding BO, enhanced CDD, training of staff and STRs. The off-site review revealed that 35 of 140 banks considered that they had no or very few high risk customers, which the FSA found was a weak understanding of the AML/CFT regulation. The review also revealed a serious lack of *MLA* compliance in several small savings banks that had not been inspected by the FSA between 2010 and 2013. In six cases, owing to the seriousness of the compliance failures it found, the FSA issued "advance notifications" (as required under the *Public Administration Act* s.16) of possible "Orders and coercive measures" that might be imposed under *MLA* s.27. While the types of activities carried out at such small savings banks may present lower ML/TF risks, nevertheless, no sanctions have been imposed. Given that it is five years since the *MLA* was updated, such serious levels of compliance failures suggest that the FSA's approach has not been effective. The FSA's supervision of the banking sector is not effective, focusing on technical compliance with laws rather than effective implementation, and is not based on ML/TF risks.

6.34. **Brokers, investment firms and fund management firms:** While AML/CFT is said to be part of all regular FSA on-site inspections, these focus primarily on conduct of business and has little focus on AML/CFT. For example, issues relating to AML/CFT had never been commented upon in any inspection report. AML/CFT issues are considered at a very high level; sample testing of transactions is carried out, but for the purpose of examining compliance with the MiFid-regulation. Norway maintains that the ML/TF risk in the securities industry is low, which may be the case, but, this is assumed and there is no real consideration of ML/TF risks in the supervision of this sector.

6.35. **Insurance:** The FSA had, up until April 2014, not undertaken any AML/CFT supervision of insurance companies. The FSA has since carried out the first AML/CFT on-site inspection of a non-life insurance company as part of the prudential inspection. The supervisors did not, prior to the undertaking, receive AML/CFT training, although a brief introduction to the template to be filled in during the inspection was given by an employee of the Banking Section. The FSA has programmed another 3 inspections, including for AML/CFT, with the purpose of highlighting AML/CFT and assessing the level of *MLA* compliance in the relevant insurance companies. Again, ML/TF risks have not been taken into consideration and the fact that examinations have been commenced in non-life insurance before life is difficult to understand from a ML/TF risk perspective.

6.36. ***MVTS – Domestic:*** Concerns exist over the supervision of this high risk sector. While there are a number of offsite controls, no on-site supervision to test the robustness of systems and controls of licensed

remitters has taken place. In 2010, Norway implemented the PSD, and subsequently authorised 31 payment institutions. Norway implemented requirements for limited authorisation of MVTS which are not defined as payment institutions in the legislation, allowing the FSA to waive some of the general rules required for authorisation of payment institutions. The initial approach was to provide for a limited authorisation, including lower capital requirements and low thresholds on the average amount of monthly transactions. In order to get as many MVTS under supervision as possible, the FSA lowered the requirements for a short period. MVTS authorised in this period were given a temporary license with a renewal requirement within two years (the transition period). In the transition period the FSA received 65 applications, and 29 MVTS were granted a limited authorisation. The FSA is still in the renewal process for those MVTS with the temporary license, although five authorisations have been withdrawn. The FSA received 37 applications for limited authorisations after the end of the transition period, but only two of these companies were granted an authorisation.

6.37. The FSA carries out desk reviews of AML/CFT compliance of the MVTS companies' by assessing semi-annual reports and applications for renewal of the limited authorisations, as well as information received from the Norwegian FIU and other police authorities, the Currency Register, the Directorate of Customs and Excise and the tax authorities. Local MVTS are also subject to independent audit and regular transaction reporting. In 2012 MVTS companies were required to provide additional information on their CDD measures when submitting their semi-annual reports. This consisted of sending in documentation of CDD procedures performed by the company for the last five customers. In addition to these formal channels, the FSA also monitor the press and, occasionally, receive tips and information from outside sources. The level of compliance with AML/CFT requirements is a concern to the FSA. Despite this, no on-site supervision has been carried out which is a significant concern given the ML/TF risk.

6.38. The FSA has established a robust licencing regime for money remitters, rejecting a significant number of applications, but during interviews conducted by the assessment team it was suggested that this may have achieved a result which is inconsistent with the initial policy objectives. Many MVTS in Norway are operating without a license. The Police are the competent authority to identify such unauthorised MVTS providers. However, in practice the FIU also plays an important role identifying unauthorised providers through STRs and currency reporting, and liaising with the FSA to determine whether these providers have made unsuccessful license applications. The FIU has then informed police, as well as financial institutions, of these unauthorised providers. Authorities provided four examples of action taken by police against unauthorised MVTS providers, while authorities informed that some other cases are ongoing. These cases were identified by the FIU through STRs and passed on to police, with some engagement with the FSA, while other cases were identified by the police in the course of criminal investigations. These entities received a criminal fine for providing MVTS services without a license. In one case, the unauthorised MVTS service provider also committed a ML offence. The other case is explained further below.

Box 6.1. Case example: unauthorised MVTS providers

In 2012, Telemark Police District fined a person 30,000 NOK (3,900 EUR) and confiscated 16,000 NOK (2,080 EUR) for operating an unauthorised MVTS provider. The transfers were conducted through the person's sole proprietorship, and no application had been made to the FSA. From January-October 2012, the firm received 1,615,000 NOK that was transferred to a company in a third country and then to the final recipients in Afghanistan. The person pleaded guilty and accepted both the fine and the confiscation. The case started with two STRs being sent to the FIU.

6.39. Although action has been taken on an ad hoc basis, there is no strategy to identify and sanction unauthorised MVTS providers based on a policy objective. Many unauthorised providers are known to authorities given the number of unsuccessful applications for limited authorisations or renewals. The FIU has led the action taken, although there has been no proactive approach. This has resulted in a limited number of sanctions.

6.40. **MVTS – EEA payment institutions and their agents:** The FSA has not carried out any supervision of EEA payment institutions and their agents operating in Norway. Under the EU payment services directive,

this falls under the obligation of the home Member State of the payment institution, except when the home Member State asks for administrative cooperation or when the payment institution operates under right of establishment. EEA payment institutions with an authorisation from another country under the PSD operating in Norway are covered by *MLA*. According to the FSA, agents of EEA payment institutions are also covered by the *MLA* although it is not explicit in the Act. On this basis, both EEA payment institutions and their agents are subject to FSA supervision for their AML/CFT obligations. Despite this acknowledgement by the FSA – and although Norway has identified the MVTS sector as high risk in the national risk assessment – there is no supervision of the extensive network of agents notified to the FSA regarding their AML/CFT obligations.

6.41. The FSA undertakes its supervisory role in accordance with the cooperation system put in place by the PSD. According to the directive the home authority is the designated main supervisor, although the home and host should cooperate in this matter. As the FSA considers that the home supervisor has the primary supervisory responsibility, the FSA has not taken any supervisory action with respect of EEA payment institutions and the large network of passported agents operating in Norway. Along with other Nordic supervisors the FSA attempted to enter into an agreement with the home supervisor of a large MVTS provider operating in the Nordic Countries. This attempt failed and the FSA has not followed through with its engagement with home supervisors. As a result, this part of the MVTS sector, which forms a large part of the MVTS sector in Norway, remains unsupervised.

6.42. **Real Estate Agents:** As part of on-site visits inspecting broader licencing requirements, the FSA examines whether real estate agents have AML/CFT polices and asks questions regarding compliance with the *MLA*. However, AML/CFT comprises only a small portion of the FSA's supervisory activities in the real estate sector. The approach was described by the sector as an audit, the usefulness of which is limited. In 2013 the FSA carried out 42 inspections of both big chains and small agencies. As with other sectors, the FSA had made no clear determination of ML/TF risks within the sector, but the fact that chains tended to be part of large financial groups with higher standards and ranges of procedures should have been taken into consideration. About 6-7 of these inspections did not include AML/CFT. Over the last four years, the FSA has conducted approximately 200 inspections of real estate agencies, including AML/CFT (out of a total of 510 real estate agencies and 1320 lawyers). The reason why the FSA carries out many inspections of real estate agents is not based on consideration of risks, rather that there are less intensive licensing requirements compared to other REs and many consumer protection related activities.

6.43. **Auditors, Audit firms and External Accountants:** There has been limited AML/CFT supervision of auditors, audit firms and accountants. The FSA is the competent supervisory authority for auditors and accountants and is responsible for monitoring of these sectors, and in its supervisory approach takes into account the work undertaken by the professional associations. NARF and DnR, also monitor its members' compliance with AML/CFT to a limited extent as part of its ordinary monitoring for compliance with other professional obligations, although they have no supervisory powers. The FSA has laid down guidelines for cooperation with NARF for coordination of on-site inspections. Under these guidelines, NARF should report findings of non-compliance with AML/CFT obligations to the FSA. However, the level of monitoring is insufficient and it is unclear whether any such findings have been reported.

6.44. The FSA undertakes both on-site and off-site inspections, taking into account the activities of the industry associations of auditors and accountants. The inspections include control of the entities' compliance with *MLA*. An on-site inspection of a larger firm is conducted over a period of 2 weeks, spending around 1 hour on AML/CFT issues. Every second year the FSA carries out off-site supervision of auditors, audit firms and external accountants. All entities must respond to questions concerning their activities, including compliance with *MLA*. The information collected provides a basis for determining how current supervision activities should be arranged, and provides general information about the sector.

6.45. The selection of candidates for inspections of auditors and audit firms is mainly based on a statutory, cyclical scheme. All practicing auditors and audit firms must be subject to a quality control process at least every six years. Auditors whom audit public interest entities (PIE) shall be subject to a quality control process at least every third year.

6.46. **Lawyers:** AML/CFT supervision of lawyers is very limited and not effective. The Supervisory Council has not undertaken a risk assessment and has no policies for carrying out AML/CFT inspections. Preventive

measures on ML/TF are not focused on when carrying out inspection of lawyers. There is some assessment of annual returns but this has a very limited value. The supervisory council displays a limited awareness of AML/CFT issues.

Risk-based supervision and regulatory responses

6.47. There has been no clear determination, based on ML/TF risk, of the type and level of resources needed to ensure effective risk-based AML/CFT supervision. The resources and capacity to conduct effective AML/CFT supervision are not adequate and specialist knowledge is insufficient.

6.48. When an inspection is closed the reporting entity receives a draft inspection report ("preliminary report") from the FSA. The reporting entity is given an opportunity to rectify breaches by a certain deadline before the report is finalised. The final inspection report is public but does not reflect breaches of the AML/CFT requirements identified at the time when the inspection was carried out, if these have been adequately addressed by the reporting entity. The FSA is authorised to impose a range of sanctions against the reporting entity under FSA supervision. However, although compliance is not at a level it should be (and in some cases serious breaches have been identified), sanctions, including coercive fines or prosecutions, available to the FSA have not been imposed. In addition, the criminal penalties available under the *MLA* have never been applied.

6.49. The majority of regulatory responses imposed by the FSA are "written warnings" in the final reports, also called "red letters". The FSA follows up within a reasonable time of the on- or off-site inspection. According to the FSA, the majority of institutions (banks and finance companies) have remedied the shortcomings at the time of the follow-up. If that is not the case administrative sanctions may be imposed if considered necessary. This FSA feels that this has not yet occurred concerning AML/CFT. The FSA did advise however about a case where they required a significant increase in the capital adequacy of one large commercial bank due to operational risks, primarily due to IT systems and partly they stated as a result of important deficiencies identified in relation to CDD and AML/CFT controls in the same period.

6.50. The FSA has not given consideration as to how the different requirements under the *MLA* are classified and what constitutes a serious breach of these requirements, and the actions that would be taken pursuant to that breach. As a result, the FSA has not prepared any internal, or public, written policies for the use of the sanctions it has available. In addition, no regulations on the amount of fines under the *MLA* have been issued to date by the MoF, even though the amounts of coercive fines are laid down in regulations for other areas of the FSA's supervisory function, such as for breaches of prudential requirements. Taken from an industry perspective there is no transparency or degree of what may be expected in the case of serious breaches. In the absence of guidance in this area, there is an expectation that the current status quo will continue and that the FSA would not use more severe actions.

6.51. As such, sanctions appear to neither be effective nor dissuasive.

6.52. Table 6.2 below sets out all warning issued by the FSA including both ordinary warnings and advanced warnings. It shows a significant increase in warnings issued to the banking sector from 2011 to 2012, which was a result of the increased on-site inspections undertaken in 2010. The FSA has issued advanced warnings and an order to cease contravening the *MLA* provisions to seven banks (one in 2010 and six in 2013), which were primarily for severe lack of compliance with AML/CFT obligations in the *MLA*. The advance warnings issued in 2013 were due to compliance failings identified in 2010 and it is a concern that compliance failings had not yet been addressed or remedied by the banks three years after they were identified by the FSA in inspection reports. The length of time between the on-site inspection in 2010 and issuance of advanced warnings in 2013 is a concern as the failings remained three years' later despite the supervisory activities of the FSA.

Table 6.2. Warnings for AML/CFT deficiencies

Industry sector	2009	2010	2011	2012	2013
Banks	2	2	1	33	27
Insurance	0	0	0	0	0
Securities	0	0	0	0	1
MVTS	0	0	0	0	0
Other financial institutions	0	0	0	0	0
Real estate agents	0	1	1	13	14
Auditors, Audit firms and External Accountants	8	1	4	35	10
Lawyers	3	3	8	3	4

Source: data provided by Norway

6.53. Despite the fact that the FSA had identified severe lack of compliance by banks with AML/CFT obligations, no other types of sanctions, such as fines or restrictions on licencing, have been imposed. In addition, in the absence of internal guidance or procedures the FSA were unable to provide any clarity regarding the nature of the *MLA* breaches that would justify the application of these sanctions and the appropriate level of sanctions that would apply for aggravated breaches. In those instances where advanced warnings were given to six small saving banks, the potential administrative coercive fines advised to the banks if they failed to comply with the cease contravening order (after a certain period of time) were determined by the FSA to be NOK 5000 (EUR 650) per day. To provide some guidance on this, the FSA also advised that it considers, in relation to enforcement of a mandatory pension scheme, that the amount of NOK 250 (EUR 32.50) per day per employee to be an appropriate penalty for lack of compliance. These amounts were communicated to the institution in the order and do not overcome the concerns relating to the dissuasiveness of the sanctions without specified amounts.

6.54. For accountants and auditors, five sanctions were in the form of withdrawal of licences for issues which included an AML/CFT component, and nine orders were made which included requirements to cease contravening the *MLA*. These sanctions were applied for a number of reasons, including severe lack of compliance with the *MLA*, breach of the duty of secrecy provisions in the *MLA*, and failure to implement CDD obligations.

6.55. No sanctions have been applied to the securities sector, other financial institutions, and the real estate sector. In addition, no sanctions other than warnings have been applied to financial institutions. This is likely caused by the insufficient supervision for AML/CFT purposes of these sectors, including the level of on-site visits, which has meant that the FSA has either not identified deficiencies or has not taken action where severe deficiencies have been identified. For MVTS providers authorised by Norway, the FSA has declined to renew certain licences which may, in part, explain the lack of sanctions against this part of the MVTS sector.

Guidance and feedback

6.56. While some feedback and guidance on compliance with AML/CFT requirements has been provided by the FSA, and they are reported as being responsive to direct enquiries from industry, significant knowledge gaps on some core issues remain in the private sector (see IO.4 above). Although the 2009 guidance was issued with industry collaboration, nothing has been issued since, and guidance given at the annual basis industry seminar is comparatively high level. Engagement at the industry or sector level has not been sufficient, despite the fact that ambiguities remain on certain core requirements.

6.57. The FSA has a good practice of publishing final inspection reports, which contain and describe breaches of the *MLA*, and the FSA considers that the key findings in such reports provide guidance. While

industry is supportive of this practice, the focus is primarily on technical compliance, and any guidance on how to improve AML/CFT measures is very limited. However, there appear to be recent developments in the inspection reports prepared by the Banking Section, whereby breaches are described more thoroughly thus making the reports more useful to the banks. The FSA has also provided some ad hoc guidance. In 2010, the FSA sent a summary of the findings of the 2010 on-site inspections to all banks and finance companies operating in Norway, including a request to issue action plans to improve compliance with the *MLA*. In 2013 a letter was sent to all external auditors and accountants to stress the importance of the external auditors' duty to follow up on breaches of requirements by MVTS providers and to report these to the FSA.

6.58. Each year Finance Norway, the Norwegian FIU and the FSA, arrange a two day AML/CFT conference which is attended by around 250 people. The conference is aimed at staff of financial institutions from Norway's largest banks and insurance companies to small hawaladars working with AML/CFT, as well as other groups, subject to the *MLA*, public authorities with AML responsibilities etc. While FSA does engage in this training, the material used was focused on high level concepts, rather than how to implement particular obligations or to mitigate certain risks.

Supervision of asset freezing measures pursuant to UNSCR 1267

6.59. The FSA does not adequately monitor reporting entities with regard to their obligations to freeze assets related to TF. The FSA has not examined this issue as part of their on-site supervisory activities and has only undertaken limited off-site supervision through a questionnaire. The only instance where the FSA considered this specifically was as part of a questionnaire to the banking sector in 2013, which included some specific questions on how they implement targeted financial sanctions. The FSA is aware that FIs rely solely on private service providers to carry out their obligations. However, it has not considered whether these measures are sufficient to meet the requirements. However, the FSA has not assessed the adequacy of reporting entities processes for the identification of assets related to TF or proliferation financing (PF). There is no supervision of DNFBPs relating to the implementation of the sanctions regimes.

6.60. There is limited coordination between the FSA and other relevant agencies (PST, FIU) in relation to TF and PF issues which appears to be a factor in the lack of focus on these issues by the FSA. The lack of coordination between FSA and PST is an important issue as it increases the difficulty for the FSA to monitor reporting entities as it is unable to apply a risk-based approach to supervision. While financial institutions understand their obligations, this may be due to international focus on UN Taliban/Al Qaida sanctions.

Conclusion on IO.3

6.61. Major improvements are needed to Norway's AML/CFT supervision. The supervisors do not possess a sound understanding of ML/TF risks and supervisory activities are primarily driven by prudential and other supervisory risks and concerns, although some targeted AML/CFT supervision has taken place. The frequency, scope and intensity of such supervision are not sufficient, nor are they based on ML/TF risks. The FSA's supervision has mostly been focused on technical compliance rather than the effectiveness and robustness of the preventive measures implemented. Sampling has been limited and some important measures, such as transaction monitoring systems or wire transfer requirements, have never been tested at all. In addition, guidance and feedback by the FSA on AML/CFT requirements has been insufficient and has not addressed significant knowledge gaps on some core issues. Certain sectors (e.g., securities, MVTS, legal sectors) and activities (e.g., targeted financial sanctions) have only been subject to limited AML/CFT supervision. Only the 18 (now 17) major banks are covered more regularly and slightly more fully for AML/CFT compliance.

6.62. While the licencing system for MVTS providers is robust, this is not combined with adequate measures to identify and sanction unauthorised providers. There is also a particular concern with the lack of supervision of passported MVTS providers which comprise a substantial portion of the market. This is an important factor given the high ML/TF risk posed by this sector. Furthermore, although the FSA is aware that compliance is not at a level it should be, and in some cases serious breaches have been identified, the limited sanctions that are available to authorities, including coercive fines or prosecutions, have not been

imposed. It is a concern that serious compliance failings have not led to remedial action despite continued non-compliance over several years, with little or no supervisory action by the FSA.

6.63. Norway has a **moderate level of effectiveness** for IO.3.

6.4 Recommendations on Supervision[1]

a. Norway should designate supervisors for dealers in precious metals and stones, TCSPs and casino gaming activities.

b. As part of the NRA, Norway should undertake comprehensive sectoral risk assessments to ensure that the ML/TF risks are adequately identified and understood by supervisors. These should be periodically reviewed to ensure they remain up-to-date.

c. On the basis of the risk assessment, Norway should ensure its future supervision is sufficiently ML/TF risk sensitive. Norway should ensure a greater level of integration of AML/CFT supervision into its broader framework of prudential and market conduct supervision.

d. Norway should set supervisory priorities based on risk which address resources and capacity of supervisors, increase the intensity, duration and frequency of off/onsite supervision to commensurate with risk. The FSA should:

- Continue to use a combination of off-site and on-site supervision but adapt the frequency, scope and intensity of supervision to the ML/TF risks.
- Ensure higher risk sectors (such as MVTS and banking sectors) are adequately supervised, including more intense, wider scope reviews, and sampling of high risk operations, such as correspondent banking, wire transfers and targeted financial sanctions.
- Focus on the effectiveness and robustness of the AML/CFT measures, rather than on technical compliance e.g., validating whether monitoring systems are effective and whether the FI understands the objectives or key performance indicators.

e. Norway should establish and implement procedures, systems and manuals to support effective AML/CFT supervision by the FSA and Supervisory Council[2].

f. Norway should ensure sufficiency of resources, to support both onsite supervision andcooperation with domestic and international authorities responsible for performing AML/CFT supervision:

- The FSA should increase the type and level of supervisory resources put into risk-based onsite supervision (e.g., time allocated to various supervisory tasks such as sample testing).
- Norway should enhance the type and level of resources required to ensure effective AML/CFT supervision is carried out by supervisors with AML/CFT experience (e.g., prioritise specialist training of its supervisors on ML/TF risk, prevention and supervision, participation in AML/CFT forums, supervisory colleges, etc.).

1 These recommendations should be read in conjunction with the recommendations on preventive measures in Chapter 5.

2 The measures recommended for the FSA are recommended to the Supervisory Council (with appropriate modification).

g. Supervisors, in particular the FSA, should ensure that AML/CFT deficiencies identified during examinations lead to supervisory actions that are dissuasive, proportionate and effective. The FSA should extend the ability to apply administrative sanctions to all provisions of the MLA, and give consideration to developing processes and procedures on what constitutes a serious breach of these requirements, and the actions that would be taken pursuant to that breach. Regulations on the amount of fines under the MLA should be issued.

h. The supervisory authorities should ensure adequate on-going private sector engagement (for example, through seminars, guidance or best practices) that supports the effective implementation of preventive measures.

7. LEGAL PERSONS AND ARRANGEMENTS

Key Findings

- There is a real risk that criminals misuse legal persons and arrangements to launder criminal proceeds.
- Norway has an extensive system of registers on legal ownership and control information, which assists in preventing misuse and obtaining beneficial ownership information. The Altinn system is an efficient way to input information, and the IT system seems generally efficient. Authorities have ready access to these systems; however they could be made more effective.
- There is considerable transparency as regards the above information, making much of it available to not only competent authorities but also reporting entities and the general public, which helps strengthen the system.
- Where ownership/control is entirely Norwegian, the basic requirements (control information in the national company register and ownership information held by companies) are readily available to competent authorities in many cases.
- Beneficial ownership information of Norwegian legal persons is not readily available where there are foreign legal persons or arrangements involved in the ownership/control structure.
- As in many countries the company registry system is passive and reactive, with little active monitoring and limited sanctions. This approach should be adjusted to introduce some form of more proactive monitoring, and stronger sanctions, which are implemented and used in practice.
- Trusts and other types of legal arrangements cannot be created under Norwegian law (thus likely reducing the money laundering / terrorist financing (ML/TF) risks of trusts in Norway given the fewer number). However, there appear to be trustees and/or beneficiaries of foreign trusts in Norway. Information available suggests that neither competent authorities nor reporting entities have timely access to beneficial ownership information on such trusts and other legal arrangements. Trustees of foreign trusts should be required to disclose this fact to reporting entities.

7.1 Background and Context

(a) Overview of legal persons

7.1. The types of legal persons that can be established or created in Norway are as follows:

- Companies – limited companies and public limited companies;
- Partnerships – general partnerships, general partnerships with shared liability, and limited partnerships;
- Societies – house building co-operatives, housing co-operatives and co-operative societies;
- Organisations – foundations, savings banks and associations.

7.2. The numbers of these legal persons for the period 2011-13 is as follows:

Table 7.1. Number of entities registered

Type of Entity	2011	2012	2013	% change 2011-13
Private Limited Company	219 977	235 174	250 367	+14%
Public Limited Company	312	279	253	-19%
Other limited liability company	7 157	5 252	2 556	-64%
Jointly Owned Shipping Company	391	360	333	-15%
European Company	5	5	4	-20%
General Partnership	17 411	16 772	16 045	-8%
Limited Partnership	674	661	633	-6%
Partnership with shared liability	21 020	20 743	20 127	-4%
Norwegian Branch of Foreign Business	30 268	29 049	27 785	-8%
Cooperative Society	945	2 330	4 164	+341%
Foundation	7 737	7 631	7 453	-4%

Source: data provided by Norway

7.3. Little information is available on the relative significance of each of the various types of legal persons either within the Norwegian economy generally or in the financial and DNFBP sectors. For example it is not known what types of legal persons comprise the companies/entities that are traded on the Oslo Stock Exchange, though many of them may be either public limited companies or shipping companies. It would appear that the private limited company is the most widely used type of legal person, probably because it can be owned and controlled by one person (at a minimum), has limited capital requirements, and the accounting, auditing and reporting obligations are also more limited than for some other types of entities.

7.4. As set out below, and in the Technical Compliance Annex, there is an extensive system of registers that provides the institutional framework for all the different types of legal persons, with a Central Coordinating Register that contains basic information on all types of legal persons. Once a legal person is created, with the appropriate fundamental documents it must be registered in one or more registers, which are maintained by the Bronnoysund Register Centre (BRC). The BRC is a government body under the Norwegian Ministry of Trade and Industry, and its primary function is to maintain and oversight a number of different national computerised registers. There are a significant number of registers that relate to legal persons such as the Central Coordinating Register for Legal Entities (1995), the Register of Business Enterprises (1988), the

Register of Company Accounts (1981), the Disqualified Directors Register (1991), and the Register of Non-Profit Organizations (2009). There are also other registers such as the Register of Mortgaged Moveable Property (1980), the Register of Bankruptcies (1993), and the National Fee Collection Office (1983). The BRC also administers which the internet portal that is used by Norwegians to input or obtain information on a range of issues related to the government – the Altinn system (www.altinn.no) (2003).

(b) Overview of legal arrangements

7.5. The Norwegian legal system does not provide for the creation of trusts or other legal arrangements, although foreign trusts or other legal arrangements are not prohibited from operating in Norway. Trusts and other legal arrangements formed overseas or governed by the laws of another country can and do operate through persons that are trustees, and who reside or otherwise act for the trust in Norway. As they cannot be established under Norwegian law, trusts and other legal arrangements are not registered or monitored in any way, and no information is available on the number or importance of such arrangements in Norway, whether they are used by Norwegian citizens or residents, or whether property in Norway is held pursuant to such arrangements.

(c) International context for legal persons and arrangements

7.6. Based on the information available, it appears that Norway is not an international centre for the creation or administration of legal persons or arrangements that are then used elsewhere. Trusts and other legal arrangements are not recognised in a general way under Norwegian law (only for anti-money laundering / counter-terrorist financing (AML/CFT) purposes), and the type, nature and number of legal persons created in Norway do not appear to be particularly designed for use in an international context, whether for tax or other purposes. There is no information available on the extent to which legal persons or arrangements that are created elsewhere hold assets in or are used in Norway. There are relatively few registered branches of foreign business enterprises, but the extent to which foreign companies, trusts etc. may hold assets directly or indirectly in Norway is unknown.

7.2 Technical Compliance (R.24, R.25)

7.7. The technical compliance with Recommendation (R.) 24 and 25 is intrinsically linked with the effectiveness of the measures assessed in Immediate Outcome (IO) 5 to prevent the misuse of legal persons and arrangements for ML/TF. In particular, under the technical methodology, countries should ensure that competent authorities have timely access to accurate and up-to-date beneficial ownership information. The measures that Norway has in place to address the technical criteria are fundamental for the assessment of effectiveness. For this reason, the majority of the assessment is contained in the assessment of IO.5 below.

Recommendation 24 – Transparency and beneficial ownership of legal persons

7.8. Norway is rated partially compliant (PC) with R.24. Norway has in place a series of measures to enhance the transparency of legal persons, primarily through a system of multiple public registries for different types of legal persons. All Norwegian legal persons, and Norwegian and foreign companies or other legal persons conducting business activities in Norway are obligated to register, and the various registers are maintained by the Bronnoysund Register Centre (BRC). Norway also requires all public limited liabity companies (PLLCs) and limited liability companies (LLCs) to maintain a register of shareholders which must be made available to any person on request. Other sources of basic and beneficial ownership information include information provided to the Tax Authority and information held in the register of company accounts. As a result of these measures, significant beneficial ownership information is available when only Norwegian companies are involved. However, where foreign companies are involved, for example by owning shares in Norwegian companies, beneficial ownership information is not contained in the various public registers. These measures are described and analysed in further detail below.

7.9. Norway requires all Norwegian PLLCs and LLCs to establish and maintain a register of all shareholders that must be made available to any person upon request. Companies must maintain the basic information on

legal ownership. Companies are required to keep this up-to-date, and although there are no direct sanctions, the shareholder can only exercise his rights when changes in ownership have been recorded.

7.10. Competent authorities also have access to the information that companies provide to the tax authority and publicly available in the register of company accounts. PLLCs and large LLCs must provide annual in its accounts to the tax authority which includes information on the 20 largest shareholders in the company. For small LLCs, the annual accounts submitted to the tax authority must contain information on the 10 largest shareholders in the company. However, this does not include beneficial ownership information as shareholders can be legal persons. This is not kept up-to-date as it is provided annually.

7.11. As a result of these measures, significant beneficial ownership information is available when only Norwegian companies are involved. However, where foreign companies are involved, for example by owning shares in Norwegian companies, beneficial ownership information is not contained in the various public registers. If the Norwegian authorities seek information about the foreign company's chain of ownership, they would have to ask the foreign company for that information, or check the business register of the home country. As a result, beneficial ownership information Norwegian companies owned by foreign companies, is not available to competent authorities in a timely manner.

7.12. In Norway, other legal persons that can be created include partnerships, cooperative societies, foundations and associations. Similar measures to those in place for PLLCs and LLCs apply to these other legal persons including registration requirements and reporting to the tax authority.

Recommendation 25 – Transparency and beneficial ownership of legal arrangements

7.13. Norway is rated PC with R.25. As noted above, even though trusts cannot be created under Norwegian law, foreign trusts are not prohibited and can be operated by trustees residing in Norway. There are no obligations (or associated sanctions) on trustees of foreign trusts to disclose their status to reporting entities, or to give authorities access to information held by them in relation to the trust (due to the fact that trusts are not recognised in Norwegian law). Reporting entities are required to identify any persons acting on behalf of a customer and explicitly ask customers whether they are "acting" for someone else (see R.10 and 22 above). Therefore the normal customer due diligence (CDD) requirements could help ensure that trustees disclose their status to reporting entities. However, no obligations are placed on the trustee.

7.3 Effectiveness: Immediate Outcome 5 (Legal Persons and Arrangements)

Risk and Transparency – legal persons and arrangements

7.14. Norway has not assessed the ML/TF risks associated with the different types of legal persons that can be created in Norway, although there is recognition that such risks do exist. Similarly, there has been no assessment of the risks that may exist in relation to trusts or other legal arrangements that are governed by the laws of other countries but where the trustee resides in Norway. The NRA makes reference to the difficulties of determining the beneficial ownership of legal persons, the vulnerabilities in this area and the fact that there are significant risks, but does not go on to consider the different threats posed by different types of legal persons or arrangements.

7.15. However, an examination of the information available regarding the numbers of different types of legal persons that have been created in Norway, and the trends, does allow some preliminary conclusions to be drawn. As can be noted in Table 7.1, private limited companies are by far the commonly used type of legal person, and the number of such companies is continuing to steadily increase. It seems likely that this type of legal person is more at risk in terms of misuse for AML/CFT purposes than many of the other types of legal persons. For example, there are only a small and decreasing number of public limited companies. The other type of legal person for which there may be some potential risks are foundations, given that they can be used both for charitable and commercial purposes, and that the nature of a foundation is that there is no ownership, only a purpose for which the foundation is created. On the one hand foundations have certain

attributes that are closer to trusts than companies, but on the other they have legal personality, and are registered and supervised like companies.

7.16. There is an extensive system of registers in Norway containing information on legal ownership and control, which has the potential to help prevent misuse and to obtain beneficial ownership information. Information in these registers is input efficiently through Altinn. The IT system for accessing and using the data seems to be efficient, with authorities having ready access to the systems and the different types of information that is recorded. The ability to access reliable information on legal persons is also facilitated by the population registers, which have information on the identity of all Norwegian citizens and permanent residents. Norway also has considerable transparency as regards information that is recorded by the government, making much of it available not only to competent authorities but also to reporting entities and the general public. Indeed this transparency principle extends as far as allowing the public to obtain information from the tax authorities on taxpayer's income or wealth, which shows a degree of transparency beyond that in most other countries.

7.17. As regards making information available on the different types of legal persons, the Bronnoysund Register Centre (BRC) provides a guide on the Altinn website on how to start a business in Norway, which includes an overview of the types of legal persons that can be created in Norway, their basic features and the creation/registration procedures. The guide also provides information and advice on choosing the appropriate type of entity and the forms that need to be completed, but does not indicate how basic and beneficial ownership information can be obtained. The information is available in Norwegian, with a lot of information also in English.

Legal persons – basic and beneficial ownership

7.18. A core element of IO.5 is the degree to which competent authorities can obtain timely access to basic and beneficial ownership information relating to legal persons created in Norway. The degree of effectiveness of the system is closely linked to the level of technical compliance.

Basic information

7.19. The various registers maintained by the BRC (principally the Central Co-ordinating Register and the Business Register) cover most types of legal persons (except a limited set of societies and organisations). In addition the Foundations Register records relevant information on foundations. The registers contain most of the basic information relating to a legal person e.g., name, status, address, basic powers and list of persons in control (for example directors of companies). Corporate directors are not permitted in Norway, and the general manager and at least half the members of the board of directors of a private company must reside in Norway or be a citizen and resident of an European Economic Area (EEA) state. Therefore, although it will be possible in many cases for authorities to find a natural person in Norway that is in control of the company and who can be questioned about the company, this will not be the case if the directors or manager reside in an EEA state. A similar situation exists for foundations. Norway advises that this is a requirement of the EEA agreement, and that the names and address of such persons is recorded. However this is not equivalent to the authorities having immediate access to a natural person they can question.

7.20. As regards shareholding information, private limited companies maintain a shareholders register, which includes identifying details of both individual and corporate shareholders, while public limited companies maintain a register of shareholders in an independent security register. Similar types of information on ownership and control are available for other types of legal persons such as foundations, partnerships and cooperative societies. All of the above information is publicly available and the law requires that it is kept up-to-date.

7.21. In addition to the information contained in the registers noted above there are two other registers that contain information that is relevant to ownership and control: the Register of Company Accounts and the Corporate Taxation Data Register. In both registers the information is a once a year snapshot of information that is correct at the date of filing. All Norwegian companies are obliged to submit their audited annual accounts

to the Register of Company Accounts within one month of being adopted at the AGM, and the accounts must be accompanied by a list of the 10 largest shareholders for most private companies (20 largest for public companies or large private companies). The board of directors is responsible for the accuracy of the annual accounts. The tax register contains, inter alia, information identifying all shareholders of Norwegian legal persons who are obligated to pay tax in Norway, and is updated annually. The above information is held by the tax authorities and is accessible by the FIU if an STR has been filed on the company or if law enforcement has reasonable grounds to suspect that a crime with a penalty of more than six months imprisonment has been committed.

7.22. There are no requirements for, or mechanisms that are used to verify or check that information that is entered or recorded is accurate. There are limited sanctions for non-compliance or for filing incorrect information, and little if any action is taken in practice to monitor or sanction either legal persons or individuals for non-compliance. Cases of non-compliance are occasionally observed due to other authorities drawing this to the attention of the BRC. The system is a reactive one overall, designed to record and store information that is provided to it. It is therefore not known to what degree the information recorded in the registers is up to date or accurate in practice. Similarly no information is available on whether changes in shareholding of private limited companies is kept up to date or is checked in any way by companies. Despite this, the authorities noted that the information held by BRC is very useful.

Beneficial ownership information

7.23. The position in Norway regarding information on the ultimate beneficial owner and whether that information can be accessed in a timely manner depends significantly on whether there are foreign ownership elements involved. There are no bearer shares or share warrants, and in relation to nominees, there is a system to deal with formal nominee shareholdings, although not more informal nominee arrangements.

7.24. The various registers maintained by the BRC contain a significant amount of information relating to beneficial ownership of companies which is publicly available. The Central Coordinating Register for Legal Entities (CCR) includes information on persons exercising control over the company including the board of directors, the general manager and the person who has the power to sign documents on behalf of the company. For the natural persons identified in these roles, the register includes the personal identity number of Norwegians, or a D-number for foreigners, and identities are cross-checked against the National Population Registry. This cross-checking is an important mechanism to prevent the provision of fictional names. Similar requirements exist for foundations and other types of legal persons.

7.25. If tracing beneficial ownership through company shareholding, then information on shareholding as at the once a year date of those returns can be obtained by law enforcement from the Register of Company Accounts or the tax register, provided that the necessary conditions noted above are met. The information from the Register of Company Accounts is publicly available. These databases provide immediate access to a snapshot in time on shareholding, though the information would not be up-to-date. In addition, every company is required to maintain an up-to-date register of its own shareholders, and public companies must do so on a securities register, which is thus more readily accessible. For private companies, competent authorities (as well as the general public) would have to go to the office of the company at which the shareholder is kept. If there were a chain of companies would make obtaining beneficial ownership information a slower process.

7.26. Law enforcement and other competent authorities can obtain a lot of information from the various registers online. A lot of information is also obtained by authorities using a web interface called Web Services that allows them to access information on legal persons using their own IT systems. It is limited to seeking information on one legal person at a time, and cannot search across the whole database against specific fields such as director's name or an address. However, authorities are able to request BRC to make such searches and this can be done swiftly. Moreover there are also private business websites (e.g., www.purehelp.no) which aggregate a range of information on both natural and legal persons, drawn from the registers, the annual accounts that are filed etc. These include information on ownership and control of legal persons, on their financial returns, and also make linkages between companies, and between individuals. The information is public and free, and is a helpful starting point both for authorities and for reporting entities.

7.27. The net result, which was confirmed by law enforcement and other authorities in Norway, is means that where Norwegian companies with Norwegian ownership are involved, the authorities advised that they are able in a large majority of cases to follow the chain of ownership to a natural person, whose identity has been in the population register. This can be done in a timely manner using the various registers and other information sources. In theory the position is more difficult for commercial foundations, since they do not have "owners". However, law enforcement authorities did not indicate that they have had problems in relation to foundations. Competent authorities also indicated that they were generally able to locate the directors of companies or other persons that manage or control Norwegian legal persons.

7.28. However, where foreign legal persons or arrangements are involved, by owning shares in Norwegian companies, beneficial ownership information is not contained in the various public registers. This also applies to the information collected and maintained by companies in their shareholder registry, which relates to legal ownership. In such cases, the public registers and the register of shareholders reflect only the name, registration number and address of the foreign company. If the Norwegian authorities seek information about a foreign entity's chain of ownership, they either have to ask the foreign entity for that information, or check the business or other registers in the entity's home country. However, the accessibility, reliability and completeness of information on the foreign legal person depends on the information the home state requires the entity to register about its owners or controllers and on the information that is available publicly from the company or other registry, or is otherwise obtainable e.g., through international cooperation.

7.29. In practice, although there had been cases where the competent authorities had been able to trace the beneficial owner, the general view was that beneficial ownership information on Norwegian companies or legal persons that involve ownership by foreign entities, is often difficult to obtain, and not available to competent authorities in a timely manner.

Monitoring and Sanctions

7.30. As in many other jurisdictions, the system of company and related registers is a passive one that is designed to be an efficient in terms of receiving information, and making that information available. The authorities in charge of the registers indicated that the documents and information that is input is not checked, and that, although there are some limited safeguards, there is no systematic or proactive monitoring of whether companies and other types of legal persons are complying with their obligations. Failures to comply with the various requirements can result in administrative fines, which increase over time. However, the maximum weekly fine is still only NOK 1 500 (EUR 195). It is also theoretically possible to bring criminal proceedings that could result in up to a year's imprisonment and/or dissolution of the company. However these sanctions are very rarely applied in practice according to the authorities, and only when serious cases are drawn to their attention by third parties. The lack of checking, monitoring and sanctioning undermines to some degree the completeness and reliability of the information that is recorded.

International Cooperation

7.31. Norway is able to provide international cooperation through the mechanisms described in Chapter 8, including for information relating to legal persons. As noted above, information relating to the ownership of Norwegian legal persons that is held on the registries is publicly available or available to the public on request. The information held by the Business Register is available in English through either the BRC website, or by contacting the BRC. The FIU provides assistance to foreign counterpart with information on Norwegian legal persons. In addition, the FIU takes the proactive step to provide these foreign counterparts with information on how to access the Norwegian registries directly, and the relevant links (both the BRC website and the private service providers). This practice allows the foreign counterpart to access the information directly which enhances the effectiveness of the cooperation with respect to Norwegian legal persons.

Legal Arrangements

7.32. Norwegian law does not provide for the creation of trusts or other types of legal arrangements, nor does it recognise (other than in relation to AML/CFT issues) that such legal arrangements have any legal status or validity. Norwegian law does not prohibit persons from acting as trustees of trusts governed by a foreign law, or from being beneficiaries of such trusts, and property located in Norway could be trust property pursuant to a governing foreign law. As noted in relation to R.10, reporting entities are required to obtain and record information about trustees, settlors and certain beneficiaries, however there is no legal obligation on a trustee to declare this fact (as opposed to the obligation on reporting entities), and reporting entities did observe that it is often difficult to know whether a person is acting in the capacity of a trustee.

7.33. There is no information on the degree to which trusts or other legal arrangements are misused as vehicles for ML/TF purposes. However some cases were provided in which persons had laundered the proceeds of offences committed in Norway using trusts as one of the mechanisms to conceal the proceeds of their offences. It appears that criminals would most often seek the assistance of professionals such as lawyers to create and use trusts, and that issues of professional secrecy could then complicate or delay the ability of competent authorities to obtain timely access to information on the beneficial owners behind the trust. In all the circumstances, it appears that competent authorities do not have timely access to beneficial ownership information on trusts.

Conclusions on IO.5

7.34. While Norway has not comprehensively assessed the ML/TF risks associated with legal persons, the information available indicates that there is a real risk that legal persons are misused to launder criminal proceeds. Norway has an extensive system of registers on legal ownership and control, which assist in preventing misuse and obtaining beneficial ownership information. Competent authorities are able to access significant beneficial ownership information in a timely manner when only Norwegian entities are involved, as they can follow the chain of ownership to a natural person through the various registers; this is a positive aspect of Norway's framework. However, where foreign companies are involved, for example by owning shares in Norwegian companies, beneficial ownership information is not contained in the various registers, and is not available in a timely manner. This is an important gap which makes Norwegian companies vulnerable to misuse. While there have been cases where the competent authorities had been able to trace the beneficial owner of a foreign company, this is not common, and this was cited by authorities as an area of difficulty. Finally, while legal arrangements cannot be created under Norwegian law, cases were provided in which the proceeds of crimes committed in Norway were laundered using trusts. There is no information on the degree to which trusts are being misused and competent authorities do not have timely access to beneficial ownership information for such trusts.

7.35. Norway has a **moderate level of effectiveness** for IO.5.

7.4 Recommendations on Legal Persons and Arrangements

a. Norway should assess the risks relating to the misuse of legal persons and arrangements (domestic and foreign) for ML/TF purposes in Norway.

b. Given the extensive system of registers in Norway, Norway should ensure that the information on legal shareholders of private limited companies that is entered by such companies into the Register of Company Accounts and the Corporate Taxation Data Register is up-to-date and accurate, for example, by requiring it to be updated more frequently than once a year, or by ensuring that the authorities have online access to the company shareholder register.

c. Companies should be required to record and maintain an up-to-date and accurate register of their beneficial owner(s). This information should be accessible online by the BRC and competent authorities. Alternatively, beneficial owners could be recorded in the BRC registers, or another comparable system created that allows timely access by authorities to

adequate, accurate and up-to-date beneficial ownership information.

d. At least one director or senior managing official should be required to be resident in Norway.

e. Norway should enhance the system for monitoring and enforcing company law requirements, through inspections and/or automatic monitoring.

f. Sanctions for failure to comply should be reviewed to determine whether more serious sanctions should be applicable in appropriate cases.

g. Obligations (and associated sanctions) should be imposed on trustees of foreign trusts to disclose their status to reporting entities, and to give authorities access to information held by them in relation to the trust.

7

8. INTERNATIONAL COOPERATION

Key Findings

- The system in place for mutual legal assistance between Nordic and European Union (EU) countries is straightforward and dealt with directly between the competent judicial authorities in accordance with the Nordic Agreement and the EU 2000 Convention. In addition, Nordic arrest warrants are forwarded directly between the competent judicial authorities in accordance with the Convention on the Nordic Arrest Warrant.
- International cooperation between Norway and its Nordic partners is very close, uncomplicated and dealt with quite speedily. In addition, formal cooperation between Norway, European Economic Area (EEA) and non-EEA countries is working well. The legal framework for mutual legal assistance and extradition is generally broad. The only deficiencies relate to enforcement of non-conviction based confiscation orders and the requirement to start domestic proceedings rather than enforce a foreign order.
- With respect to other forms of cooperation, the financial intelligence units (FIU), law enforcement agencies (LEAs) and the Customs Authority are well engaged in international cooperation with their counterparts, both upon request and spontaneously.
- The Norwegian police are very involved in cooperation with Nordic and EU countries to strengthen and improve the fight against international crime, including for money laundering (ML), associated predicate offences and terrorist financing (TF). However, they have noted that the potential for them to obtain information from abroad has not been fully exploited.
- There is a sound legal framework in place to allow the FSA to exchange information with foreign counterparts in the financial sector, but so far the FSA's international information exchange has not focused on AML/CFT matters, nor has it been extended to non-financial sector anti-money laundering / counter-terrorist financing (AML/CFT) counterparts.
- Norway does not maintain comprehensive statistics on mutual legal assistance and extradition which makes it difficult to assess the effectiveness of their international cooperation, and the assessment team has had to rely on qualitative information in this regard. It is noted that the Norwegian authorities did not follow up on any of the specific recommendations included in the 2005 Mutual Evaluation Report regarding this kind of statistics, namely that Norway should keep statistics concerning: (i) the number of requests; (ii) the nature of requests; (iii) whether requests were granted or refused; (iv) what crime the requests were related to; and (v) how much time was required to respond to the requests

8.1 Background and Context

8.1. Norway's closest partners regarding both formal and informal international cooperation are the Nordic and EU countries. The legal framework for mutual legal assistance and extradition is generally broad as outlined below. The MoJ is the designated central authority for mutual legal assistance and extradition pursuant to a number of conventions, including, the European Convention on Mutual Assistance in Criminal Matters, 1959; the UN Convention against Transnational Organized Crime, 2000; the UN Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances, 1988 and the UN Convention Against Corruption, 2003. However a lot of the cooperation with Nordic/EU/Schengen countries takes place directly between prosecutors.

8.2 Technical Compliance (R.36-40)

Recommendation 36 – International instruments

8.2. Norway is rated compliant (C) with Recommendation (R.) 36. Norway has signed and ratified the Vienna, Palermo, Terrorist Financing and Merida Conventions, and has implemented those Conventions as required under the FATF Standards. Norway has also signed and ratified the Council of Europe (Strasbourg) Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime 1990, but not the more recent Warsaw Convention 2005.

Recommendation 37 – Mutual legal assistance

8.3. Norway is rated largely compliant (LC) with R.37. The legal basis for Norway's mutual legal assistance regime is found in laws such as the *Extradition Act* (*EA*), the *Courts of Justice Act*, and the *Regulations relating to International Cooperation in Criminal Matters 2012* (*Regulations on International Cooperation*). Other laws such as the *CPA* may be used in response to foreign requests to the same extent and on the same basis as in domestic cases, and apply fully to ML, associated predicate offences and TF. Assistance can be provided irrespective of whether there is a treaty. However, if assistance through coercive measures are sought then dual criminality applies (unless it is a Nordic country). Dual criminality is based on whether the conduct underlying the offence is criminalised in Norway and the requesting country. The legal powers are broad, do not contain any unreasonable restrictive conditions, and appear sufficient to respond to almost all foreign requests (see also R.38). The Ministry of Justice (MoJ) is the designated central authority for mutual legal assistance, though requests can also be sent directly between judicial and law enforcement authorities in Nordic and European Union countries. The MoJ monitors requests in the case management system, *Websak*. However, this does not include requests made directly from or to other authorities. Although there are no specific confidentiality requirements relating to mutual legal assistance requests, all concerned authorities have confidentiality requirements under their own internal or national security protocols.

Recommendation 38 – Mutual legal assistance: freezing and confiscation

8.4. Norway is rated LC with R.38. Norway does not have specific legal requirements concerning the enforcement of foreign freezing, seizing or confiscation orders but relies on domestic powers such as those in the *CPA*. Where a foreign state is a signatory to the Vienna, Strasbourg or Merida Conventions, and seeks assistance under those conventions, then Norway can recognise and enforce the foreign order directly. However, if that is not the case then Norway cannot give effect to the foreign order directly but must start its own proceedings. This applies to all property that is the proceeds of or an instrumentality of ML, predicate offences and TF. Norway's laws do not refer to the enforcement of foreign non-conviction based (NCB) confiscation orders, and domestically, the requirement to use the criminal standard of proof under s.34 would mean that NCB orders could not be enforced. As regards other measures in place, it is possible to share assets with other countries, but there is no mechanism for managing property that has been seized or confiscated.

Recommendation 39 – Extradition

8.5. Norway is rated LC with R.39. Any person who is charged, accused or sentenced by a foreign state for a punishable act may be extradited in accordance with the *EA*. Both ML and TF are extraditable offences. Extradition with other Nordic countries is governed by the *Convention on the Nordic Arrest Warrant* which entered into force on 16 October 2012. Extradition to all other countries is regulated in the *EA*, and may only take place if there is dual criminality and the offence is punishable under Norwegian law with imprisonment for more than one year. A difference in the classification or denomination of the offence does not affect the dual criminality principle. There are clear procedures for timely execution of extradition requests, and judicial authorities have case management systems in place to track extradition requests. However, this does not include requests made directly from or to other authorities.

8.6. Norway does not extradite its nationals to non-Nordic countries. When extradition is refused because the person in question is a Norwegian national, proceedings can be brought in Norway. Simplified procedures for extradition are in place with other states parties to the *Schengen Convention*, such as direct transmission of extradition requests between the appropriate ministries. There are also simplified procedures to extradite consenting persons for both Nordic and non-Nordic countries.

Recommendation 40 – Other forms of international cooperation

8.7. Norway is rated LC with R.40. Norwegian legislation allows for a wide range of information exchange with foreign authorities for preventing and detecting criminal acts. There is no legal impediment for information to be exchanged both spontaneously and upon request. The FSA is able to provide assistance to foreign supervisory counterparts without the need of a Memorandum of Understanding (MOU). The FIU has a sound legal basis for the exchange of information with its foreign counterparts and has mechanisms for cooperation and responds adequately to requests. Where possible, information is sent and received via the Egmont Secure Web. Norwegian LEAs have appropriate powers and mechanisms to cooperate with foreign competent authorities, especially the Nordic countries and countries in the EEA. Finally, customs authorities do not have secure gateways for the transmission and execution of requests.

8.3 Effectiveness: Immediate Outcome 2 (International Cooperation)

8.8. The lack of detailed risk information regarding transnational aspects of ML presents a challenge to effective implementation. While the National Risk Assessment (NRA) has only general information regarding transnational risks, the National Criminal Investigation Service (KRIPOS) and National Authority for Investigation and Prosecution of Economic and Environmental Crime (ØKOKRIM) threat assessments include some information regarding risks from Nordic countries, EU countries and other countries and regions including organised crime risks from the Baltic region and West Africa.

Mutual legal assistance and Extradition

8.9. Nordic and EU-countries are Norway's most important partners in international cooperation, especially in relation to mutual legal assistance and extradition. Mutual legal assistance requests between Norway and Nordic and EU/Schengen-countries are mostly sent directly between the judicial authorities in accordance with the Nordic agreement and the EU 2000-Convention. This provides for simplified and less time consuming procedures with requests and responses sent directly from prosecutor to prosecutor. The only negative aspect that the assessment team identified is that these requests are not centrally registered and no comprehensive statistics are available which could assist in the assessment of effectiveness. Importantly, Norway does not keep statistics on the crime type of mutual legal assistance and extradition matters and it is therefore the number of matters relating to ML/TF cannot be determined. However, feedback received from other Nordic countries indicates that, in general, this direct exchange of information works well and it is rapid and uncomplicated. This statement is particularly true for cooperation with prosecutors and LEAs in the Oslo police district.

8.10. The MoJ is the designated central authority pursuant to a number of EU and UN Conventions on which Norway heavily relies for providing and requesting mutual legal assistance. In addition, Norway has two formal bi-lateral mutual legal assistance treaties. For countries where there is no formal agreement, Norway follows the provisions in Chapter 5 of the EA which state that such requests shall be complied with wherever possible. In practice, assistance not based on formal agreements is generally provided. Norwegian authorities indicated that the lack of bilateral agreements is seldom an impediment for successful cooperation and it takes a very flexible approach when providing assistance to countries which are not a party to the Conventions or a bilateral treaty. Norway has an open and constructive approach in providing mutual legal assistance which enhances its effectiveness. This was confirmed by the feedback received from 18 countries. The majority of the countries which responded did not present any information which stated that they have encountered problems with cooperation with Norway[1].

8.11. Norway has taken action to ensure that mutual legal assistance is provided in a timely manner and the *Regulations on International Cooperation in Criminal Matters* referred to above guide both the central and regional authorities on how to deal with requests, including prioritisation of requests, follow-up on on-going requests, and the timing of responses. These are supplemented by the circular letter on International Cooperation in Criminal Matters issued by the MoJ. In addition, to ensure the prioritisation of the requests it receives, the MoJ has introduced a routine whereby the MoJ sends a reminder of the request to the competent Norwegian authority after three months. While no official statistics are available with regard to the time it has taken Norway to respond to mutual legal assistance requests, the authorities indicated that even the more complicated requests were fully satisfied within 12-18 months (at most). Norway has specific procedures in place to deal with urgent requests and it is common practice that these are submitted via INTERPOL channels and confirmed via formal channels shortly afterwards.

8.12. Norway has also shown that it is actively engaged in seeking mutual legal assistance. An increasing number of larger and more complex cases have international ramifications and proceeds and/or evidence are often not present in Norway. Norway has provided examples of economic crimes where assistance has been successfully sought, both on evidence gathering and on asset tracing and freezing.

Box 8.1. International cooperation: the *Gruben case*

The *Gruben case* the laundering in Norway of proceeds which were generated from tax offences committed abroad. Large cash exchanges from NOK to Euro were conducted in various banks and exchange offices in the Oslo-area by people linked to the defendant and were reported as suspicious transactions to the FIU. ØKOKRIM was responsible for this investigation and identified some ML aspects in Norway, including through STRs received by the FIU, evidence on international financial transactions. The predicate offence could only be identified through international assistance as the proceeds were derived from investments abroad. This led ØKOKRIM to undertake significant engagement with other countries through informal contact and formal mutual legal assistance requests to determine the source of the funds. The mutual legal assistance received from other countries led to a successful ML conviction relating to the proceeds of tax evasion, estimated to NOK 17 million (EUR 2.2 million) (as at the time of the on-site visit the case was on appeal). The defendant was sentenced for ML to 3 years and 6 months in prison.

1 Armenia; Austria; Australia; Belgium, Canada; France; Greece; Hong Kong, China; Ireland; Isle of Man, UK; Japan; Macao, China; Mexico; Russia; San Marino; Slovenia; Sweden; and United States.

8.13. In order to support and strengthen coordination in serious cross-border crime, Norway has entered into an agreement with Eurojust. In accordance with the agreement, Norway has seconded a Liaison Prosecutor to Eurojust. Eurojust has proved to be a valuable counterpart and facilitator when dealing with mutual legal assistance. ØKOKRIM has several investigations where Eurojust has been of assistance. In this context, joint investigation teams appear to help and have had a positive impact on the effectiveness of Norway's international cooperation.

8.14. As explained above, simplified procedures for extradition are in place for states which are parties to the *Schengen Convention* and for Nordic Arrest Warrants. The Nordic system of arrest warrants has been inspired and influenced by the development of the European Arrest Warrant scheme. Under each of the regimes, there are strict time limits for decisions regarding extradition and few grounds for refusal. Norway has signed three bilateral treaties in respect of extradition. However, according to the Extradition Act, extradition may take place irrespective of the existence of an extradition treaty between the parties. It has not been shown that Norway's lack of bilateral treaties has been an impediment to cooperation in this area. Also, as with mutual legal assistance, the quality and assistance provided by Norway in the context of extradition appears to be good. Information supporting this statement was received from international partners, especially the Nordic partners. The circular letter cited above deals with extradition requests, including on prioritisation of requests and timeliness in responding. It normally takes from six months to one year to decide on and execute an extradition request; this depends on the complexity of the case and how often the decisions of the courts and the MoJ are appealed. During the on-site the team was advised that the longest time that Norway had taken to execute an extradition request was three years. However, simplified extradition procedures normally only take two to three months.

8.15. ML and TF are extraditable offences. Norway does not extradite its nationals to non-Nordic countries. However, when extradition is refused on this basis, the case can be dealt with in Norway. There are no statistics to rely on how often this has already happened. In practice, the Norwegian Interpol and Sirene office informs the state that has issued an alert, at an early stage, that Norwegian nationals will not be extradited. Consequently, there are not many such requests for extradition. However, Norwegian nationals have been prosecuted in Norway for offences committed abroad because of the lack of possibility to extradite. Usually the requesting state has to ask the Norwegian authorities to prosecute the matter.

Other forms of international cooperation

8.16. With the exception of the FSA, most of Norway's competent authorities are well engaged in international cooperation with foreign counterparts. Norway's FIU is actively involved in direct and indirect information exchange, especially on behalf of domestic LEAs, and promotes this tool when coordinating and cooperating with other domestic authorities. In addition, Norway's competent authorities provide very little feedback to their international counterparts regarding the usefulness of the information provided and that the value the information received has added to the domestic processes.

8.17. Norway's FIU is well engaged in information exchange with its foreign counterparts as part of its analytical process. Collecting information from foreign counterparts is one of many sources of information the FIU uses (see R.29 and IO.6 above). The FIU also responds to requests from foreign FIUs and it uses all of the information sources available to it. Overall, positive feedback was received from the FIU's foreign counterparts regarding the nature and level of cooperation provided.

8.18. The FIU has assigned the information exchange with foreign partners to one of its analysts. Centralising requests received ensures that the FIU responds to foreign requests within a reasonable amount of time (maximum one month) and gives priority to urgent requests which are answered within the timeline sought by the foreign partner. In addition, specific expertise in dealing with requests from foreign FIUs is developed. While the FIU is also engaged in spontaneous information exchange, the majority of requests sent and received can be categorised as upon request. Information exchange with foreign FIUs takes place via the Egmont Secure Web which provides a secure gateway. The FIU also keeps comprehensive statistics regarding its information exchange, including regarding timing of responses, which provide a good basis for the assessment of effectiveness. In addition to quantitative information, the FIU was able to present

the assessment team with several case examples which lead to the conclusion that the FIU has been and is successful in requesting and providing information from/to foreign counterparts.

8.19. The FIU plays an important role in facilitating indirect information exchange between competent authorities. It reaches out on behalf of LEAs, especially other teams within ØKOKRIM and PST. The FIU provided the team with the necessary assurances that foreign counterparts are always aware when a request is formulated on behalf of a LEA. The FIU also provided several case examples to show how indirect information exchange is used as an important source of information for LEAs. One of these examples relates to the Anders Behring Breivik case and the information provided demonstrates that the Egmont cooperation was a very useful tool for receiving information from other countries in a swift, safe and efficient way. Several foreign FIUs were approached and this resulted in the collection of very useful information concerning Breivik's financial activities in other countries. At least seven of those answers proved to be so useful that the police immediately engaged in formal mutual legal assistance with the countries concerned for use of the information as evidence in the criminal case.

8.20. The Norwegian FIU does not require an MOU in order to cooperate with foreign FIUs. Therefore, the FIU does not actively seek to sign MOUs. It does, however, recognise that other FIUs may need to have an MOU in place for the exchange of information and tries to comply with the needs of other FIUs in this regard. The FIU has signed 10 MOUs with foreign FIUs.

8.21. KRIPOS plays a central role in international police cooperation, and has an important responsibility with regard to coordination of information with various foreign LEAs and relevant arenas of police cooperation, such as INTERPOL. KRIPOS is also Norway's central point of contact for foreign LEAs, and provided the assessment team with feedback indicating that, overall, the local police districts and the various teams within ØKOKRIM take a positive approach when providing necessary assistance to foreign police. Some supporting case examples have been provided in relation to ML/TF and associated predicate offences. However, there are some examples where lack of resources at the local level and/or different priorities may have hindered the provision of full support needed by foreign authorities.

8.22. The ML Unit at ØKOKRIM provided the assessment team with several examples indicating how international cooperation has been both effective and efficient, both from the requesting and providing side. Some of these cases have also involved the repatriation of confiscated assets/sharing of assets with other jurisdictions (see Box 3.5 & 8.1). International assistance can be provided quickly and money can be seized relatively easily but the formal procedures that need to follow take much more time to complete. While international information exchange by ØKOKRIM is intensive, this is not necessarily reflected in statistics, especially not when it involves exchange of information with neighbouring countries. However, based on the different material and information that has been provided it appears that there is a high level of international cooperation and related expertise shown by ØKOKRIM's ML Unit.

8.23. The PST is extensively engaged in international information exchange. It cooperates both bilaterally and multilaterally with police and security authorities in a number of countries. Cooperation with other intelligence services is based on regular meetings with PST's main counterparts, and also on more thematic and case based meetings with other counterparts in different countries.

8.24. The PST is also a member of a European security partnership, the Club of Bern. In order to strengthen its efforts against Islamist terrorist activities, in 2001 the club of Bern established a separate co-operation forum called the Counter Terrorist Group, in which PST participates. PST also represents Norway in NATOs Special Committee and in the Police Working Group on Terrorism and is in liaison with foreign police authorities through Norwegian membership of Interpol, Europol and Eurojust.

8.25. Operational cooperation takes place on a daily basis, including in relation to general operational intelligence and law enforcement investigations. The exchange of information appears to be fast and efficient, and there are routines on how quickly the requests shall be replied to. The PST provided information on several cases to illustrate its successful engagement in international cooperation.

8.26. One of the cases was a covert operation carried out from 2007. This was an investigation of an extreme Islamist network operating in Norway and providing financial and logistic support to Al-Shabaab. It involved

the cooperation of and parallel investigation carried out by three FATF member countries. As a result of a coordinated operation, two persons were arrested in Sweden at the same time as the arrest of the Norwegian suspects. In another matter, PST arrested three individuals on 8 July 2010, charged with conspiracy to commit a terrorist act. The investigation lasted for more than 3 years. There was broad cooperation with other law enforcement agencies. During the investigation PST carried out interrogations in 5 different countries. In court (in Oslo), the prosecution had witnesses from these other countries. Two persons were found guilty of entering into terrorist conspiracies and received 8 years and 3 years prison sentences. Another was found guilty of contributing to making explosives which were to be used in a criminal act and was sentenced to 120 days of imprisonment.

8.27. Norwegian Customs and Excise participate in different international operations regarding detection of cash smuggling. Participation in these operations focusses on sharing of information with domestic LEAs and internationally with foreign customs authorities. Norwegian customs authorities appear to have good experience in sharing of information with other customs authorities about persons declaring cash leaving Norway in order to detect if cash is declared entering into the indicated destination country. Norway provided the assessment team with several case examples, especially the Athena and Atlas cash smuggling operations, which led to successful seizures of cash both in Norway and abroad.

8.28. On the basis of the EEA-agreement therefore there are no barriers to exchange information for regulatory purposes between Norway and other EEA countries. Based on a Nordic MoU there is formalised contact between the FSA and other Nordic financial supervisory authorities, such as annual meetings, regular sector specific meetings and expert meetings but there are no examples of discussions on AML/CFT supervision at any of these meetings.

8.29. The FSA also has bilateral MoUs with counterparts in some European countries, India, US and Russia. In addition, the FSA has a multilateral Cooperation and Coordination Agreement on the prudential supervision of a large Nordic financial group. None of these are directed at AML/CFT supervision and Norway has been unable to provide information on how these channels have been used for AML/CFT supervision. In addition to the limited formalised international work, cooperation takes place on an ad hoc basis though this is not usually initiated by Norway. For example, subsequent to a request from the Swedish FSA to develop a standard procedure for AML supervision of a major Nordic bank (still under development), the FSA carried out an inspection in that bank focusing on beneficial ownership and the origin of customers' assets. The result was presented for Nordic supervisory authorities in 2012.

8.30. In 2011, the FSA in coordination with supervisory authorities from Sweden and Denmark contacted the relevant supervisory authority in Ireland with the purpose of initiating cooperation over the supervision of agents of a payment service provider authorised in Ireland and operating in the Nordic countries. However, no formalized cooperation was established and no inspections of agents have been carried out in Norway. This attempt did fail, however, and the FSA has not followed through in relation to entering into cooperation with the home supervisor (See IO.4 above).

8.31. In the context of international cooperation, outside of formal EEA structures and ad hoc exchanges, Norway was able to provide very limited information on how it sought or provided exchange of information to foreign supervisory counterparts for AML/CFT purposes. With the exception of the single outreach to the home supervisor of the MVTS provider, the FSA has not engaged in any AML/CFT specific exchange of information.

Conclusion on IO.2

8.32. Norway's system for international cooperation demonstrates many of the features of an effective system. The lack of statistics relating to international cooperation makes it difficult to assess, but based on qualitative information it is clear that Norway takes an open and collaborative approach to international cooperation. The method of international cooperation varies due to the level of engagement which is to be expected, but there is strong cooperation with Norway's close partners, such as the Nordic states, where cooperation is close, uncomplicated and dealt with speedily. This includes through the use of Nordic arrest warrants, which are forwarded directly between the competent judicial authorities. Norwegian LEAs are very involved in cooperation with EEA countries under the EU framework for cooperation, including for ML,

predicate offences and TF. Formal cooperation between Norway and non-EEA countries also appears to be working quite well, based on a legal framework for mutual legal assistance and extradition that is generally broad. With respect to other forms of cooperation, the FIU, LEAs and the Customs Authority are well engaged in international cooperation, both upon request and spontaneously.

8.33. Norway has a **substantial level of effectiveness** for IO.2.

8.4 Recommendations on International Cooperation

a. Norway should, as a matter of priority (noted in the 2005 MER), have a data and case management system that would enable the authorities to keep statistics on all mutual legal assistance and extradition concerning: (i) the number of requests; (ii) the nature of requests; (iii) whether requests were granted or refused; (iv) the type of crime to which the requests relates; and (v) how much time was required to respond to the requests.

b. Norway should prioritise implementation of measures for international cooperation in keeping with identified risks.

c. Norway should establish a clear legal basis for the enforcement of foreign freezing/seizing/confiscation orders when they are formulated under a request made by a foreign state under any treaty to which Norway is a signatory.

d. The FSA should prioritise and support international cooperation on regulation and supervision of FIs and DNFBPs commensurate with the risks faced by Norway. In particular, the FSA should:

- establish and use clear and secure gateways and mechanisms that will facilitate and allow for the transmission and execution of requests. In addition, the FSA should broaden its assistance to international supervisors for all types of FIs and DNFBPs it supervises.
- work with European partners to establish an effective supervisory regime for passported FIs, and in particular the MVTS sector.

e. Noting the risks outlined in the NRA, Customs authorities should prioritise international cooperation, including setting up and using secure gateways for the transmission and execution of their requests.

f. Norway's competent authorities should provide feedback to their international counterparts regarding the usefulness of the information provided and the value of the information received added to their domestic processes.

Technical Compliance Annex

1. INTRODUCTION

This annex provides detailed analysis concerning the level of technical compliance for Norway with the FATF 40 Recommendations. It does not include descriptive text on the country situation or risks, and is limited to the analysis of technical criteria for each Recommendation. It should be read in conjunction with the Mutual Evaluation Report.

2. NATIONAL AML/CFT POLICIES AND COORDINATION

Recommendation 1 – Assessing Risks and applying a Risk-Based Approach

a2.1. At the time of the 3rd Mutual Evaluation Report (MER) there was no requirement for a national risk assessment or the other risk related requirements set out in R.1.

a2.2. ***Criterion 1.1*** – Norway issued its first National Risk Assessment (NRA) in March 2014, following an eight month study, led by the MoJ, with the FIU, taking a leading role. The NRA refers to STR data from 2010-13, though it should be noted that the quantity and quality of these STRs are regarded by the FIU as being unsatisfactory. The NRA also draws to a limited extent on some other threat assessments, but does not consider the nature or volume of the ML threats associated with various types of predicate offences, nor does it draw to any real extent on the risks identified by law enforcement or the private sector concerning underlying predicate offences. Only generic information is available on ML techniques, which is based on limited information sources, and there is no assessment of the relative importance of the threats and of the potential consequences or impact. While some information is available on vulnerabilities, there are other vulnerabilities cited during the onsite visit which are not referenced. The NRA therefore does not properly identify and assess the ML/TF risks.

a2.3. Other threat assessments and analyses have been issued by specific agencies for the areas under their responsibility such as organised crime or drug trafficking, including by the FIU for ML, and ØKOKRIM and KRIPOS on profit-driven crime in Norway. Although these assessments collectively provide some risk information in some areas, they do not address in a coordinated and comprehensive way the risks for Norway concerning ML and the underlying predicate offences. As regards TF, the PST issues annual threat assessments and there appear to be a noticeably stronger mechanisms and products identifying and assessing TF risk. The finding on c.1.1 also has a negative impact on several other criteria, in particular, c.1.5 and c.1.7.

a2.4. **Criterion 1.2 –** The preparation of the NRA was conducted by an inter-governmental expert group created through a Cabinet decision, with representatives of the Ministries of Justice and Finance, the National Police Directorate, FIU, PST and FSA. The work on the NRA is part of a broader review of the entire law enforcement structure and workings, which was instigated following the Breivik terrorist attack. The temporary expert group did not properly co-ordinate actions to assess risks. Rather it was left to the FIU to draft almost all of the NRA and several key agencies either did not participate in the exercise and/or do not agree with its contents.

a2.5. **Criterion 1.3 –** As noted above, although the Norwegian NRA is very recently produced, and there is an intention that the NRA will be updated biennially, and funds have been allocated to the MoJ to complete this work. The PST publishes annual assessments on terrorism and TF.

a2.6. **Criterion 1.4 –** The inter-governmental nature of the expert group has helped to promote sharing of the risk assessment information amongst competent authorities. Other information on risks and threats, including from international sources, is shared amongst the principal relevant Ministries (Finance, Justice and Public Security, and Foreign Affairs) and their respective agencies using formal, informal and ad hoc channels of cooperation. There is also a recently established co-ordination group on serious crime with representatives of the public and private sector. Information on risk is also made publicly available on the government-run (FIU and FSA) web page www.hvitvasking.no. There is a mix of communication channels though it appears that the level of communication and sharing of ML/TF risk information with reporting entities is less satisfactory.

a2.7. **Criterion 1.5 –** Norway advises that resource allocation, including implementing specific risk-based measures to combat ML/TF, is determined by the annual Fiscal Budget, and that this process can involve a broad consideration of a range of factors including ML/TF risk. More detailed resource allocation is then decided at ministry and agency level. The budget process does allocate resources, including for AML/CFT purposes such as more FIU staff or a new computer system, but there does not appear to be any link with the assessment of ML/TF risks.

a2.8. **Criterion 1.6 –** Norway has created a number of exemptions regarding the application of CDD measures (*MLR* s.10), which are based on *3AMLD*. It has not been demonstrated that these categories are low risk or that the preconditions required under c.1.6 are met.

a2.9. **Criterion 1.7 –** Reporting FIs must apply "other customer due diligence measures" (in addition to the basic CDD measures) to situations involving a "high risk of transactions associated with proceeds of crime" or TF and terrorism offences, and also to foreign PEPs and correspondent banking (*MLA* ss. 15-16). However as noted in R.10, although enhanced CDD is required in high risk cases, concerns remain, such as: the narrower concept of "high risk transactions", no examples of such high risk scenarios except for foreign PEPs and correspondent banking, no elaboration of the nature of the "other CDD measures" and the fact that these other measures only relate to CDD and not to other AML/CFT areas e.g. enhanced internal controls.

a2.10. **Criterion 1.8 –** The *MLA* requires reporting entities to apply and adapt the level of CDD (including on-going monitoring, record keeping, timing and third party reliance) according to the level of risk that the entity assesses: s.5. The implication is that if the risk level is assessed to be lower, then (implicitly) simplified measures could be taken. There are no specific conditions attached, and the only specific provisions that deal with simplified CDD do not provide for simplified measures, only for exemptions": *MLA s.13, MLR s.10*. Taken together, the *MLA* and the FSA guidance do not provide clarity on the obligations, which has resulted in reporting entities taking a conservative approach generally. Moreover as Norway has not fully assessed its ML/TF risks, the preconditions for simplified measures are not met.

a2.11. **Criterion 1.9 –** The FSA and the Supervisory Council for Legal Practice are the competent authorities for AML/CFT supervision. Both have comprehensive inspection and monitoring powers as well as powers to impose sanctions to ensure implementation of the preventive measures. However, monitoring of AML/CFT compliance has not extended to requirements on FIs and DNFBPs to assess risk and implementing measures for risk mitigation. Overall, the supervision undertaken will not ensure compliance by reporting entities with R.1 (see also R.26-28).

a2.12. **Criterion 1.10 –** Obligations for reporting entities regarding risk are based on the requirement to conduct CDD measures using a risk-based approach, where risk is to be assessed on the basis of customer type, customer relationship, product and/or transaction: *MLA* s.5. The reference to the use of an RBA is brief, and is not expanded elsewhere in the *MLA* or *MLR*. It implies that the reporting entity must identify and assess the risks. As regards the categories of risk, it is not clear that all types of risk need to be considered; however, this may depend on the meaning underlying the text used i.e. there is no clear need to consider country/geographic risk, and also vis-à-vis services and delivery channels. As regards documenting the risk assessments, there is an obligation for reporting FIs to be able to demonstrate that the extent of measures carried out is adapted to the risk concerned. This may be adequate in many cases but this is not the same as documenting the risk assessment, and consideration should be given as to how the requirement can be reinforced. The requirement to apply CDD using a RBA is an on-going one. There is also the obligation in *MLA* s.14 to update documentation and information concerning customers. Therefore the requirement to keep risk assessments updated is partially and implicitly met. There is no mechanism that ensures that risk assessment information held by a reporting entity is provided to supervisors.

a2.13. **Criterion 1.11 –** Reporting FIs are required to have satisfactory internal control and communication procedures to fulfil the obligations in the *MLA*, and those procedures must be established at the highest management level, with a management level official assigned special responsibility for following up the procedures. Although this is not a direct and specific requirement to have policies and procedures to manage and mitigate risk, there is the indirect and more generic obligation to have procedures that will enable the requirements of the *MLA* to be met, which include a number of risk based obligations, and which must be approved by senior management. However, since the obligations have important deficiencies, this negatively impacts this criterion. The *MLA* does not require the controls to be monitored, although this is referred to in the FSA Guidelines. As regards higher risks and enhanced measures see c.1.7 above.

a2.14. **Criterion 1.12 –** The *MLA* and *MLR* appear to require simplified measures based on risk, but do not attach conditions, and the only detailed provisions relate to exemptions. Similarly, FSA Guidance gives the appearance of allowing simplified measures, due to the headings, but the actual text refers to exemptions, and

the position is not at all clear (see c.1.8 above). Exemptions are specifically prohibited if there is a suspicion of ML/TF.

a2.15. **Weighting and conclusion:** The recent NRA has established a mechanism that could be used to assess ML/TF risk. However, the flaws with the NRA mean that Norway has not properly identified and assessed the ML risks that it faces. In addition, neither allocation of resources nor mitigating measures are applied on the basis of ML/TF risk. These are important technical deficiencies. Authorities possess a better understanding of TF risks and base their operational work on this. **Norway is rated PC with R.1**.

Recommendation 2 – National Cooperation and Coordination

a2.16. In its 3rd mutual evaluation report (MER), Norway was rated LC with co-ordination requirements (see paragraphs 401-404). The MER found that Norway had implemented mechanisms that facilitate domestic co-operation at both the operational and policy levels, and that the relevant agencies were authorised to cooperate.

a2.17. **Criterion 2.1 –** Norway does not have national AML/CFT policies which are sufficiently informed by ML/TF risk, nor does it regularly review its policies. Norway nominally establishes its AML/CFT policies through the annual budget allocation to relevant agencies. The MoJ, the Police and the MoF have jointly issued a series of action plans for combating economic crime (1992, 1995, 2000, 2004, and 2010) which Norway views as the key strategy documents for Norway's AML/CFT efforts. The Action Plan against Economic Crime 2010-11 (covering 2010-14) was not provided to the team in English and it is assumed that it has little focus on AML/CFT. Norwegian officials articulated an overarching national strategy to combat extremism and terrorism, including measures to combat TF. The national policies and strategies for TF incorporate AML/CFT preventive elements, but these are fragmented, not up-to-date and AML/CFT is generally a secondary consideration. There is a lack of pro-active strategic approach to AML/CFT and any policies that exist are not carried out in a coordinated manner. As a result, AML/CFT priorities vary between competent authorities. ML/TF risk has only been considered in implementing AML/CFT measures on a limited and ad hoc basis, and it is unclear how risk is taken into account when setting annual priorities through the budget process.

a2.18. **Criterion 2.2 –** Norway takes a multi-agency approach to developing and implementing national AML/CFT policies. The responsibilities for Norway's AML/CFT policies are divided between the MoF, MoJ and MFA, and entities subordinated to these ministries. However, Norway does not have a coordination mechanism that is responsible for national AML/CFT policies.

a2.19. **Criterion 2.3 –** Norway does not have adequate mechanisms in place to enable the various authorities to coordinate on AML/CFT. Cooperation is generally undertaken on an informal and ad hoc basis. The review of AML/CFT legislation and regulations in 2009, involved consultation between the relevant national authorities and the private sector, in line with Norwegian Government requirements contained in the *Instructions for Official Studies and Reports* (2005), and the coordination requirements associated with the Cabinet and budget processes. However, this process was followed for the review of Norway's AML/CFT laws and has not occurred on a regular basis for national AML/CFT policies. There are no mechanisms to facilitate cooperation and coordination between the FIU and the FSA concerning the development and implementation of AML/CFT activities. This is a particular concern given the key roles these agencies play in Norway's AML/CFT regime. While some high level coordination takes place, this is not AML/CFT specific and the occasional cooperation at the operational level is insufficient.

a2.20. Norway has some examples of other operational level cooperation for ML, as informal and ad hoc meetings are held on a case-by-case basis. Given that they are located in the same agency, there are well established cooperation mechanisms between the FIU and the investigative units in ØKOKRIM. However, the coordination between the FIU and the police districts is not as strong. While some coordination takes place, there are no effective mechanisms to facilitate this coordination at both an operational and policy-making level. Annual cooperation meetings are held between the Public Prosecution Authority, the Police Director, the Head of ØKOKRIM and the Director of Taxes where AML/CFT may be a topic raised. A similar mechanism exists between the senior management of ØKOKRIM and FSA where AML/CFT can be discussed. However, these high level mechanisms are not sufficient and AML/CFT forms a minor part of the agenda. There is

no cooperation between the FSA and the police districts. The nature and level of cooperation between the various competent authorities remains a concern.

a2.21. In relation to TF, the PST also cooperates closely with other partner agencies, such as the FIU, regional police districts, customs authorities, the Police Immigration Service and KRIPOS and the MFA. The PST has formalised dialogues, and also cooperate on a case-by-case basis. However, it is a concern that the PST and FSA do not have any mechanisms to coordinate, particularly given the FSA's role in the implementation of the *Al-Qaida and Taliban Regulations* (see R.6 below). Norway has also established the Contact Group for the Prevention of Acts of Terrorism, comprising of public and private sector entities, including the FSA and the Business and Industry Security Council (representing financial institutions). The Contact Group meets 2-3 times per year, and TF issues may be considered.

a2.22. **Criterion 2.4 –** Norway has established coordination mechanisms to combat exports of goods and technologies relevant for the development of weapons of mass destruction and the financing of proliferation. An operational working group meets weekly or bi-weekly to review applications for export licences and transfers of funds to and from Iran. Representatives from the PST, the customs authority, the export section of the MFA and the legal department of the MFA participate. The group also assesses export and financial exchanges with other states, including DPRK. However, it is a concern that the FIU and FSA do not appear to participate in this or any other proliferation forum, even on an 'as necessary' basis. It is also a concern that the PST and FSA do not have any mechanisms to coordinate, particularly given the FSA's role in the implementation of the *Iran and DPRK Regulations* (see R.7 below).

a2.23. **Weighting and conclusion:** Norway does not have national AML/CFT policies and there is no coordination mechanism for AML/CFT. While some informal and ad hoc cooperation between authorities takes place, this is not sufficient. **Norway is rated PC with R.2**.

Recommendation 33 – Statistics

a2.24. In its 3rd MER, Norway was rated PC with previous requirements concerning statistics. Norway took action to address some of the deficiencies and the 4th Follow-up Report (FUR) concluded that Norway had raised its compliance to a level essentially equivalent to LC (see paragraphs 92-99).

a2.25. **Criterion 33.1(a) –** The FIU keeps comprehensive statistics regarding STRs received and disseminated. It produces an overview of STRs and other information received as well as how the information is processed and disseminated. There are statistics concerning the number of STRs received, the number of cases (containing one or several STRs) opened, information sent to supervisory authorities, dissemination of intelligence reports to LEAs and also notifications of information disseminated to *Indicia*. The FIU does however not keep statistics reflecting the actual use of the information disseminated.

a2.26. **Criterion 33.1(b) –** Norway was not able to provide the assessment team with adequate and reliable statistics regarding ML investigations, prosecutions and convictions. The police districts maintain statistics in relation to reported offences according to s.317 of the *Penal Code* (*PC*); but without distinction between receiving and ML offences. The Norwegian Prosecution Authority is the designated authority to keep statistics regarding ML prosecutions and convictions. However, Norway was unable to provide comprehensive statistics, as those provided were not reliable and had significant flaws. ØKOKRIM also maintains statistics on ML prosecutions and convictions. The PST keeps statistics regarding TF investigations as well as other actions taken to prevent TF.

a2.27. **Criterion 33.1(c) –** Norway does not maintain comprehensive statistics regarding property frozen; seized and/or confiscated. In principle, each police district and special unit within the police keeps its own statistics in relation to frozen and seized property. These statistics are required to be kept as part of internal control procedures based on Regulation 2010/007 regarding processing of seizures in criminal cases. Norway reports that the Police Directorate maintains a national database for criminal cases which also contains information regarding convictions and related confiscations, including the number of confiscations and the amounts (in NOK) confiscated. ØKOKRIM maintains statistics on confiscation orders, but not on actual

amounts confiscated. Norway was unable to provide statistics on asset freezing/seizures, total amounts confiscated, or confiscations by KRIPOS.

a2.28. **Criterion 33.1(d) –** There are no statistics regarding the total number of mutual legal assistance and extradition requests sent/received. Mutual legal assistance requests to and from EU/Schengen represent the majority of the MLA requests in Norway. Statistics regarding these mutual legal assistance requests are not available because these requests are generally communicated directly between the competent judicial authorities. The MoJ electronically registers some basic data regarding other mutual legal assistance requests in the MoJ's case file system "*Websak* when the requesting state is not an EU/Schengen state or when the request was sent directly to the competent judicial authority in Norway. Norway keeps basic data on extradition requests in *Websak*, except requests for concerning execution of arrest warrants between Norway and other Nordic countries. The latter requests are communicated directly between the competent judicial authorities and not centrally registered.

a2.29. The FIU keeps comprehensive statistics regarding its information exchange with other FIUs (both incoming and outgoing requests) in its IT system *"Ask"*. The FSA does not keep statistics regarding AML/CFT specific information exchanges with foreign counterparts. Norwegian LEAs do not keep records of information exchange with foreign LEAs.

a2.30. **Weighting and conclusion:** Norway does not maintain comprehensive statistics on key issues including international cooperation, asset seizure and confiscation, and ML investigations and prosecutions. The only reliable and comprehensive statistics are those maintained in relation to STRs and TF investigations. **Norway is rated PC with R.33**.

3. LEGAL SYSTEM AND OPERATIONAL ISSUES

Recommendation 3 – Money laundering offence

a3.1. ML is principally criminalised in s.317 of the *PC*. In its 3rd Mutual Evaluation Report (MER), Norway was rated LC for the ML offence and C for requirements concerning *mens rea* and corporate criminal liability (see paragraphs 75-96). The main technical deficiencies were that: the criminalisation of ML did not cover self-laundering and that the conspiracy offence was not sufficiently broad. In 2006 Norway addressed these deficiencies by amending s.317 (self-laundering) and adding s.318 (ML conspiracy) of the *PC.*

a3.2. **Criterion 3.1** – As noted in the 3rd MER, s.317 fully covers all the physical elements of the ML offence required under the *Vienna Convention* and the *Palermo Convention*[1]. However, it should be noted that for 3rd party laundering (not self-laundering) the offence is described as "aiding and abetting" the predicate offence, rather than as a free standing offence.

a3.3. **Criteria 3.2 & 3.3** – Section 317 makes it an offence to launder "the proceeds of a criminal act", and thus covers the proceeds of all criminal offences. This approach covers a wide range of offences in all 21 categories of designated predicate offence (including tax offences).

a3.4. **Criteria 3.4 & 3.5** – In s.317, the term "proceeds" covers all types of property, regardless of the value, that directly or indirectly represents the proceeds of crime. It is not necessary that a person be convicted of a predicate offence to prove that the property is the proceeds of crime.

a3.5. **Criterion 3.6** – Although the offence does not expressly refer to foreign predicate offences, the preparatory works make it clear that predicate offences for ML extend to conduct that occurred in another country, constituted an offence in that country, and would have constituted a predicate offence had it occurred domestically.

a3.6. **Criterion 3.7** – Since its last evaluation, Norway has extended s.317 to expressly cover self-laundering, which is separately criminalised in a different paragraph of s.317.

a3.7. **Criterion 3.8** – It is possible under the general *Criminal Procedure Act* (*CPA*) to infer the intent and knowledge required to prove the ML offence from objective factual circumstances.

a3.8. **Criterion 3.9** – The criminal sanctions that can be applied to natural persons convicted of ML are proportionate and for technical compliance purposes could be considered dissuasive, though at the minimum end of the range. Although the penalty for ordinary ML is limited to up to 3 years imprisonment and/or a fine (unlimited in amount), aggravated ML has a penalty of up to 6 years imprisonment and is used based on a number of factors, which include the value of the property being laundered (i.e. if more than NOK 100 000 – EUR 13 000). In addition drug ML is subject to 21 years imprisonment. Furthermore, the penalty for ML can be doubled in cases involving organised crime but not by more than five years imprisonment.

a3.9. As regards ordinary ML and aggravated ML, the maximum penalty for ordinary ML is lower than in many other countries, but is consistent with the penalty for many other economic crimes in Norway. As regards the offence of aggravated ML it is notable that this is available in cases where quite small amounts of money are laundered. The unlimited fine also adds to the sanctions options; however, an effective confiscation regime should deprive an offender of any criminal proceeds. The offence of ML conspiracy (s.318) has a penalty of up to 3 years (doubled if it involves organised crime – Penal Code s.60a).

a3.10. **Criterion 3.10** – Legal persons are subject to criminal liability and can be penalised with unlimited fines. Parallel civil or administrative proceedings are not precluded with respect to legal persons.

1 See Article 3(1)(b)&(c) of the *Vienna Convention*, and Article 6(1) of the *Palermo Convention*.

a3.11. **Criterion 3.11** – A range of ancillary offences to the ML offence are now available, following the addition of s.318 *PC* which criminalises conspiracy. Aiding and abetting a ML offence is not expressly covered as an offence, unlike other offences, but Norway refers to the Preparatory Works as explaining that this is covered, and provided two case examples of aiding and abetting ML.

a3.12. **Weighting and conclusion:** Norway is compliant with all technical criteria. **Norway is rated C with R.3**.

Recommendation 4 – Confiscation and provisional measures

a3.13. The legal provisions concerning confiscation and provisional measures are set out in the *PC* s.34-38 and *CPA* s.202-217. In its 3rd MER, Norway was rated C for these requirements (see paragraphs 108-125), and the confiscation regime was considered to be a comprehensive one. There has been no change to the legislation since the 3rd MER, and the legal provisions remain generally comprehensive.

a3.14. **Criterion 4.1** –Norway has a broad set of legal powers to deprive criminals of their proceeds or instrumentalities. Confiscation of the proceeds from any criminal offence (or property of corresponding value) is mandatory, including any profit or other benefit derived directly or indirectly from the proceeds: *PC* s.34. The amount of the proceeds can be proven to the civil standard. Confiscation of instrumentalities used or intended for use in the commission of any criminal offence (or property of corresponding value), or which are the product of such an offence, may be confiscated if this is considered an appropriate penalty for the act: *PC* s.35. Action can also be taken against proceeds held by third parties who knew that the property was derived from a criminal offence or it was a gift in whole or in part, and similarly for instrumentalities. These powers are equally applicable where the offence is terrorism or TF.

a3.15. **Criterion 4.2** –The police and prosecution authorities, including ØKOKRIM, have investigative powers to identify and trace assets, including the power to order production of documents, conduct surveillance, and search persons and premises (see also R.30-31). The law provides for three types of provisional measures — freezing, seizure and charging. Freezing applies to property suspected of relating to terrorism or TF and has the effect that the suspect (or a third party) is legally prevented from disposing of it. The property may alternatively be physically seized: *CPA* s.202d-202g. Seizure orders under *CPA* s.203 deprive the suspect (or a third party) of the possession of the property, and prevents any dealing with it. They can also be used to freeze property e.g., police will leave proceeds in a bank account with an instruction to the bank that the account holder cannot deal with it. Charging involves placing a charge on the property for a specific amount in order to secure payment of a possible confiscation order. In all cases the initial decision or application can be made *ex parte* and without giving prior notice. Legal arrangements (contractual or otherwise) containing provisions that are contrary to the law are considered null and void e.g., where persons knew/should have known that their actions would prejudice the ability of the authorities to recover property subject to confiscation.

a3.16. Charging orders can be used against certain types of property held by a defendant or third parties, and can be used to secure a value-based confiscation claim (unlike seizure). However neither the power to charge nor to seize assets can be used against all of the defendant's assets, which may create problems in extended confiscation cases where not all of the property that is owned or controlled by a defendant has been identified at the time of charge. Moreover, courts do not have the power to order a defendant to disclose all of his/her assets (except possibly where there is a charging order), although investigative methods could be used. The Commission on Confiscation recommended (prior to the 3rd MER) that a power to seize all assets should be provided, but the legislation was not amended to allow this.

a3.17. **Criterion 4.3** - As noted above, criminal proceeds or instrumentalities held by 3rd parties can be confiscated. However, if a third party was bona fide and paid money or other assets of an equivalent value to the property that was proceeds, then confiscation is not permitted. Any benefit gained by undervaluing the proceeds could however be recouped.

a3.18. **Criterion 4.4** – Powers exist to seize and charge property, and to dispose of property if it could be damaged or deteriorate. When a confiscation order has been made then if there is seized property, the Public Prosecutor can order its disposal, and if a pecuniary order has been made, then the National Collection Agency

seeks to recover the civil debt. There is also a power to appoint an administrator over charged property so as to ensure that income does not go to the defendant, but there are no other specific powers or mechanisms that enable the authorities to manage property. In many cases the type of property does not require any active management e.g., a bank account that is frozen or a seized motor vehicle, or the combination of a charge and an administrator might suffice. However in some cases there could be a need for property to be actively managed e.g., a restaurant or other business, and Norway does not have the mechanisms or the specific legal powers to do this.

a3.19. One very effective additional power that is available to prosecutors is the power to use extended confiscation in serious cases (i.e. cases which could result in a penalty of 6 or more years imprisonment or if the penalty is 2 years or more, the type of offence may result in a considerable gain (NOK 75 000 or more – EUR 9 750) and if the offender was convicted within the previous five years of an offence resulting in a considerable gain: *PC* s.34a. If extended confiscation applies then it can also cover the property of a spouse in certain circumstances, as well as property of the offender's close relatives, or legal persons that the offender owns or controls: *PC* s.37a. In such cases, the prosecution must prove on a balance of probabilities that the property stems from criminal acts committed by the offender, and if extended confiscation applies in full then the burden of proof is reversed and the offender must prove on the balance of probabilities that the assets were legally obtained: *PC* s.34a.

a3.20. Section 34 may also allow confiscation of proceeds even when a person is not convicted (NCB). However, there are several preconditions which make the section difficult to use in practice. The wording of s.34 is not particularly clear: "Confiscation may be effected even though the offender cannot be punished because he was not accountable for his acts (sections 44 or 46) or did not manifest guilt". Moreover one judgment indicated that a conviction is required under s.34, but another Supreme Court decision appears to allow confiscation of proceeds even where a defendant is acquitted due to lack of mens rea, provided that it is proved to the criminal standard that the *actus reus* of the crime occurred, and that the property is proceeds of that specific crime. Thus, although not entirely clear, it appears that NCB confiscation may be possible, but with some stringent preconditions.

a3.21. **Weighting and conclusion:** Norway has a good legal framework for confiscation but does not have measures in place to manage seized or confiscated property. **Norway is rated LC with R.4**.

Operational and Law Enforcement

Recommendation 29 – Financial intelligence units

a3.22. In its 3rd MER, Norway was rated PC with these requirements (see paragraphs 146-159). Norway took action to substantially address the deficiencies identified in the MER and Norway's 4th Follow-up Report (FUR) concluded that Norway had raised its compliance with the relevant requirements to a level essentially equivalent to LC. The revised R.29 puts an enhanced focus on access to information; the analytical functions of the FIU; and the dissemination of information.

a3.23. **Criterion 29.1** – The FIU is part of ØKOKRIM, and is a law enforcement/judicial type of FIU with a multi-disciplinary team headed by a senior public prosecutor. It is responsible for receiving, analysing and disseminating information disclosed by the entities with the reporting obligation: s.4 *MLA*.

a3.24. **Criterion 29.2** – The FIU is Norway's central agency for the receipt of STRs filed by reporting entities as required by R.20 & 23. If a reporting entity has a confirmed suspicion that a transaction is associated with the proceeds of crime or a violation of ss.147a, 147b and 147c of the *PC*, it shall on its own initiative submit information to the FIU concerning the transaction and the circumstances that gave rise to the suspicion: *MLA* ss.17-18. The reporting entities should also, as far as possible, provide additional information that supplements a transaction to the FIU: *MLR* s.13. Reporting FIs are required to electronically report all cross-border currency transactions, including physical carriage of cash or BNIs, cross-border bank transactions

and use of credit cards[2], as well as currency exchanges to the Register of Cross Border Transactions and Currency Exchange (the Currency Register): *Currency Register Act (CRA*) s.5. The information must be submitted in electronic format within five days after completion of the transaction. This register is kept by the customs authorities while c.29.2 requires that the FIU should also serve as the central agency for this kind of disclosures. However, the FIU, as part of ØKOKRIM, has direct access to the Currency Register.

a3.25. **Criterion 29.3** – A reporting entity shall, upon request of the FIU, provide the FIU with all necessary information concerning the transaction and the suspicion it has disclosed: *MLA* s.18. The FIU has direct access, through its database "*Ask"* to a wide range of databases and registers, including all police registers; the Currency Register; public registers (e.g., the business register); registers for government use (e.g., the population register); and commercial databases (e.g., credit bureaus).

a3.26. **Criterion 29.4** – The FIU's database system *"Ask"* has analytical and data processing functions and directly links STRs to relevant public and police sources, and all requests and messages from other FIUs and police units. *"Ask"* allows FIU staff to perform the necessary analysis to develop intelligence products. Additional analysis is conducted "manually" and largely consists of analysis of transactions; the known financial capability of any subject; past criminal histories; etc. The analysis can include crime group mapping. The scope of strategic analysis currently carried out by the FIU is very limited. The FIU's former strategic analysis resulted in the production of a report on modus operandi and trends based on STRs in 2011 and no strategic analysis has been produced since that time. At present, there is one post dedicated to this function but this position had been vacant for 18 months and a new staff member took up these duties shortly after the on-site visit.

a3.27. **Criterion 29.5** – The FIU has a wide range of formats (e.g., charges, police reports to on-going investigations, intelligence reports, and the *Indicia* registry) for dissemination, spontaneously and upon request, of information to the police and prosecutorial authorities and authorities which have supervisory powers, such as the FSA and the tax and customs authorities. The main platform or channel for dissemination of information from the FIU to domestic LEAs (with the exception of the PST) is *Indicia*. The information is posted on *Indicia* after an in-depth analysis conducted by the FIU, using all sources of available information. The *Indicia* registry does not allow for uploading of supporting material, such as bank statements or other relevant financial information. In cases where the FIU wants to make this type of information available to LEAs, it disseminates the information in the form of an intelligence report with the supporting documents attached. Dissemination of information to the PST is always done in the form of intelligence reports using the police's data system.

a3.28. **Criterion 29.6** – The FIU has internal procedures and guidelines for security and confidentiality. There are strengthened procedures in place for handling, storage, protection of, and access to information contained in *the* FIU's IT system *"Ask*", which can only be accessed by FIU staff. The majority of FIU staff members (prosecutors and police officers) have specific security clearances to deal with sensitive financial intelligence and other data. There are no indications that the non-security cleared staff members would not have an understanding of their responsibilities in handling and disseminating sensitive and confidential material. Members of the Supervisory Board (see c.29.7 below) are not security cleared but are required to sign a confidentiality agreement consistent with *Supervisory Board Regulations* s.6. In addition, members are required to treat information to which they gain access as confidential: *MLA s.31*, and it is a criminal offence to breach such confidentiality: *PC s.121*.

a3.29. **Criterion 29.7** –Being part of ØKOKRIM has not prevented the FIU from independently carrying out its core functions. It is able to engage with other domestic authorities and can exchange information with its foreign counterparts without undue interference. However, the FIU does not have its own budget and it is dependent on ØKOKRIM's budget which could constitute an impediment for ensuring its operational independence even though Norwegian authorities report that this risk is mitigated by the fact that ØKOKRIM's Director is fully responsible for allocating the budget so that the FIU reaches its objectives.

2 The use of credit cards outside of Norway by Norwegian citizens and the use of credit cards in Norway by foreigners are treated as cross-border currency transactions.

a3.30. More importantly, the FIU continues to remain subject to the oversight of a Supervisory Board, including a representative from the private sector, in relation to protection of privacy and personal data, specifically, the requirement to delete certain data from its database after five years and its power to freeze transactions: *MLA* ss.31, 18 and 19. In that context, the members of the Supervisory Board are entitled to be given access to any information, documents or material that they deem necessary for their supervision, regardless of when this information and associated material were received by the FIU, with the exception of information relating to an on-going investigation (that is from the point where a formal investigation is opened). However, there is a lack of formal feedback mechanisms to inform the FIU about the use of data it has disseminated. This makes it difficult to determine which FIU data are used by LEAs for investigative or other purposes. In addition, the working methods of the Supervisory Board are not defined in regulation and are decided by its members: *Supervisory Board Regulations* s.7. This results in a situation where the Supervisory Board also conducts unannounced visits to the FIU in addition to its regular meetings. Consequently, the concern expressed in the 3rd MER and 4th FUR remains.

a3.31. On 1 July 2014, the Norwegian *Data Protection Authority Act* and related regulations entered into force and the FIU became subject to the additional oversight by the Data Protection Authority (DPA). Norway has issued regulations to supplement s.52-14 of the *Police Data Registration Act* to provide for a special mandate for the DPA to supervise the FIU's data–security measures, including in relation to the receipt, storage and dissemination of information (both to national and international counterparts). It is not clear if and how the oversight of the DPA will affect the work and independence of the FIU, nor is it clear how responsibilities will be divided between the Board and the DPA. At present, the Supervisory Board visits the FIU up to four times per year for 2-3 hours each visit.

a3.32. **Criterion 29.8** – The FIU has been a member of the Egmont Group since 1995. It engages in frequent exchange of information with foreign counterparts based on the Egmont Principles of Information Exchange and uses the Egmont Secure Web system for this purpose.

a3.33. **Weighting and conclusion:** Most of the technical requirements for the FIU are met, but there are deficiencies, the most important being the failure to produce strategic intelligence since 2011. The concern regarding operational independence remains from the 3rd round. **Norway is rated LC with R.29**.

Recommendation 30 – Responsibilities of law enforcement and investigative authorities

a3.34. In its 3rd MER, Norway was rated C with these requirements (see paragraphs 175-178).

a3.35. **Criterion 30.1** – Norway has a comprehensive network of law enforcement and prosecution authorities who have designated responsibility for investigating ML/TF. The DGPP is responsible for ensuring that ML/TF offences are properly investigated and prosecuted, and decides who should have the main responsibility for an investigation. In addition to local police, Norway has seven special permanent units that are organised directly under the National Police Directorate. These units offer assistance to the regional police districts and some of them also have prosecuting authority. ØKOKRIM is one of these permanent units and specialises in the investigation of complicated economic crime, including ML. ØKOKRIM has nine specialised teams, including a multidisciplinary asset confiscation team and specialised investigation teams for tax and corruption offences. The FIU is also part of ØKOKRIM.

a3.36. ML offences and confiscation cases are investigated by the police under the instruction of the Prosecution Authority in the police district where the offence was committed. There are specialised economic crime teams in all police districts. The local police do not investigate TF cases, which are the responsibility of the PST. To the extent that financial investigation is required, ØKOKRIM may also be involved in a TF case. TF investigations are primarily investigated at the head office of the PST, but all the 26 PST-district offices conduct preventive intelligence-cases in their districts, on all issues related to the PST's responsibilities.

a3.37. **Criterion 30.2** – All law enforcement authorities are authorised to investigate ML/TF offences during a parallel financial investigation.

a3.38. **Criterion 30.3** – The local police districts as well as the seven special permanent units of the police have the authority to expeditiously identify, trace, and initiate freezing and seizing of property that is, or may become, subject to confiscation, or is suspected of being proceeds of crime. The local police may seek assistance from ØKOKRIM, especially its assets confiscation team.

a3.39. **Criterion 30.4** – In Norway, all financial investigations of predicate offences are conducted by law enforcement authorities.

a3.40. **Criterion 30.5** –Investigation of ML/TF offences arising from, or related to, corruption offences are carried out by the anti-corruption team within ØKOKRIM.

a3.41. **Weighting and conclusion: Norway is rated C with R.30**.

Recommendation 31 – Powers of law enforcement and investigative authorities

a3.42. In its 3rd MER, Norway was rated C with the requirements regarding the responsibilities of law enforcement and investigative authorities (see paragraphs 179-183).

a3.43. **Criterion 31.1** – Norwegian competent authorities responsible for investigating ML, associated predicate offences and TF are able to obtain access to all necessary documents and information for use in those investigations.

a3.44. **Production orders:** Competent authorities have the power to compel production of objects that are deemed to be significant as evidence if the possessor is obliged to testify in the case. The word objects means movable property, including documents, electronically stored information and financial information that is held or maintained by financial institutions and other businesses or persons (i.e., transaction records, CDD data, account files and business correspondence, and other records, documents or information): *CPA* s.210. The Prosecution Authority must submit a request for a production order to the Court. In urgent cases, the Prosecution Authority may compel information directly, but must then submit the case to the Court for subsequent approval as soon as possible.

a3.45. **Search:** Competent authorities have the power to search premises for financial records, etc. if there are reasonable grounds to suspect that a criminal act punishable by imprisonment has been committed. The objective must be to search for evidence or things that may be seized or charged: *CPA* s.192. A search of the suspect's person may also be conducted on the same conditions as a search of his premises: *CPA* s.195.

a3.46. **Witness statements:** The police and Prosecution Authority do not have the power to compel witness statements, unless the witness is a public official or a person that acts on behalf of the state or a municipality: *CPA* s.230. A witness is obliged to attend at the police station (if served with a summons) to indicate whether he/she is willing to give a statement, and may consent to so doing: *CPA* s.230. The general principle is that witnesses are required to give a statement to the court: *CPA* s.108. Witnesses bound by certain secrecy laws (*Savings Banks Act* s.21; *Commercial Banks Act* s.18; *Act on insurance activity* s.1-6; FIA ss.3-14; *Securities Trading Act* s.10-9, and *Security Register Act* s.8-1) are required to provide statements to the police about matters covered by these laws: *CPA* s.230.

a3.47. **Seizure:** Competent authorities have the power to seize financial records, etc. provided that those records may have significance as evidence: *CPA* s.203. The principal rule is that the Prosecution Authority takes the decision on seizure; however, the police may take the decision when the suspect is caught in the act, pursued following the act, or on finding fresh evidence. In such cases, the Prosecution Authority must be notified as soon as possible and decides whether the seizure should be sustained: *CPA* s.206. Any seizure action is taken without prior notice to the suspect or third parties.

a3.48. **Criterion 31.2 –** Norway has legislative measures in place that provide law enforcement with a range of investigative techniques when conducting ML/TF or other criminal investigations, including: (i) video surveillance and technological tracking: *CPA* chapter 15a; (ii) concealed video surveillance of a public place: *CPA* s.202a; (iii) technological tracking when a person with just cause is suspected of an act or attempt of an

act punishable by imprisonment for five years or more: *CPA* s.202b; (iv) break-in for the purpose of placing a technical direction finder, or placing such finders in clothes or bags that the suspect wears or carries, when a person with just cause is suspected of an act or attempt at an act punishable for 10 years or more: *CPA* s.202c; and (v) control of communication apparatus if the maximum penalty is five years or more or if it is a drug related case: *PCA* s.216b, cf. 162 PC. Most of these techniques can thus only be used for serious offences (where the maximum penalty is five or ten year's imprisonment): *CPA* chapter 15a. The exception is video surveillance which can be used when there is just cause to suspect that criminal act(s) punishable by a term exceeding six months have been committed: *CPA* s.202a. Covert audio surveillance is never available in ML cases PCA s.216m.

a3.49. While competent authorities are also able to conduct secret searches and communications surveillance and to access computer systems, these investigative techniques are available when the maximum penalty is 10 years or more i.e. drug related ML or aggravated ML by an organised criminal group: *CPA* ss.200a and 216a, cf. *PC* s.162.

a3.50. Other coercive measures, such as infiltration, (undercover) operations and provocation are available in certain cases, including for ML, predicate offences or TF. These measures are not statutorily regulated and the specific crime types or cases where such techniques can be used, is not clearly defined. Rather, the use of non-statutory investigation methods has been recognised and developed through case law, especially by the Supreme Court, which has set conditions and limitations, and supported by rules and internal guidelines issued by the prosecuting authority. In general, such techniques can only be used if the crime is considered as a serious threat to society. Thus these measures would likely apply in all TF cases, but for ML offences, the scope and nature of the offence and the amounts of funds involved will be important factors when determining whether use of these techniques is permissible.

a3.51. **Criterion 31.3** – CPA s.210 allows the Prosecution Authority, police districts and special units such as ØKOKRIM to get a production order from the court requiring financial institutions to produce the records of account holders (see c.31.1). In urgent cases, the Prosecution Authority can compel this information directly. These powers can be used without prior notification to the owner. The customs authorities have similar powers in the *Value Added Tax Act* s.16-2. The time taken to respond to requests varies but in urgent cases can be very quick.

a3.52. In addition, account information is available in the taxation register as FIs report information on accounts, account holders and account balances to the tax authorities: *Tax Administration Act* s.5. LEAs have direct access to this information which is provided to the taxation authority on an annual basis, and can use this to identify many accounts in a timely manner. However, this information is only updated annually thus leaving a small gap when new accounts are created or the ownership of legal persons and arrangements changes. The *Tax Assessment Act* provides that the duty of confidentiality is overridden in criminal cases and this allows the tax authorities to share information they hold regarding income and asset declarations with the Prosecution Authority and the police both spontaneously and upon request.

a3.53. **Criterion 31.4** – The FIU is an integral part of ØKOKRIM and is empowered to provide all relevant information it holds in relation to ML, associated predicate offences and TF to the Prosecution Authority and other law enforcement authorities.

a3.54. **Weighting and conclusion:** The only deficiency is that Norway's mechanism to identify whether natural or legal persons hold or control accounts is limited since the register is only updated annually. **Norway is rated LC with R.31**.

Recommendation 32 – Cash Couriers

a3.55. In its 3rd MER, Norway was rated PC with these requirements. Norway took action to address the three deficiencies identified in the MER (paragraphs 286-196) and the 4th FUR concluded that Norway had raised its compliance to a level essentially equivalent to LC (paragraphs 118 to 122). While Norway is part of the Schengen area, it is a separate customs territory outside the EU.

a3.56. **Criterion 32.1** – Norway has implemented a declaration system for both incoming and outgoing cross-border transportation of currency and bearer negotiable instruments (BNI): *CA* s.3-1 and *RCA* s.3-1-11. Norway has also established an obligation to declare cross-border transportation of currency and BNI through mail and cargo prior to, or arrival of, the shipment: *CA* ss.4-10 & 4-11 and *RCA* ss.4-10-2(7) & 4-11-1. In addition, enterprises providing security guard services may be specifically authorised by the Directorate of Customs and Excise to declare directly on the Currency Register: *RCA* s3.3-1-11(3). There are only two such specifically authorised companies, freighting currency for businesses and banks, which have an obligation to declare within five days after importation/exportation. Given that these two companies are authorised and represent a low risk of non-reporting, the delay in reporting is not a concern.

a3.57. **Criterion 32.2** – All persons carrying out a physical cross-border transportation of currency and BNI with a value exceeding the equivalent of NOK 25 000 (EUR 3 250) are required to make a written declaration and present themselves to the customs authority at the point of entry to/exit from Norway: *CA* s.3-1 and *RCA* s.3-1-11.

a3.58. **Criterion 32.3** – This criterion is not applicable to Norway since it has implemented a written declaration system for all travellers carrying amounts above NOK 25 000 (EUR 3 250).

a3.59. **Criterion 32.4** – Upon discovery of a false declaration of currency and BNI or a failure to disclose them, customs officers have the authority to obtain further information from the carrier with regard to the origin of the BNI and their intended use: *CA* s.13-7.

a3.60. **Criterion 32.5** – Where persons make a false declaration or fail to make a declaration, customs authorities have the power to impose an administrative fine of 20% of the total amount of currency or BNI not declared: *CA* s.16-15 and *RCA* s.16-15-2. If the customs authorities suspect that currency or BNI carried by a person, regardless of the amount and whether any declaration was made, is associated with a crime that can be punished by imprisonment for more than six months, then they must report the case to the police/prosecutor for further investigation. In these instances, the currency and/or BNI concerned are immediately seized: *CA* s.16-13 and *CPA* s.206.

a3.61. **Criterion 32.6** – The customs authorities register all declarations in the Currency Register (see also R.29 above). The register does not include data regarding currency and BNI cross-border transactions which are related to proceeds of crime and which the customs authorities report to the police/prosecutor (see c.32.5 above). However, these cases are also reported for information to the FIU. The FIU and LEAs have direct on-line access to the Currency Register. Moreover, it is customs authorities' practice to also systematically inform the FIU about all cash smuggling cases above NOK 150000 (EUR 20 000), both in cases where an administrative fine was imposed and in cases where funds were seized.

a3.62. **Criterion 32.7** – As explained above, the customs authorities work closely together with the police, the FIU, and other domestic authorities. The co-operation between the customs authorities and the police is based on a formal agreement of 9 September 2010 which sets out the basic principles for high-level and operational cooperation, including exchange of information, use of equipment and mutual assistance. On that basis the customs authorities and local police districts have established routines and practices for day-to-day cooperation.

a3.63. **Criterion 32.8** – As mentioned above in relation to c.32.5, currency and BNI which are suspected to be related to proceeds of crime or related to TF are immediately seized: *CA* s.16-13 and *CPA* s.206. In cases of false declarations, customs authorities stop the currency or BNI carried by the person immediately to withhold an administrative fine of 20% of the total amount not declared and to determine whether there is a suspicion of ML/TF or predicate offences.

a3.64. **Criterion 32.9** – The customs authorities register all declarations in the Currency Register. Norway can exchange this data, either spontaneously or upon request, on the basis of bilateral and multilateral agreements regarding customs cooperation. The information can be equally exchanged by the FIU and the police with their foreign counterparts as well in the context of MLA. While the register does not contain any data regarding the cases handed over to the police/prosecutor because of a suspicion of a crime that can be punished with imprisonment for more than six months, this data would normally be included in the police

registers.

a3.65. **Criterion 32.10** – The Currency Register contributes to preventing and combating crime: *CRA* s.1. Only authorised personnel have access to the information contained in the register: *CRA* s.6. The *CRA* specifically provides that the police, including the FIU as part of ØKOKRIM, the prosecuting authorities, tax authorities, the National Insurance, and Statistics Norway in addition to customs authorities can access the register.

a3.66. **Criterion 32.11** – If the customs authorities suspect that currency or BNI carried by a person (regardless of the amount and whether any declaration was made) are the proceeds of crime or related to TF, then they report the case to the police/prosecutor for investigation. If the suspicions are confirmed, then the sanctions and measures described in relation to R.3-5 above will come into play.

a3.67. **Weighting and conclusion: Norway is rated C with R.32**.

4. TERRORIST FINANCING AND FINANCING OF PROLIFERATION

Recommendation 5 – Terrorist financing offence

a4.1. In its 3rd Mutual Evaluation Report (MER), Norway was rated LC with the requirements regarding the TF offence (see paragraphs 97-107) . Norway had not criminalised the collection of funds in the knowledge that they are to be used by a terrorist organisation or an individual terrorist. This deficiency remains outstanding.

a4.2. **Criterion 5.1** – TF is criminalised in a manner that is largely consistent with the TF Convention. It is an offence to obtain or collect funds or other assets with the intention that they should be used (in full or in part) to finance terrorist acts or other violations in s.147a: *PC* s.147b *first paragraph*. Further, it is an offence to make funds or other assets, bank services or other financial services available to terrorists or terrorist organisations, or person or enterprise acting on behalf of a terrorist or terrorist organisation: *PC* s.147b *second paragraph*. The term 'enterprise' is defined broadly in the preparatory works as meaning a company, society, corporation, cooperative or other association, one-man enterprise, foundation, estate or public activity. In addition, it is an offence to provide financial or material support to terrorist organisations when the organisation has taken steps to realise the purpose by illegal means: *PC* s.147d. The definition of 'terrorist act' includes a requirement that a criminal act referred to in the section has been committed with the intention of seriously disrupting society, intimidating population, or compelling a government, etc.: s.147a. The potential concern is that, because of this additional element of intention related to a terrorist purpose, the definition of 'terrorist act' used for the TF offence does not cover all of the conduct required in the UN conventions which is required by reference to Article 2(1)(a) of the TF Convention. There is no such requirement of intention in all of the offences in the UN conventions. As a result, the TF offence in s.147b does not cover all of the conduct covered by Article 2(1)(a) of the TF Convention. However, this is a minor technical issue and the funding of the conduct covered by the UN conventions without the additional intention element would be a criminal act as aiding and abetting of these criminal acts. Despite this issue, it is considered that Norway has criminalised TF on the basis of the TF Convention.

a4.3. **Criterion 5.2** – It is an offence to make available funds or other assets, or bank services or other financial services to terrorists or terrorist organisations for any purpose: *PC s.147b*. However, Norway has not criminalised as a stand-alone offence the collection of funds in the knowledge that they are to be used (for any purpose) by a terrorist organisation or an individual terrorist. Norway advised that the collection of funds is criminalised as an attempt to make funds available to terrorists or terrorist organisations under *s.147b*, though this has not been considered by the courts. In any event, the criminalisation of this conduct as an ancillary offence is not sufficient to meet the criterion. In addition, the scope issue noted above is also an issue for this criterion based on the definition of 'terrorist act' in the Glossary.

a4.4. **Criterion 5.3** – The TF offences apply to any funds. There is no restriction in the *PC* that would indicate that funds from both legitimate and illegitimate sources are not covered.

a4.5. **Criterion 5.4** – There is no requirement that the TF offence requires that the funds were actually used for a terrorist act, nor that it be linked to a specific attack.

a4.6. **Criterion 5.5** – The TF offence is subject to the same principles as the ML offence concerning: (i) inferring the intentional element of the offence from objective circumstances; (ii) criminal liability for legal persons; and (iii) the possibility of parallel criminal, civil or administrative proceedings. These requirements are met for the purpose of the terrorist financing offence.

a4.7. **Criterion 5.6** – The penalties for TF are proportionate and dissuasive, as it is punishable by a term of imprisonment not exceeding 10 years. Accomplices are liable to the same penalty: *PC* s.147b.

a4.8. **Criterion 5.7** – Criminal liability for TF offences applies to legal persons which are punishable by a

fine, and the enterprise may also by a court judgment be deprived of the right to carry on business or may be prohibited from carrying it on in certain form: *PC* ss.26a, 27, 48a-b. There is no limit on the size of the fine that can be imposed and there are no known cases of legal persons being found guilty of TF offences. However, for the offence of conspiracy to commit a TF offence, the penalty is 3 years 'unless the offence comes under a more severe penalty provision': *PC* s.162c. It is unclear whether this means that the penalty for conspiracy to commit a TF offence is 3 years or 10 years. A penalty of 3 years is not dissuasive or proportionate given the penalty for TF is 10 years.

a4.9. **Criterion 5.8** – Norway has a comprehensive range of ancillary offences to the TF offence. In particular, it is also an offence to: (i) attempt to commit TF (s.49); (ii) participate as an accomplice in a TF offence: *PC* s.147c; or (iii) enter into an agreement to commit TF (conspiracy) as part of the activity of an organised group or network: s.162c.

a4.10. **Criterion 5.9** – Norway has adopted an 'all crimes' approach to the criminalisation of ML and therefore TF offences are predicate offences for ML.

a4.11. **Criterion 5.10** – Norway's TF offence has broad application and can be used to punish the financing of a terrorist act even where the terrorist act was committed outside of Norway. There is qualifying language in s.147a—such as references to "society" and "that country" may indicate that s.147a could be interpreted as being limited to terrorist acts committed domestically. The Preparatory Works and their legal traditions indicate that the offence does cover terrorist offences committed outside Norway. In addition, s.147b must be read in conjunction with s.12 of the *PC* which is a general provision that provides for extra-territorial jurisdiction in respect of certain offences (including s.147a-b) for Norwegian nationals and residents and in certain cases even for foreigners. Consequently, the financing of terrorist acts committed both domestically and abroad are covered.

a4.12. **Weighting and conclusion:** While the TF offence meets most technical criteria, it does not cover the collection of funds in the knowledge that they are to be used by a terrorist organisation or an individual terrorist. This deficiency remains outstanding from the 3rd round MER. **Norway is rated LC with R.5**.

Recommendation 6 – Targeted financial sanctions related to terrorism and terrorist financing

a4.13. In its 3rd MER, Norway was rated PC with these requirements (see paragraphs 127-145). It was found that Norway had implemented measures to freeze terrorist assets, but the freezing regime did not fulfil all the required elements. Since the MER, Norway has issued guidelines for financial institutions and DNFBPs and established procedures. While the legislative framework for the sanctions regime remains largely unchanged, Norway issued a new Regulation on sanctions against Taliban of 8 November 2013.

a4.14. **Criterion 6.1(a)-(e)** – Under the *Act Relating to the Implementation of Mandatory Decisions of the Security Council 1968*, the King in Council has the authority to make regulations to implement binding measures from the UN Security Council into Norwegian law. Norway implements UNSCR 1267/1989 and 1988 (the UN Taliban/Al Qaida sanctions), and their successor resolutions, through the *Regulation on sanctions against Al-Qaida of 22 December 1999* (the *Al-Qaida Regulations*) and the *Regulation on sanctions against Taliban of 8 November 2013* (the *Taliban Regulations*)[1]. The PST is the Norwegian competent authority for identification and designation in accordance with the UN Taliban/Al Qaida sanctions. In addition, the MFA is responsible for the regulations, and it is authorised to amend, suspend or repeal these regulations (Art. 9). The PST is responsible for identifying targets and the MFA is responsible for proposing a person for designation (6.1(b)).

a4.15. **Criterion 6.2(a)-(e)** – Norway has sought to implement targeted financial sanctions pursuant to UNSCR 1373 through a mechanism to freeze terrorist assets in the *CPA*. However, Norway does not have a

1 While Norway relies on the EU framework to some extent to implement targeted financial sanctions for proliferation financing (R.7), it does not rely on this for terrorist financing (R.6).

mechanism to make designations pursuant to UNSCR 1373 as required by Recommendation 6 and therefore does not have a mechanism to identify targets for designation. Norway does have a mechanism which allows authorities to freeze without delay any assets of a natural or legal person suspected of terrorism offences, or an enterprise directly or indirectly owned or controlled by a suspected person: *CPA* s.202d-g. The PST or a public prosecutor may decide to freeze assets, without going to court, when a person is 'with just cause suspected' (more than 50% likely) of committing, or attempting to commit, a terrorist act or TF offence. The freezing order can either list the identified funds or assets that are known or can include any assets owned by the person. The one freezing order that has been made applied to specific property of the person and can include present or future assets. However, under this mechanism, a freezing order can only able be made as part of an ongoing criminal investigation and the order must be renewed every four weeks by the court (although the court may set a longer time limit if it deems that a new consideration in four weeks is not required): *CPA s202e*. This mechanism does not establish any prohibition from making funds available to persons subject to a freezing action under this mechanism, though the provision of funds to a terrorist or terrorist organisation would be considered a TF offence: *PC* s147b *second paragraph*. Therefore, while this mechanism provides for additional terrorist asset freezing, it does not implement all aspects of the targeted financial sanctions pursuant to UNSCR 1373 as required by Recommendation 6. Norway cannot consider requests for designation by foreign countries, although the asset freezing mechanism may be used when acting upon a rogatory letter from another country if Norwegian authorities open an investigation. The MFA is the competent authority for receiving lists of designated persons from other jurisdictions which are then distributed to the relevant agencies.

a4.16. **Criterion 6.3(a)-(b)** – In relation to the UN Taliban/Al Qaida sanctions, Norway relies on normal criminal laws to provide authority to collect or solicit information to identify persons and entities suspected of meeting the designation criteria. While the PST is responsible for the collection of information to identify persons and entities that meet the designation criteria, it does not have any mechanism or procedures to do this. In relation to freezing action under s202 of the *CPA*, the prosecutor may order persons to provide assistance necessary for freezing assets under s.202g. The legislation allows the PST or public prosecutor to freeze the assets, and the prosecuting authority must then bring the case before the district court within 7 days. However, as noted above, this mechanism can only be used as part of an ongoing criminal investigation and there is no prohibition from making funds available to persons subject to a freezing action under this mechanism.

a4.17. **Criterion 6.4** – In relation to the UN Taliban/Al Qaida sanctions, the regulations provide for the authority to freeze and prohibitions applying without delay by automatically incorporating any changes in UN lists into the Norwegian legal system. The *Al-Qaida Regulation and Taliban Regulation* also prohibit anyone from making funds available for the benefit of the entities listed and cross-reference the UN lists to implement targeted financial sanctions without delay: Art.3. In relation to freezing action under s202 of the *CPA*, Norway is able freeze the specific assets without delay once a decision to freeze has been taken. However, as noted above, this mechanism can only be used as part of an ongoing criminal investigation and there is no prohibition from making funds available to persons subject to a freezing action under this mechanism.

a4.18. **Criterion 6.5(a)** – In relation to the UN Taliban / Al Qaida sanctions, the freezing obligations and prohibition on providing funds and services applies on Norwegian territory (including Norwegian airspace), on board any aircraft or any vessel under Norwegian jurisdiction, to any Norwegian national inside or outside Norway to legal persons established or constituted under Norwegian law and to any legal person in respect of any business done in Norway: Art 1. The regulations do not explicitly reference that that freeze action must be *ex parte*, however Article 6 prohibits any acts which would have the effect of circumventing freeze actions and would prohibit prior notice to the subject of a freeze action or prohibition on dealing.

a4.19. **Criterion 6.5(b)(i)-(iv)** – (i) In relation to the UN Taliban/Al Qaida sanctions, the freeze obligation extends to all financial assets or economic resources in Norway 'belonging to, owned, held or controlled by a natural or legal person, entity, body or group listed in the Sanctions Committee's' lists: Art.3. (ii) Funds and economic resources 'controlled by' a designated entity are covered: Art 3. (iii) Funds generated from funds owned or controlled by a designated entity are covered under the definition of funds: Art 2. (iv) The obligations to freeze the funds or assets of persons and entities to be frozen when acting on behalf of, or at the direction of, designated persons or entities is met by the requirement to freeze funds or assets 'controlled by' a designated entity, which extends to persons acting on their behalf in relation to those funds: Art.3.

a4.20. **Criterion 6.5(c)** – The *Al-Qaida and Taliban Regulations* set out a prohibition of making available funds to or for the benefit of designated persons and entities: Art 3. There is no corresponding prohibition on making funds available to or for the benefit of persons in relation to UNSCR 1373.

a4.21. **Criterion 6.5(d)-(f)** – The FSA has provided guidelines to REs to inform them where to obtain the up-to-date designation lists and urges them to monitor the list of the UN Sanctions Committee through their electronic monitoring systems. The FSA also publishes the designation lists on its website. However, Norway does not have any system or mechanism to alert REs to changes to the designation lists when updated to the FSA website. Anyone who freezes funds or economic resources is required to immediately inform the MFA: Art.3. The Regulations include measures to protect the rights of *bona fide* third parties acting in good faith when freezing terrorist assets: Art.7.

a4.22. In relation to freezing action under s202 of the *CPA*, the PST has an internal procedure for the communication of a freezing order made by the PST or prosecutor to an entity which holds the assets or funds subject to that order. Under this procedure, the PST notifies the entity immediately, and the freezing order is also made public on the FSA's website. The FSA has provided guidelines on this asset freezing mechanism which explains the purpose and nature of this mechanism to financial institutions. The PST is also responsible for communicating de-freezing decisions to relevant entities. The *CPA* does not have specific measures to protect the rights of *bona fide* third parties acting in good faith. However, any person freezing assets would be doing so in response to an order received from the PST and/or a public prosecutor. .

a4.23. **Criterion 6.6(a)-(g)** – The *Al-Qaida and Taliban Regulations* state that any person or entity that is subject to a decision to freeze funds may request to be delisted in accordance with relevant sanctions committee's procedures: Art.3. The FSA's guidance on sanctions further explains that persons listed on the UN lists may submit a request to an agent appointed by the UN Secretary General to be removed. The guidance also notes that alternatively, a request for de-listing can be submitted via the MFA and provides contact details for this process. The FSA's Guidance provides a link to Sanctions Committee's website which contains relevant documents to request review and de-listing. Persons or entities with the same or similar name as designated persons or entities that are inadvertently affected by a freezing mechanism (i.e. a false positive) may contact the MFA, which is the competent authority for this. In its guidance, the FSA encourages financial institutions and DNFBPs to monitor the lists published by UN Sanctions Committees to ensure that they are aware of de-listings as soon as they occur. With regard to unfreezing under the *CPA*, if the conditions for freezing the assets are no longer fulfilled, such freezing shall be terminated without undue delay: s.202f.

a4.24. **Criterion 6.7** – The *Al-Qaida and Taliban Regulations* establish the procedures to provide access to funds frozen under those regulations in accordance with c6.7 and the relevant UNSCRs: art.4. With regard to unfreezing under the *CPA*, funds and/or assets that are required for basic expenses of the person, their household or any person they maintain, may not be frozen: *CPA* s202d, second paragraph.

a4.25. **Weighting and conclusion:** While Norway's framework to implement targeted financial sanctions pursuant to UNSCR 1267 is generally sound, the mechanism to implement targeted financial sanctions pursuant to UNSCR 1373 as required by Recommendation 6 can only be used as part of an ongoing investigation and does not establish a prohibition on making funds available, which are serious deficiencies. **Norway is rated PC with R.6**.

A4

Recommendation 7 – Targeted financial sanctions related to proliferation

a4.26. **Criterion 7.1** – Under the *Act Relating to the Implementation of Mandatory Decisions of the Security Council 1968*, the King in Council has the authority to make regulations to implement binding measures from the UN Security Council into Norwegian law. The MFA has the authority to suspend, amend, or repeal such regulations. Norway implements UNSCRs 1737 (2006), 1747 (2007), 1803 (2008) and 1929 (2010) through the *Regulation on Sanctions against Iran of 9 February 2007* (the *Iran Regulations*). Norway implements UNSCRs 1718 (2006) through the *Regulation No. 1405 relating to sanctions and restrictive measures against North Korea of 15 December 2006* (*the DPRK Regulations*), which adopts the EU framework in the *European Council Regulation (EC) No. 329/2007*. Norway recently revised the DPRK Regulations, with the revised regulations entering into force on 28 March 2014.

a4.27. R.7 requires implementation of targeted financial sanctions to occur *without delay*—a term that, in this context, is defined to mean "ideally, within a matter of hours". However, there are delays in transposing designations made by the UN into Norwegian law. The MFA is responsible for updating the annexes to the *Iran and DPRK Regulations* when the UN makes a designation. After being adopted by the MFA, the amended document is sent to Lovdata (the entity in charge of publishing laws and regulations) for inclusion in the regulation. For the Iran Regulations, the process to update Annex VIII takes 1-4 weeks. For the DPRK Regulations, the process to update Annex A takes 1-4 weeks, in addition to delays at EU level of approximately 4 weeks as Norway has adopted the EU framework. Once the UN makes a designation, the EU moves to amend the designation list in the annex to the corresponding EU Regulation. Because of the time taken to consult between the European Commission departments and translate the designation into all of the official EU languages, there is often a delay in when the designation and freezing decision is issued by the UN and the time that it is transposed into EU law. New designations are treated as being urgent and are generally processed in times at the lower end of this range. Other amendments to the list (such as deletions) are less urgent and will take more time to be transposed into EU regulation. These delays are a significant concern as the targeted financial sanctions for proliferation financing are not implemented without delay. The impact of this deficiency may be mitigated in part by the relative infrequency with which new entities are designated under relevant UN resolutions, and by wider measures taken by Norway applying to Iran and DPRK. In particular, Norway has established an authorisation process for transactions with Iranian entities above certain thresholds which allows the authorities to deny authorisation for transactions with potential targets for designation under UN resolutions, even if these have not yet been transposed into Norwegian law. This could potentially also be used to prevent the execution of transactions with designated entities during the period between their UN listing and the transposition.

a4.28. **Criterion 7.2** – The MFA is responsible for ensuring implementation of all UN Security Council's sanctions, and also the restrictive measures adopted by the EU to which Norway is aligned.

a4.29. **Criterion 7.2(a)-(c)** – Under the *Iran Regulations*, Norway requires all natural and legal persons to freeze all funds and economic resources belonging to, owned, held or controlled by designated persons, entities and bodies: Art.23.1-3. The freezing obligations relating to the UN lists extend to all funds or economic resources belonging to, owned, held or directly or indirectly controlled by the designated persons, entities and bodies: Art.23.1-2. The obligations to freeze the funds or assets of persons and entities to be frozen when acting on behalf of, or at the direction of, designated persons or entities is met by the requirement to freeze funds or assets 'controlled by' a designated entity, which extends to persons acting on their behalf in relation to those funds: Art.23.1-2. The *Iran Regulations* also prohibit the making of funds or economic resources available, directly or indirectly, to or for the benefit of the natural or legal persons, entities or bodies designated by the UN unless licensed: Art.23.4.

a4.30. Under the *DPRK Regulations*, Norway requires all funds and economic resources belonging to, owned, held or controlled by the persons, entities and bodies designated by the UN to be frozen: *Appendix A, EC No. 329/2007 Art.6(1)*. Norway also requires all funds and economic resources belonging to, owned, held or directly or indirectly controlled by persons, entities and bodies designated by the EU to be frozen: *Appendix A, EC No. 329/2007 Art.6(2)-(2a)*. The *DPRK Regulations* also prohibit the making of funds or economic resources available, directly or indirectly, to or for the benefit of the natural or legal persons, entities or bodies designated by the UN unless licensed: *Appendix A, EC No. 329/2007 Art.6(4)*.

a4.31. **Criterion 7.2(d)** – The FSA has provided guidelines to financial institutions and DNFBPs to assist with the implementation of the *Iran and DPRK Regulations*. The guidelines inform financial institutions and DNFBPs where to obtain the up-to-date designation lists and urges them to monitor the list of the UN Sanctions Committee through their electronic monitoring systems. However, the guidelines have not been updated to reflect the revised DPRK regulations. The FSA also publishes the designation list on its website. Norway does not have any system or mechanism to alert REs to changes to the designation lists when updated to the FSA website.

a4.32. **Criterion 7.2(e)** – The *Iran Regulations* require anyone who freezes funds or economic resources to immediately inform the MFA: Art.23.8. The *DPRK Regulations* require anyone who freezes funds or economic resources to inform the MFA and immediately provide any information that would facilitate compliance with

the EU regulations, including information about accounts and amounts frozen: *Appendix A, EC No.329/2007 Art.10*.

a4.33. **Criterion 7.2(f)** – The Regulations also include measures to protect the rights of *bona fide* third parties acting in good faith when freezing funds or economic resources: *Iran Regulations Art.42.1 and DPRK Regulations Appendix A, EC No. 329/2007 Art.11*.

a4.34. **Criterion 7.3** – The FSA is responsible for monitoring compliance by financial institutions and DNFBPs with the *Iran and DPRK Regulations*. However, the only measure the FSA has adopted for monitoring and ensuring compliance was to include a small number of questions on these regulations in their general questionnaires to banks which is provided as part of their desk-based reviews. The FSA has not undertaken any measures for other types of reporting entities outside of the banking sector. Persons, both natural and legal, who violate or wilfully aid and abet a violation of the *Iran or DPRK Regulations,* are liable to a fine or imprisonment not exceeding three years or both. Persons who negligently violate or negligently contribute to the violation of such regulations are liable to a fine or imprisonment up to six months, or both: *Act relating to the implementation of mandatory decisions of the Security Council of the United Nations: s.2*.

a4.35. **Criterion 7.4 (a)-(d)** – The Regulations provide details and the process for submitting a request to the UN focal point for de-listing: *Iran Regulations Art.23.9 and DPRK Regulations s3*. The FSA's guidance further explains that listed persons may submit a de-listing request to an agent appointed by the UN Secretary General and notes that a request can also be submitted via the MFA. Persons or entities with the same or similar name as designated persons or entities that are inadvertently affected by a freezing mechanism (i.e. a false positive) may contact the MFA, which is the competent authority for this issue. In its guidance, the FSA encourages financial institutions and DNFBPs to monitor the lists published by UN Sanctions Committees to ensure that they are aware of de-listings as soon as they occur.

a4.36. The MFA may authorise access to funds under the *Iran and DPRK Regulations*, or the making available of certain funds or economic resources when it has determined that the funds are: (i) necessary for basic needs of a designated person of their dependent family members; (ii) for professional fees; (iii) for payment of fees or service charges for routine holding or maintenance of frozen funds or economic resources: *Iran Regulations Art.26.1(a), DPRK Regulations Appendix A, EC No. 329/2007 Art.7(1)*. The MFA can only authorise access if the relevant UN Sanctions Committee has not objected within five working days of notification: *Iran Regulations Art.26.1(b), DPRK Regulations Appendix A, EC No. 329/2007 Art.7(1)*. The MFA may also authorise the release or making available of certain funds if it determines that they are necessary for extraordinary purposes and the relevant Sanctions Committee has been notified and approved: *DPRK Regulations Appendix A, EC No. 329/2007 Art.7(2)*.

a4.37. **Criterion 7.5** – The addition to frozen accounts of interests or other earnings due on those accounts or payments due under contracts, agreements or obligations is permitted, provided that such amounts also become subject to the freeze: *Iran Regulations*: Art.29.2(2), *DPRK Regulations Appendix A, EC No.329/2007 Art.9*. In addition, the MFA may authorise the release of certain frozen funds or economic resources in accordance with c7.5 and relevant UNSCRs: Art.25(a)-(b).

a4.38. **Weighting and conclusion:** The ability to freeze without delay is a fundamental component of targeted financial sanctions. Consequently, the delay in transposing UN designations into Norwegian law (c.7.1) is a serious technical deficiency. In addition, the very limited monitoring by the FSA for compliance is a concern (c.7.3). **Norway is rated PC with R.7**.

Recommendation 8 – Non-profit organisations

a4.39. In its 3rd MER, Norway was rated NC for these requirements (see paragraphs 399-400). Weaknesses included a need to review the laws and regulations that relate to NPOs; a lack of 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 terrorist acts or terrorist organisations. Many of these deficiencies have been addressed.

a4.40. **Criterion 8.1** – In 2007 Norway amended its legal framework through the *Act on the Registration of Charitable Fundraising* which established a voluntary licensing regime for the charitable collection of funds by NPOs. Although the Act is new, following discussion with the NPO sector the Ministry of Culture commenced a review of the adequacy of the operation of the new Act through an external evaluation. A joint government/NPO sector group is working to review the regime and propose amendments to the regulatory framework. Norway has the capacity to obtain timely information on the activities, size and other relevant features, to identify the features and types of NPOs that are particularly at risk of being misused for TF. The Ministry of Culture cooperates with the academic sector to research various aspects of NPOs, including the numbers and features of various aspects of the sector. The PST annual threat assessments consider aspects of the NPO sector's vulnerability to terrorism and TF, particularly risks for NPOs to be used domestically for collection and provision of funds and material support for terrorism. The PST identifies that these higher risk groups do not control many resources or a significant share of the sector's international activities. The MFA periodically identifies vulnerabilities of the network of larger NPOs which are active in charitable and human rights activities outside of Norway, including TF risks in conflict zones and terrorism-prone areas.

a4.41. **Criterion 8.2** – There has been outreach to NPOs, however this has varied across the sector. The MFA periodically conducts outreach to the network of larger NPOs which are active in charitable and human rights activities outside of Norway. In 2012, the MoJ published the *"Guide on how to avoid terrorist funding: Your contribution can be misused"* and circulated it in Norwegian and several other languages spoken by minority groups in Norway. Norway has included a number of NPO umbrella organisations in the working group to assess the problems with illegitimate charitable fundraising (including for TF) and possible measures to ensure the NPO sector is not misused, including for TF. The PST has an ongoing and targeted outreach to NPOs and relevant organizations, also in collaboration with some selected police districts.

a4.42. **Criterion 8.3** – Norway has pursued policies to promote transparency, integrity and public confidence in the administration of NPOs through a range of mostly voluntary measures. Foundations are required to register with the Registry of Foundations. While there are no mandatory requirements for other NPOs to register, policies support NPOs registering on a voluntary basis with the Register of Non-Profit Organisations and the Central Coordinating Register for Legal Entities due to incentives including favourable taxation treatment and public funding. The collection of funds in Norway is not regulated. There is a voluntary register for fundraising, supervised by the Foundation Collection Control in Norway. All registers contain essential governance information on NPOs which are publicly available.

a4.43. **Criterion 8.4** – The network of larger NPOs (charitable and human rights activities) which account for (i) a significant portion of the financial resources under the control of the sector; and (ii) a substantial share of the sector's international activities (both fund raising or delivering in higher risk areas off-shore) are predominantly funded by the Norwegian government through the MFA. In such cases, these NPOs have to report on the use of the received means, and subject themselves to control measures. Large NPOs receiving government funds have to comply with auditing and accounting legislation, and those which are registered for tax-free status are subject to controls from the tax authority. The MFA, through the Foreign Service Internal Control Unit (FSCU), together with The Norwegian Agency for Development Cooperation (Norad), controls the use of bilateral international development assistance by requiring public information, financial statements of income and expenditure, financial accountability, licensing or registration, "know your beneficiaries and associated NPOs" and record keeping. Associations which do not receive public funding are not, in general, required to implement the controls and standards set out in c.8.4.

a4.44. **Criterion 8.5** – Given the largely voluntary nature of registration of NPOs in Norway, sanctions appear to be limited to removal of benefits accruable to NPOs, including halting (public) funding and removal of tax-exempt status. It is not clear that the legislation explicitly provides for measures to sanction cases of non-compliance by measures which may extend to freezing accounts, removal of trustees, fines or de-licensing. De-registration is an available sanction, as is a publication of untrustworthy fundraisers on the website of the Foundation Collection Control in Norway: www.innsamlingskontrollen.no.

a4.45. **Criterion 8.6** – The normal law enforcement measures would apply in any investigation or prosecution of an NPO. Additionally, foundations can be investigated by the Foundation Authority.

a4.46. **Criterion 8.7** – International requests are handled through the international network of the Norwegian Police Security Service and other relevant forms of international cooperation.

a4.47. **Weighting and conclusion:** Norway has implemented measures which generally meet the criteria for R.8. However, a few technical deficiencies remain, including those relating to available sanctions (c.8.5). **Norway is rated LC with R.8**.

5. PREVENTIVE MEASURES

Preamble: Scope of Financial institutions

a5.1. The following types of financial institutions are licensed, supervised and authorised to operate in Norway and are subject to the AML/CFT requirements contained in the MLA and MLR: savings banks, commercial banks, finance companies and mortgage companies, life and non-life insurance companies, investment firms, e-money institutions, postal giro offices, payment institutions, management companies for securities funds and branches of foreign financial institutions. These FIs engage in the 13 types of financial activities and operations as defined in the FATF Glossary. FX spot trading is not covered by the MLA, but this is such a narrow issue that it has been discounted.

Recommendation 9 – Financial institution secrecy laws

a5.2. In its 3rd MER, Norway was rated C on the requirements concerning secrecy laws (see paras. 242-247), and the regime was considered to be fully compliant.

a5.3. **Criterion 9.1** – A duty of confidentiality is imposed by statute on officers, employees or auditors of savings banks, commercial banks, management companies for securities funds, the parent company in a financial group, insurance companies, financial and e-money institutions, finance and mortgage companies and investment firms.[1] In essence, the duty is to maintain the confidentiality of any information concerning the customer which comes to the knowledge of the employee by virtue of their position. However, disclosure is permitted if this specifically prescribed by law e.g. to report suspicious transactions to ØKOKRIM as required under *MLA* s.7. Section 11 of the *MLA* specifically provides that this does not constitute a breach of the duty of secrecy, and moreover allows financial institutions and insurance companies to exchange customer data if this is a necessary step in investigating suspicious transactions. This appears to be a useful provision, and it is recommended that Norway extend this to other types of financial institutions, and for other purposes such as compliance with recommendations 13, 16 and 17. Financial institutions indicated that the confidentiality requirements prevent them from exchanging customer data and risk information within a financial group, other than in the context allowed under s.11. Competent authorities such as the FSA and ØKOKRIM can access and share (both domestically and internationally) information held by reporting entities when they need to.

a5.4. **Weighting and conclusion:** Norway only has one deficiency relating to the lack of clarity in regards to sharing of information, in particular within financial groups. **Norway is rated LC with R.9**.

Customer due diligence and record-keeping

Recommendation 10 – Customer due diligence

a5.5. In its 3rd MER, Norway was rated PC on CDD requirements (see paragraphs 203-223). The main deficiencies related to a lack of requirements concerning customers that were legal persons or arrangements, beneficial ownership, and obligations for higher risk customers. CDD obligations were significantly enhanced with the legislative changes in 2009 with additional measures concerning beneficial owners, the purpose and nature of the business relationship, monitoring of customer relationships, and conducting enhanced due diligence for some categories of high risk customer. This was considered sufficient in the 4th FUR to amount to the equivalent of an LC.

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

a5.6. **Criterion 10.1** – Reporting FIs are not allowed to register anonymous accounts or accounts in fictitious names due to the requirements in the *MLA* s.7 & 8 to identify and verify customer identity.

a5.7. **Criterion 10.2** – Reporting FIs are required to apply CDD measures when (a) establishing customer relationships (defined as the point when the customer can use the services of the reporting FI), (b) conducting occasional transactions involving NOK 100 000 (EUR 13 000) or more (including multiple linked transactions), c) there is a suspicion that a transaction is associated with proceeds of crime or TF offences, or (d) there is a doubt as to whether previously obtained data concerning the customer are correct or suffice: *MLA* s.6. However, there is no additional obligation to conduct full CDD when carrying out occasional transactions that are wire transfers as covered by R.16. Norway has applied *EC Regulation 1781/2006* on payer information accompanying funds transfers. This requires that for single or multiple occasional transactions above EUR1 000, information on the payer must be obtained and verified however there is no obligation regarding the other aspects of the CDD process e.g. to identify any beneficial owner: MLR s.20.

a5.8. **Criterion 10.3** – One component of the CDD measures required under s.6-8 is that permanent and occasional customers (when required - see above) must be identified and there must be verification of the customer's identity on the basis of a valid proof of identity: *MLA* s.7. The identity documents must be original documents, issued by a public authority or other body that has a satisfactory and generally accepted level of security concerning the issuance of documents: *MLR* s.5. The document must contain full name, signature, photo and personal ID number or D number (or if the person does not have such a number then the date of birth (DOB), place of birth (POB), sex and nationality). Examples of documents that meet the requirements include a valid passport or other approved travel document, a Norwegian Bank ID (a widely used ID card issued by banks based on a passport or another form of original ID), and a Norwegian driving licence (these have the identifying information referred to above). Requirements for legal persons and arrangements are dealt with in c.10.9 below.

a5.9. It should be noted that the MLA allows verification to be done on a basis other than valid proof of identity if the reporting FI is sure of the customer's identity. FSA guidelines suggest that this exemption can be applied if the FI employee knows the customer personally or the customer relationship is of a "certain duration". However, it also states that absolute certainty of identity is needed. This seems potentially open to abuse, although *MLA* s.5(2) does require that reporting FIs must be able to demonstrate that the extent of the measures is commensurate with the risk. In addition the system for verifying identity in cases where accounts are opened non-face to face (potentially higher risk) has a weakness regarding use of certified copies of ID documents. The FSA Guidance allows such certification to occur in several ways, and one valid method is for two persons who are of age and Norwegian residents to sign and date the copy and provide some contact information. This does not appear to provide any safeguard against abuse.

a5.10. **Criterion 10.4** – This was a deficiency noted in the MER, and Norway introduced a requirement in 2009 that reporting FIs must obtain documentation, e.g. written power of attorney, certifying that the natural person has the right to represent a customer that is a legal person, and must identify and verify their identity using valid proof of identity: *MLA* s.7. Reporting FIs are also now required to identify any persons acting on behalf of a customer, on the basis of a valid proof of identity using a document, issued by an authorised body, and which contains the representative's full name, signature, photograph and personal ID number. They should, for control purposes, explicitly ask customers whether they are "acting" for someone else.

a5.11. **Criterion 10.5** – Reporting FIs are required to take reasonable measures to verify the identity of beneficial owners: *MLA* s.7. Beneficial owners are generally 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" *MLA* s.2). This general definition is then further elaborated by adding five situations (as per those listed in *Directive 2005/60/EC* Art.3 No. 6a-b), where a person "in all cases" is to be regarded as a beneficial owner. Verification on the basis of "reasonable measures" means that it is to be conducted on a risk sensitive basis: *MLA* s.5.

a5.12. **Criterion 10.6** – Reporting FIs are required to gather information concerning the purpose and intended nature of the customer relationship when applying CDD measures: MLA s.7.

a5.13. **Criterion 10.7** – Pursuant to *MLA* s.14, reporting FIs are required to conduct on-going monitoring of existing customer relationships and ensure that transactions are consistent with their knowledge of the customer and its activities. Financial institutions (as defined *FI Act*) (though not other types of reporting FIs) are also required to have electronic surveillance systems as part of their internal control mechanisms: *MLR* s.18. There is an obligation on reporting FIs to update documents and information on customers when the reporting FI has doubts about previously obtained information: *MLA s.14*.

a5.14. **Criterion 10.8** – There is no clear obligation, either in law or enforceable means, for reporting FIs to have a broader understanding of a customer's business and its ownership and control structure, though some elements might be implied e.g. from the beneficial ownership or RBA requirements.

a5.15. **Criterion 10.9** – For legal persons the precise nature of the requirements depend on whether the legal person is registered, and if so in which register – primary corporate registers are the Register of Business Enterprises, Central Co-ordinating Register for Legal Entities. The Central Co-ordinating Register (CCR) is the base register that obtains key information on all legal persons, including entities registered in the Register of Business Enterprises, the Register of Foundations etc., and this information is then a source for other registers. It has the following types of information recorded: organisation number; business name; address; organisational form; type of business/industry; memorandum and articles of association; date of formation/ foundation; details of general/business; partnership or ownership information (where relevant); board members; accountant/auditor; persons empowered to sign for the entity; the Norwegian representative (if foreign entity); information on the business group and ownership (if relevant) and on branches etc. It appears that adequate information is recorded in this register and that the different types of identifying information must be provided and verified under *MLR* s.7-8. The powers to regulate/bind the legal person and/or its senior management will either be contained in the articles of association (usually the case) or in a supplementary document if there are additional or delegated powers. Both such types of documents must be provided. A permanent address should be obtained (*MLA* s.8), the various registers also require a "registered address", and Norway has confirmed that a permanent place of business is information that is required in all registers.

a5.16. **Criterion 10.10** – As regards beneficial owners the MLA copies the requirements of *3AMLD*, and the definition sets out five specific situations where natural persons having an ownership or control interest in a legal person as beneficial owners must be identified and reasonable measures taken to verify their identity and status as beneficial owners. As in *3AMLD* the requirement applies where that interest is 25% or more. Paragraphs (a) and (b) of the definition of beneficial owner refer to:

1. 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);
2. a natural person who exercises control over the management of a legal entity.

a5.17. These requirements to identify and take reasonable measures to verify appear to be broadly in line with the requirements of c.10.10. As regards companies, paragraph (a) is broadly worded and would cover persons that have a beneficial ownership interest either through share ownership in the company or through their control over a person that had such ownership, while paragraph (b) seems broad enough to cover persons exercising control over or through the company management. In addition, as noted above, senior management is identified as part of the customer identification process. Guidance issued by the FSA clarifies and gives beneficial ownership examples.

a5.18. The listed company exception is however problematic, since it automatically exempts all entities with financial instruments listed on a regulated market in an EEA state or equivalent requirements in other countries. There is an assumption that all EEA states (and other equivalent countries) have requirements to ensure adequate transparency of beneficial ownership.

a5.19. As regards other types of legal persons, such as foundations or partnerships, the paragraphs (c)-(e) of the definition, which also follow *3AMLD*, appear to be sufficiently broadly worded to cover the three step ownership and control process set out in c.10.10:

1. a natural person who is the beneficiary of 25% or more of the assets of a foundation, trust or corresponding legal arrangement or entity;
2. a natural person who has the main interest in the establishment or operation of a foundation, trust or corresponding legal arrangement or entity; or
3. a natural person who exercises control over more than 25% of the assets of a foundation, trust or corresponding legal arrangement or entity.

a5.20. **Criterion 10.11** – Norwegian law does not allow for the creation or recognition of trusts or other legal arrangements, however trustees (and similar persons under other legal arrangements) of trusts formed under foreign laws may reside in Norway and conduct transactions related to the trust. The beneficial ownership requirements noted above apply. Paragraph (e) covers trustees, and potentially also protectors (although there is no guidance on this issue), who by their function exercise control over trust assets, while paras.(c) and (d) cover identified beneficiaries with a (vested) interest in 25% or more of the assets of the trust. Arguably, paragraph (d) might also cover settlors as persons that have the "main interest" in the establishment of a trust. However not all beneficiaries are covered, and there is no requirement or mechanism whereby these categories of persons must be identified and their identity verified. Moreover there are no specific provisions concerning the information that must be obtained when the beneficiaries of a trust are designated by characteristics or by class.

a5.21. **Criterion 10.12** – There are no specific provisions requiring beneficiaries of life and investment related insurance policies to be identified. Where such beneficiaries are also customers or beneficial owners then the requirements set out above would apply, but if that is not the case then the law is silent. There is a specific provision on the timing of due diligence that allows the identity of a beneficiary of a life insurance policy to be verified after a policy is taken out provided it is done before the payment of any benefit or the exercise of any rights under the policy. However, as noted above, CDD requirements apply only to customers, whether permanent or occasional (above NOK 100 000 (EUR 13 000)), and beneficial owners. Norway considers that the beneficiary of a pay-out under a life insurance contract is also covered under the occasional transactions requirements. However, the legislation refers explicitly to customers: *MLA* s.6-7. There are no specific requirements relating to information on life insurance beneficiaries which are designated by class or other means.

a5.22. **Criterion 10.13** – There are no provisions requiring the consideration of risk factors relating to the beneficiary of a life insurance policy, when applying enhanced CDD, and no specific requirement to identify or verify the identity of the beneficial owner of the beneficiary. The only obligations are those relating to the obligation to conduct enhanced CDD when a transaction has a high ML/TF risk: *MLA* s.15.

a5.23. **Criterion 10.14 & 15** – The general obligation is that CDD measures shall be applied prior to the establishment of a customer relationship or carrying out of a transaction: *MLA* s.9. A relationship is established when the services of the reporting FI can be used: *MLA* s.2. There are three exceptions:

1. verification is allowed during the establishment if this is necessary to avoid "prevention of general business operations" and there is little risk of ML/TF. This seems consistent with c.10.14 since it is only extends the timing to "during" the establishment. However, FSA Guidance allows PEPs checks and the related enhanced due diligence measures to be done without undue delay but after the relationship is established. The basis is that such customers might be entering the relationship by phone or internet. This seems neither "necessary" nor is risk taken into account.
2. the life insurance exception noted above, which is satisfactory in principle.

3. verification is allowed after a bank account is opened provided that the account cannot be used for transactions until verification occurs, which appears to be satisfactory since in essence the ability to conduct transactions on an account is the point at which the relationship is established.

a5.24. MLR s.8 allows legal persons that are registered in any Norwegian register to produce proof of identity with six months after the establishment of the business relationship, however this is in fact restricted to situations concerning newly incorporated companies which need a bank account to receive initial share subscriptions and which can't use the account for purposes other than to receive such funds until CDD requirements are fulfilled.

a5.25. **Criterion 10.16** – In the 3rd MER the lack of legal measures regarding existing customers was found to be a deficiency. In the 2009 *MLA* Norway responded by adding requirements to conduct on-going monitoring (*MLA* s.14) and to update customer documentation and information when there are doubts (*MLA* s.6). As noted in the 4th FUR the provisions are not fully in line with the concept of applying CDD to existing customers on the basis of materiality and risk at appropriate times. The FSA Guidance refers to the above sections and suggests it is not necessary to renew the CDD on all customers or beneficial owners. It also indicates that where the identity of a customer was verified under the 2003 *MLA*, the risk may generally be assumed to be low, although there does not appear to be any basis for such an assumption. Thus, although some measures have been introduced, the timing of the obligation to update customer information is not specified, and the requirements only partially address the FATF requirements.

a5.26. **Criterion 10.17** – As noted in the 4th FUR, reporting FIs must apply "other customer due diligence measures", in addition to the basic CDD measures stipulated in MLA, to: (a) situations involving a "high risk of transactions associated with proceeds of crime" or TF and terrorism offences; (b) business relationships and transactions with foreign PEPs; and (c) correspondent banking relationships (*MLA* ss. 15-16). FSA's guidelines provide some additional examples, including cross references to the 2004 FATF Methodology, although these are not as extensive as those set out in the new FATF Standards. Enhanced CDD is required but some concerns remain: as a matter of language, the concept of "high risk transactions" is somewhat narrower than the "higher risk" requirements in R.10, and this is not offset by guidance that gives a broader interpretation. In addition, as noted in the 4th FUR the nature of the "other CDD measures" to be taken in such circumstances is not further elaborated.

a5.27. **Criterion 10.18** – MLA s.13 is headed *simplified CDD measures*, but provides that regulations can be published allowing exceptions to the obligation to conduct CDD. *MLR* s.10 provides that CDD requirements do not apply to certain types of customers or products (unless there is a suspicion of ML/TF), based upon *3rd AMLD* Art.11. The only requirement for reporting FIs is to obtain sufficient information to make sure that the circumstances are covered, although Norway observes that reporting FIs must still conduct a risk assessment under *MLA* s.5, including with respect to the customers/products that are exempted. However, the requirement in the FATF Standards is that the country can only create exemptions from AML requirements under R.10 (including with respect to CDD) if the preconditions (which include showing proven low risk) have been met. Those conditions have not been met and thus the legislative scheme of exemptions, which is different from having simplified measures, is not consistent with c.10.18.

a5.28. **Criterion 10.19** – MLA s.10 provides that if CDD cannot be applied then reporting FIs shall not establish a customer relationship or carry out the (occasional) transaction. An established customer relationship shall be terminated if continuing the relationship entails a risk of transactions associated with ML/TF. This latter requirement is not in line with the Standards, which require that relationships be terminated in all cases where CDD cannot be completed. There is also no specific requirement to consider making an STR in such circumstances.

a5.29. **Criterion 10.20** – There is no provision that allows reporting FIs not to perform CDD if this would result in the customer being tipped off.

a5.30. **Weighting and conclusion:** Norway has enacted the core CDD requirements, such as identifying and verifying customer identity and the beneficial owner, in line with the 2003 FATF Standards. However there are a significant number of smaller deficiencies such as those relating to risk, to life insurance beneficiaries

and to understanding the customer's overall business and control/ownership structure. Most of these are new requirements added in the 2012 Standards. **Norway is rated PC with R.10**.

Recommendation 11 – Record-keeping

a5.31. In its 3rd MER, Norway was rated C with previous record-keeping requirements (see paragraphs 248-253). Although neither the laws nor the FATF Standards have changed, certain deficiencies have been noted in relation to the keeping of transaction records.

a5.32. **Criteria 11.1 & 11.3** – Obligations concerning the keeping of transaction records are set out in the *Bookkeeping Act 2004 and Regulations* (which apply to all types of businesses). Sections 4-6 of the Act, read with the Regulations, appear to impose requirements to keep complete transactions records. Such records must be retained for five years. Although generally worded, the preparatory works and other documents showed that transactional records need to be kept in sufficient detail so that individual transactions can be reconstructed. Such records are available in practice to competent authorities.

a5.33. **Criterion 11.2 –** The documents used to verify the data required to be obtained under *MLA* s.7-8 (customer identification, beneficial ownership information and information on purpose and use) must be retained for five years after termination of the customer relationship or after an occasional transaction is carried out, unless longer periods are required by other laws (*MLA* s.22). This would also include any updated records obtained under *MLA* s.14. Although there is no explicit requirement to retain records created as part of on-going monitoring, there is a requirement to retain records that are created when (or which relate to) examining transactions to confirm/disprove a suspicion of ML/TF under *MLA* s.17. These records must be retained for five years after the transaction is carried out. This appears to require records to be maintained on any analysis conducted, but this is only for five years after the transaction(s), and not five years after the termination of a business relationship as required. If such analysis relates to occasional transactions, it would be necessary that all transactions and records that are related to the potentially suspicious activity should be retained for five years after the date of the most recent relevant transaction analysed. There is no requirement in the *MLA* to retain records of account files or business correspondence. All these documents must be destroyed within one year after expiry of the retention period: *MLA* s.22.

a5.34. **Criterion 11.4** – Pursuant to *MLA* s.25, reporting FIs must have systems that enable them to provide rapid and complete responses to enquiries from ØKOKRIM or supervisory authorities concerning specific customers or types of customers. Electronic data should be stored in an easily accessible location in order to permit checking, organised in a manner that permits efficient follow-up, properly secured to prevent damage and alteration, and be available on a timely basis.

a5.35. **Weighting and conclusion:** The only concern is that the requirement to keep records of analysis is for five years from the date of analysis (not the date of termination of a relationship). **Norway is rated LC with R.11**.

Additional Measures for specific customers and activities

Recommendation 12 – Politically exposed persons

a5.36. In its 3rd MER, Norway was rated non-compliant with old R.6 as it had no AML/CFT measures concerning politically exposed persons (PEPs); see paragraph 224. Since then, Norway has introduced requirements relating to PEPs in the *MLA* and *MLR*.

a5.37. **Criterion 12.1** – The *MLA* establishes measures concerning the establishment of customer relationships with foreign PEPs. A PEP is defined as a natural person who holds or held during the last year a high public office or post in a state other than Norway and their immediate family members and close associates: *MLA* s.15; *MLR* s.11. The *MLR* defines 'close associate' as a person: i) who is known as a beneficial

owner in an entity jointly with a PEP; or ii) who has close business connections with a PEP. The *MLR* further describes what is meant by 'holder of high public office or post' as a range of high-ranking positions listed: *MLR* s.11. This includes Heads of State and Ministers; members of national assemblies; members of the highest courts; members of the board of auditor bodies; high-raking diplomats and military officers; and members of an administrative, managerial or controlling body of state-owned organisations. It is a concern that the application of the enhanced due diligence requirements outlined in the MLA only apply to foreign PEPs who have held a high public office or post during the previous year. This seems to be too prescriptive and the prescribed timeframe of 1 year is not in line with an RBA, and is not sufficient to meet the definition of a PEP in the FATF Glossary which includes individuals 'who are or have been' in the prescribed roles.

a5.38. Reporting entities are required to conduct 'appropriate CDD measures' to establish whether customers are PEPs: *MLA* s15. For customers that are PEPs, the measures to be taken are: 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 iii) carrying out enhanced on-going monitoring: *MLA* s.15. The PEP requirements refer explicitly to the customer, and although the concept of "close associate" (see above) includes the beneficial owner of a legal person/arrangement customer where the PEP is the beneficial owner or jointly owns: *MLR* s.11. This does not include PEPs that are beneficial owners behind individual customers. Moreover the FSA Guidance expressly states that PEPs that are beneficial owners are not covered by the PEPs requirements.

a5.39. **Criterion 12.2** – The definition of PEP includes a holder of an office or post in an international organisation which corresponds to the high-ranking positions outlined in the *MLR* s.11. However, this approach is not satisfactory and has limitations as the government positions in the list do not correspond well to the concept of senior management positions in an international organisation. Reporting entities must comply with the same obligations for international organisation PEPs as they do for foreign PEPs, including the limitation regarding beneficial owners as identified in c.12.1. Norway does not have any measures relating to domestic PEPs.

a5.40. **Criterion 12.3** – As noted at 12.1, the definition of a PEP in the MLA includes immediate family members and close associates and reporting entities are required to apply the same requirements: *MLA* s.15. Including family members and close associates themselves as PEPs under the MLA creates a confusing and circular definition. As noted, Norway does not have any measures relating to domestic PEPs.

a5.41. **Criterion 12.4** – Norway does not have any specific measures in place in relation to life insurance policies and PEPs.

a5.42. **Weighting and conclusion:** While Norway has measures in place for foreign PEPs, there are no laws covering domestic PEPs, and the measures relating to international organisation PEPs are limited. Other technical deficiencies also exist regarding the narrow definition of PEP and requirement given the timeframe of the past 12 months in the absence of an RBA, and absence of measures for PEPs that are beneficial owners of individual customers. **Norway is rated PC with R.12**.

Recommendation 13 – Correspondent banking

a5.43. Norway was rated NC with correspondent banking requirements, and PC on shell banking. The main deficiencies were a lack of measures concerning establishment of cross-border correspondent banking relationships, and deficiencies regarding relationships with shell banks. The 2009 *MLA* introduced specific requirements on these points, and despite a remaining shortcoming (relating to the lack of application of correspondent banking requirements when entering into such relationship with institutions in other EEA-countries), the 4th FUR concluded that Norway had reached a level equivalent to LC on both recommendations (see 4th FUR paragraphs 68-76).

a5.44. **Criterion 13.1** – Although the requirements introduced in the 2009 *MLA* mirror those of R.13, the scope of application is limited to respondent credit institutions located outside the EEA and not to any other type of FIs, nor does it cover credit institutions within the EEA.

a5.45. **Criterion 13.2** – *MLA* s.16 requires that, in relation to settlement accounts, credit institutions ascertain that the respondent credit institutions[2] have verified the identity of and perform on-going monitoring of customers having direct access to accounts at the credit institution, and is able upon request to provide relevant due diligence data to the credit institution. Although the requirements mirror those of R.13, their scope of application is limited to respondent institutions located outside the EEA.

a5.46. **Criterion 13.3** – *MLA* s.16 prohibits credit institutions from entering into or from continuing correspondent banking relationships with shell banks. It also requires 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.

a5.47. **Weighting and conclusion:** The key remaining deficiency is that the measures described under c.13.1-2 do not apply to credit institutions within the EEA. This is a concern given that the large majority of the corresponding banking relationships are within the EEA. **Norway is rated PC with R.13**.

Recommendation 14 – Money or value transfer services

a5.48. Norway was rated PC with these requirements in the 3rd MER (see paragraphs 334-336). Since then, Norway has amended its laws for MVTS providers who are now regulated entities under *MLA* and subject to authorisation and AML/CFT requirements.

a5.49. **Criterion 14.1** – Providers of payment services are required to have authorisation from the FSA: *FIA* s.4b-2. The definition of payment service includes the provision of money remittances which meets the definition of MVTS in the FATF Glossary: *FCA s.11(1)(d)*. Entities must have authorisation to carry on business as a payment institution, which includes a fit and proper test: *FIA* s.2-4 and Chapter 4b. This means that the FSA will make an assessment of the owner's fitness and propriety to assure proper and adequate management of the entity and its activities. The FSA may also grant a limited authorisation for MVTS providers, which allows the FSA to waive some of the general rules required for authorisation of payment institutions: *FIA* s.4b-3. The limited authorisation creates limits on total transaction amounts per month, and involves an assessment of the provider's AML/CFT policies and procedures and of the fitness and propriety of the management and operation of the entity.

a5.50. In line with the *PSD*, Norway allows payment institutions authorized in other EEA countries to establish and carry on business through a branch or agent, or carry on cross-border activities in Norway without further authorisation: *FIA* s.4b-1. This is on condition that the entity is authorised to carry on business in its home country, and is subject to supervision by the competent authority in that country. Such payment institutions are registered with the FSA, in accordance with the *Regulations on Payment Services, Chapter 10*. In order for an entity located in another EEA country to register a branch, or an institution providing cross-border services or providing payment services through agents in Norway, the home supervisor must provide to the FSA the institution's name, address, name of the person responsible for the branch, its organisational structure and services it will provide. To register agents, the home supervisor must also provide a description of the internal control AML/CFT mechanisms and evidence that the directors and management of the agent are fit and proper persons.

a5.51. **Criterion 14.2** – Carrying out unauthorised MVTS is a breach of the FIA, punishable by fine or imprisonment of up to 1 year: *FIA s.5-1*. The Police Districts are responsible for identifying and sanctioning unauthorised MVTS providers. The police and FIU have taken some action to identify unauthorised providers as part of their work, as they have come across such providers as part of investigations or through STRs. Norway provided two examples where sanctions have been applied, and indicated that other cases are ongoing. However, this is not carried out on a regular or systematic basis.

2 Note that *MLA* s.16 refers to "correspondent" rather than "respondent" credit institutions. However, the authorities confirm that the reference should be read to mean "respondent".

a5.52. **Criterion 14.3** – The FSA is the authority responsible for monitoring the compliance of MVTS providers with AML/CFT obligations. Authorised MVTS providers are subject to off-site supervision including reporting to the FSA on a semi-annual basis on their monitoring and reporting obligations. In addition, the MVTS providers that receive a limited authorisation are obliged to renew their authorisation every two years which includes an assessment of their AML/CFT procedures. However, the FSA has not undertaken any on-site inspections of MVTS providers.

a5.53. Branches and agents in Norway of MVTS providers from the EEA are subject to the *MLA*, pursuant to ss.3-4, and are therefore required to comply with Norway's AML/CFT requirements. However, the FSA does not monitor for AML/CFT compliance: MVTS branches and agents, nor MVTS providers located in other EEA countries that offer services in Norway. Under the EU Payment Services Directive, this falls under the obligation of the home Member State of the payment institution when the home Member State asks for administrative cooperation or when the payment institution operates under right of establishment. On two occasions, the FSA was informed by the FIU of concerns relating to compliance with AML/CFT measures (including on CDD, STRs and training of agents) of international MVTS networks. In these instances the FSA, in consultation with the FIU, arranged and participated in several meetings with compliance personnel of these networks. In addition, the FSA informed home supervisors through correspondence and meetings. However, home supervisors do not undertake supervision of these agents and branches, and no action was taken by the home supervisors in response to the concerns raised by Norway. Norway sought to enter into a supervisory agreement with one of these home supervisors regarding these MVTS providers; although no agreement was entered into.

a5.54. **Criterion 14.4** – Authorised MVTS providers are required to receive approval from the FSA to operate agents. The FSA keeps an online register of these agents.

a5.55. **Criterion 14.5** – In order to register agents, the authorised MVTS providers' AML/CFT program must include training and monitoring of agents.

a5.56. **Weighting and conclusion:** The lack of monitoring for MVTS providers passported into Norway is a significant concern given that this is a high risk sector and the large portion of the market share that the multinational providers hold (c.14.3). **Norway is rated LC with R.14**.

Recommendation 15 – New technologies

a5.57. In its 3rd MER Norway was rated compliant with previous new payments requirements (see paragraphs 226-231). Since then the FATF standards relating to the risks posed by new technologies have substantially changed and Norway has enacted the *MLA* in 2009.

a5.58. **Criterion 15.1** – Norway has only taken limited steps to identify and assess the risks that may arise in relation to the development of new products and new business practices, including new delivery mechanisms, and the use of new or developing technologies for both new and pre-existing products. Norway recently undertook its first national risk assessment which included consideration of some of the risks posed by new technologies, such as the risks posed by virtual currencies and new payment systems. In addition, Norway considered to a limited extent the risks posed by new technologies in the 2011 ML trends report. However, while the NRA identified some threats relating to new technologies, the concerns outlined above in R.1 regarding the level of assessment also apply here. There is no specific requirement for all reporting entities to identify and assess the risks posed by new technologies. Rather, there is the general obligation on reporting entities to apply CDD on the basis of risk, including where risk is assessed on the basis of the customer type, customer relationship, product or transaction: *MLA* s.5.

a5.59. **Criterion 15.2** – There are no specific requirements for all reporting entities to undertake risk assessments prior to the launch or use of new products, practices and technologies, nor to take appropriate measures to manage and mitigate the risks. There are general requirements to assess risks and implement related measures under the *Regulation on Risk Management and Internal control*, which include in relation to new events (such as new products) before activities commence. However, these regulations are not related to ML/TF risk and refer generally to 'risks and capital requirements'. Norway considers that ML/TF risks

are amongst the risks which must be assessed and mitigated pursuant to these regulations; however, it is not clear whether the regulations are relevant for the purposes of ML/TF risk as the regulations nor the associated guidance do not refer to ML/TF risk, and they were not provided to the assessment team until after the on-site visit. CDD requires copies of certified documents for non-face-to-face verification of identity. Where a person's identity is to be verified through non-face-to-face means on the basis of 'physical proof of identity', the reporting entity is required to obtain further documentation to verify identity. The FSA advises reporting entities that in such cases, certain parties can certify copies: *FSA Guide* 2.9.1. The reporting entity should seek further documentation if it has doubts to compensate for the increased risk of the customer's non-appearance. If obtaining further information does not dispel the doubt, the customer relationship must not be established except by personal appearance.

a5.60. **Weighting and conclusion:** Norway has not met R.15 as it has not adequately assessed risks associated with new technologies and there are no clear requirements on reporting entities to address these risks. **Norway is rated PC with R.15**.

Recommendation 16 – Wire transfers

a5.61. Norway was rated NC with the requirements regarding wire transfers in the 3rd MER (see paragraphs 254-260). However, since the 3rd MER Norway has enacted s.20 of the *MLR* which transposed into Norwegian law the *EU Regulation on wire transfers (1781/2006/EC)* of 15 November 2006 (the EU Regulation). The EU Regulation applies to transfers of funds, in any currency, which are sent or received by a payment services provider (PSP) established in the EEA: Art.3. A PSP is defined as a natural or legal person whose business includes the provision of transfer of funds services: Art.2(5).

a5.62. **Criterion 16.1** – The payer's PSP (the ordering financial institution) is required to ensure that transfers of funds are accompanied by complete payer information consisting of the name, address, and account number: Art.4-5. The address may be substituted with the date and place of birth of the payer, a customer identification number, or national identity number. Where the payer does not have an account number, the PSP is required to substitute it with a unique identifier which allows the transaction to be traced back to the payer. For transfers of EUR 1 000 or more, the payer's PSP is also required to verify the complete payer information on the basis of documents or information obtained from a reliable and independent source: Art.5(2). This includes several smaller transactions that appear to be linked. Transfers outside the EEA must be accompanied by complete information on the payer: Art.7. For transfers within the EEA, only the account number of the payer or a unique identifier is required to accompany the wire transfer: Art.6. For the purposes of R.16, wire transfers entirely within the EEA are considered to be domestic wire transfers. There is no requirement in the EU Regulation for the ordering institution to include the required beneficiary information.

a5.63. **Criterion 16.2** – For batch files from a single payer, where the payee's PSP is outside the EEA the complete information should not be required for each individual transfer, if the full information accompanies the batch and each individual transfer has an account number or a unique identifier: Art.7(2). There is no requirement in the Regulation in relation to beneficiary information.

a5.64. **Criterion 16.3** – The payer's PSP is required to ensure that transfers of funds are accompanied by complete payer information, including for transfers under EUR 1 000: Art.5. There is no requirement in the EU Regulation for the ordering institution to include the required beneficiary information.

a5.65. **Criterion 16.4** – Under the EU Regulation, the payer's PSP, before transferring the funds, is required to collect, but not verify, the complete information on the payer on the basis of documents, data or information obtained from a reliable and independent source for transfers under EUR 1 000, unless the transaction is carried out in several smaller transactions that appear to be linked: Art.5(4). However, as a reporting entity, the ordering institution is required to apply CDD measures to their customer (the originator), including verification of the customer's identity, when there is a suspicion of ML/TF or when there is doubt as to whether the customer's data is correct: *MLA* s.6(3)-(4).

a5.66. **Criterion 16.5 and 16.6** – The EU regulation makes a distinction for transfers where both the payer PSP and payee PSP are located in the EEA. For such transfers, only the account number or the unique identifier

allowing the transaction to be traced back to the payer need accompany the transfer, provided that complete payer information can be provided within three working days of a request from the payee's PSP: Art.6(2). There is a concern that the definition of transfers within the EEA in the Regulation at Art.6(1) is wider than that permitted as a domestic transfer in R.16. This definition includes a chain of wire transfers that takes place entirely within the EU. However, Art.6(1) only refers to the situation where the PSP of the payer and the PSP of the payee are situated in the EEA. This means that where an intermediary institution is situated outside the EEA, this may be considered a transfer within the EEA under the Regulation, but not a domestic transfer under R.16.

a5.67. **Criterion 16.7** – The payer's PSP is required to keep records of complete information on the payer which accompanies transfers of funds for five years: Art.5(5). There is no requirement to maintain beneficiary information collected.

a5.68. **Criterion 16.8** – The payer's PSP must comply with the requirements outlined above before transferring funds. Each member state is required to law down the rules on, and apply, penalties for infringements: Art.15(1). In Norway, failure to comply with the Regulation is a breach of the *MLR* at s.20 which transposes the EU Regulation and the sanctions, and concerns, outlined in R.35 apply.

a5.69. **Criterion 16.9** – An intermediary PSP (the intermediary financial institution) is required to ensure that all information received on the payer is maintained with the transfer: Art.12. However, there is no requirement to ensure that any accompanying beneficiary information is also retained with it.

a5.70. **Criterion 16.10** – An intermediary PSP inside the EEA, when receiving a transfer of funds from a payer's PSP outside the EEA, may use a payment system with technical limitations (which prevent information on the payer from accompanying the transfer of funds) to send transfers of funds to the payment service provider of the payee: Art.13(1)-(2). This provision applies, unless the intermediary PSP becomes aware that information on the payer is missing or incomplete. In such circumstances, the intermediary PSP may only use a payment system with technical limitations if it is able to inform the payee's PSP of this fact: Art.13(4). In cases where the intermediary PSP uses a payment system with technical limitations, the intermediary PSP has to make available to the payee's PSP, upon request, all the information on the payer which it has received, irrespective of whether it is complete or not, within three working days of receiving that request: Art.13(4). In all cases, an intermediary PSP is required to keep records received for five years: Art.13(5).

a5.71. **Criterion 16.11** – There is no requirement for intermediary institutions to take reasonable measures to identify cross-border wire transfers that lack originator or beneficiary information.

a5.72. **Criterion 16.12** – There is no requirement for intermediary institutions to have risk-based policies and procedures for determining when to execute, reject, or suspend a wire transfer lacking originator or beneficiary information, and when to take the appropriate action.

a5.73. **Criterion 16.13** – The payee's PSP (beneficiary financial institution) is required to detect whether the required information on the payer is missing: Art.8. The payee's PSP is required to have procedures in place to detect: for transfers within the EEA, the account number or the unique identifier; and for transfers from outside the EEA, the complete payer information or for batch files, the payer information in the transfer: Art.8(a)-(c). However, there are no obligations for missing beneficiary information.

a5.74. **Criterion 16.14** – There is no requirement in the Regulation for the payee's PSP to identify the beneficiary if it has not been previously verified, for cross-border transfers of EUR 1 000 or more. Reporting entities are required to conduct CDD on transactions involving NOK 100 000 (EUR 13 000) or more for occasional customers: *MLA 6.2*. However, this threshold is significantly higher than EUR 1 000, and the CDD requirement is focussed on the originator/customer and not on the beneficiary of such a transaction. The record keeping requirements relating to CDD requirements would also apply: *MLA s8*.

a5.75. **Criterion 16.15** – When there is incomplete payer information, the payee's PSP is required to either reject the transfer, or ask for the complete payer information: Art.9. The payee's PSP is also required to consider the missing or incomplete payer information as a factor in assessing whether the transfer of funds, or any related transaction, is suspicious, and whether it must be reported to the relevant authorities: Art.10.

For a payer's PSP who regularly fails to provide information, the payee's PSP should (after giving warnings and setting deadlines) consider rejecting all transfers: Art.9(2). Such termination should be reported to the relevant authorities. However there are no obligations if beneficiary information is missing.

a5.76. **Criterion 16.16** – The Regulation applies to MVTS providers as the definition of payment service provider is a natural or legal person whose business includes the provision of transfer of funds services: Art.2(5). This is consistent with the concept of payment institutions (which includes MVTS) in the *Financial Institutions Act*. Norway has advised that this includes branches and agents of MVTS providers operating in other EEA countries.

a5.77. **Criterion 16.17** – The case of an MVTS provider that controls both the ordering and the beneficiary side of a wire transfer is not specifically addressed in the EU Regulations. An MVTS provider in Norway is required to report a suspicious transaction where it suspects that a transaction is associated with proceeds of crime and that suspicion has not been disproved after further enquiries: *MLA* ss.17 and 18. However, when an MVTS provider controls both the ordering and beneficiary side of a wire transfers, there is no specific obligation to take into account information from both sides. If the suspicion arises in Norway, an STR is required to be filed in Norway but not in any other country affected.

a5.78. **Criterion 16.18** – Norway ensures that reporting entities, when processing wire transfers, take freezing action as required by the targeted financial sanctions for terrorism and TF through a combination of requirements. Norway's guidance on targeted financial sanctions urges reporting entities to monitor the list of the UN Sanctions Committee through their electronic monitoring systems, including the monitoring of wire transfers (a requirement in the *MLA* s.24).

a5.79. **Weighting and conclusion:** The EU Regulations leave significant gaps in the wire transfer requirements as there is an absence of any requirements relating to information on the beneficial owner (c.16.1-3, 16.13, 16.15). Other serious problems include the lack of requirements on intermediary FIs (c.16.11-12). **Norway is rated PC with R.16**.

Reliance, Controls and Financial Groups

Recommendation 17 – Reliance on third parties

a5.80. Norway was rated N/A in the 3rd MER concerning reliance on third parties on the basis that it effectively prohibited reporting entities from relying on third parties to perform CDD. The 2009 *MLA* introduced provisions that allow reporting entities to rely on third parties to perform certain CDD measures. However, the 4th FUR noted deficiencies that remain and are analysed below.

a5.81. **Criterion 17.1** – Norway introduced *MLA* s.11 to allow, under certain conditions, reporting entities to rely on some aspects of the CDD process (verification of identity of customers and beneficial owners, and gathering of information on the purpose and nature of the customer relationship), to be carried out by third parties. The list of acceptable third parties is based around the list of reporting entities, corresponding institutions in EEA countries, or institutions from other states that have statutory registration or licensing obligations and rules on CDD, retention and monitoring corresponding to those applicable in the EEA. The type of third parties upon whom reliance may be placed is thus primarily based on an equivalence test. In so doing, the law clearly stipulates that such reliance does not absolve reporting FIs from their obligations to ensure that CDD measures are applied in accordance with the *MLA*. In addition to reliance on third parties, the *MLA* separately provides for reporting FIs to outsource their obligations to service providers pursuant to written contracts. Most reporting entities and postal operators are allowed to act as service providers: *MLA* s.12.

a5.82. The conditions for allowing such reliance include that the third party make the relevant CDD information available and, when so requested, immediately forward copies of identification data and other documents to the relying reporting FI. The conditions place the obligations on the third party which, in

the case of a third party located outside Norway would be difficult to enforce, rather than on the relying reporting FI to satisfy itself that this data will be made available without delay upon request. There is no requirement for the relying reporting FI to satisfy itself that the third party in Norway has measures in place for compliance with CDD and record-keeping requirements in line with R.10 & 11. This is not fully in line with the requirements of c.17.1, however, the entities permitted to act as a third party are themselves subject to the *MLA*: *MLA* s11. Third parties in other countries must be subject to CDD and record keeping requirements that are equivalent to those in the *MLA*, and subject to supervision: *MLA* s11(1)(11).

a5.83. **Criterion 17.2** – Norway does not impose any limitation on the range of countries where third parties can be relied upon and does not have regard to information on country risk. Despite this, FSA guidance does refer reporting entities to the assessments and other reports issued by the FATF and FSRBs, and encourages financial institutions to have measures in place to satisfy themselves that the third party is regulated and supervised, and has measures in place to comply with CDD requirements. However, this guidance is not binding as it is not law or other enforceable means.

a5.84. **Criterion 17.3** – There are no specific provisions in the *MLA* that would modify the manner in which a relying reporting FI could satisfy the conditions for reliance when a third party is part of the same financial group as the relying reporting FI.

a5.85. **Weighting and conclusion:** Norway's measures to permit the reliance on third parties leave important gaps as FIs are not required to satisfy themselves that the third party has measures in place for CDD and record keeping and can provide documentation upon request. These deficiencies are mitigated by the fact that third parties must be regulated for AML/CFT, yet the absence of any positive responsibility on FIs is an important deficiency. In addition, Norway does not meet c.17.2. **Norway is rated PC with R.17**.

Recommendation 18 – Internal controls and foreign branches and subsidiaries

a5.86. In its 3rd MER Norway was rated LC for both these requirements (paragraphs 302-304). The main deficiencies were that there was no legal obligation on reporting entities to establish screening procedures to ensure high standards when hiring employees; there were concerns about how effectively internal controls had been implemented; and there was no requirement to inform the FSA if their foreign branches or subsidiaries were unable to observe AML/CFT measures because this was prohibited by the host country. Some limited additional measures were included in the *MLA* in 2009 as outlined below.

a5.87. **Criterion 18.1** – Reporting entities are required to have in place satisfactory internal control and communication procedures to ensure compliance with their AML/CFT obligations: *MLA* s.23. Reporting entities must appoint a person of managerial rank to oversee the procedures and take measures to ensure their employees are familiar with AML/CFT obligations, including how to identify and process suspicious transactions. The *MLA* does not require reporting entities to have screening procedures to ensure high standards when hiring employees nor to have an independent audit function to test the AML/CFT system in place. However, certain reporting entities[3] are required to have an independent audit department or internal audit function that reports to an entity's board of directors. Among its responsibilities, is the monitoring of systems of internal control and risk management: *FIA* s.3.11. At reporting entities without an internal audit function, the board of directors must ensure that an external body confirms whether implementation of the internal control system is being monitored.

a5.88. **Criterion 18.2** – None of the essential elements are met, and financial groups are not specifically required to implement group-wide programmes against ML/TF.

a5.89. **Criterion 18.3** – Reporting entities are required to ensure that their foreign branches and subsidiaries are familiar with the internal control requirements, and apply CDD, on-going monitoring and

3 Public credit institutions, public trustee's offices and foundations, management companies, investment firms, certain finance companies, payment institutions and electronic money institutions.

record-keeping measures that are consistent with requirements of the 2009 *MLA*. The law also prescribes measures that branches and subsidiaries should take in the event that local laws do not allow the application of such measures (i.e., to so inform the FSA, and apply other measures to counteract the risk of transactions associated with proceeds of crime or terrorism. However, the scope of application of these requirements is limited to branches and subsidiaries established in states outside the EEA.

a5.90. **Weighting and conclusion:** The restriction of the measures to branches outside the EEA is an important shortcoming given that a large majority of branches and subsidiaries are located within the EEA. There are also concerns with c.18.1 and c18.2. **Norway is rated PC with R.18**.

Recommendation 19 – Higher-risk countries

a5.91. In its 3rd MER, Norway was rated C with the requirements on higher-risk countries (see paragraphs 265-266). R.19 contains new requirements that were not assessed under the 2004 Methodology, but which are assessed under criteria 19.1 and 19.2 of the 2013 Methodology.

a5.92. **Criterion 19.1** – There is no requirement for reporting entities to apply enhanced due diligence, proportionate to the risk, to business relationships or transactions from countries for which the FATF calls to do so. However, reporting FIs are required to apply enhanced CDD in situations that by their nature involve transactions with a high ML/TF risk: *MLA* s.15. The FSA's non-binding guidance specifies that the situation where a transaction is carried out to or from a customer in a country that lacks satisfactory measures to combat ML or TF may prompt FIs to conduct enhanced CDD: FSA Circular 8/2009 s.2.11.1. This means that in practice, reporting FIs would apply enhanced CDD in certain circumstances to mitigate this deficiency. In addition, as described below, the MoF is able to impose restrictions on the activities of REs that include requiring them to apply enhanced CDD, though it has not done so to date and there are no existing requirements: MLR s.16.

a5.93. **Criterion 19.2** – Norway has the power to apply counter-measures against higher risk jurisdictions both in situations called upon to do so by the FATF and independently of any call by the FATF: *MLA* s.33. The Ministry of Finance has issued regulations which can be applied when called upon by the FATF: *MLR* ss.15-16. These regulations impose a special, systematic reporting obligation in relation to customer relationships and transactions and/or special prohibitions or restrictions on establishing customer relationships or conducting transactions. Concrete obligations and/or prohibitions to implement the regulations will be adopted by the MoF in the form of a decision which will be posted on the FSA's website: FSA Circular 8/2009 s.2.11.1.

a5.94. **Criterion 19.3** – Norway ensures that FIs are advised of concerns and weaknesses in the AML/CFT systems of countries that are named by the FATF, through FSA statements published on the FSA's own website as well as on the joint FIU/FSA website (see also R.34 below). In addition FSA guidance refers reporting entities to all the websites of the FATF and FSRBs, which contain assessment and other reports including information on the weaknesses in the AML/CFT systems of other countries.

a5.95. **Weighting and conclusion:** the deficiency in c.19.1 means **Norway is rated LC with R.19**.

Reporting of Suspicious Transactions

Recommendation 20 – Reporting of suspicious transaction

a5.96. In its 3rd MER, Norway was rated LC with these requirements (see paragraphs 269 to 271). The 2013 Methodology added tax crimes as a predicate offence for ML.

a5.97. **Criterion 20.1 & 20.2** – There is a mandatory legal requirement for reporting FIs to report to the FIU suspicious transactions that are related to ML, TF and proceeds of crime more generally: *MLA* ss.17-19 and *MLR* ss.12-13. There is an obligation to further examine transactions that are suspected to be associated with proceeds of crime or TF offences (this suspicion is defined to refer to unusual transactions) to see if

the suspicion is confirmed or disproved: *MLA* s.17, *MLR* s.12. If not disproved then an STR must be filed: *MLA* s.18. They also set out the procedures for submitting STRs and related information to the FIU. The STR reporting obligation applies to both completed and attempted transactions, regardless of the amount. While the limitation in the scope of the TF offence (see R.5 above) could potentially have negative spill-over on the TF related reporting obligation, the reporting obligation is sufficiently broad to require reporting of suspicions relating to the collection of funds in the intention that they are to be used by a terrorist. The reporting obligation applies to transactions associated with the proceeds of crime, which includes a broad range of tax crimes. While more complex than a requirement to report suspicious transactions, the process and its result still appear to be in line with R.20.

a5.98. **Weighting and conclusion: Norway is rated C with R.20**.

Recommendation 21 – Tipping-off and confidentiality

a5.99. In its 3rd MER, Norway was rated C with these requirements (see paragraph 278).

a5.100. **Criterion 21.1** – Reporting FIs and their employees are protected from both criminal and civil liability if information in relation to the reporting requirement is communicated in good faith to the FIU: *MLA* s.20. While the *MLA* does not specifically indicate that this provision equally applies to directors of FIs, the *2009 MLA* preparatory works mention in paragraph 5.4.1 that Art.26 of the *3rd AMLD* and the FATF's previous requirements in this regard include an institution's management and employees. Paragraph 5.4.2 further states that the 2003 *MLA* already provided an exemption from criminal penalties and civil compensation claims when information is provided to ØKOKRIM in good faith. On that basis, it can be concluded that s.20 also applies to reporting FIs' directors.

a5.101. **Criterion 21.2** – Reporting FIs and their officers and employees are prohibited from "tipping-off" a customer or any third party about the fact that an STR or related information is being filed with the FIU: *MLA* s.21. The MLR sets out situations in which the "tipping-off" provision does not apply (e.g. in communications with the prosecuting authority, in the context of exchange of information at group level) on the condition that information is exchanged for purposes of combating ML, TF or any associated crime: *MLR* s.14. Neither the *MLA* nor the *MLR* explicitly mention that the "tipping off" provision applies to directors of FIs, although Norway has indicated that the prohibition applies all persons who could possibly do this, including reporting FIs' directors. Importantly however, there are no penalties or sanctions for individuals breaching this provision, and the only penalty applicable to reporting entities is in relation to licencing restriction or withdrawal. Under the FATF Standards a requirement must have a proportionate and dissuasive sanction for non-compliance to be considered.

a5.102. **Weighting and conclusion:** The lack of any sanction for individuals for tipping-off is an important deficiency. **Norway is rated LC with R.21**.

Designated non-financial businesses and professions

Preamble: Scope of DNFBPs

a5.103. The 3rd MER mentioned that the following DNFBPs were subject to the AML/CFT requirements under the 2004 *MLA* and the *MLR*: real estate agents, dealers in precious metals and stones, lawyers and other independent legal professionals, accountants and auditors. It was further clarified that the following DNFBPs did not exist in Norway: land-based casinos and notaries. Notarial services are generally carried out by lawyers in Norway. The fact that AML/CFT obligations did not apply to TCSPs was a scope issue.

a5.104. The following DNFPBs are currently subject to the *MLA* and *MLR* and qualify as reporting DNFBPs for the purposes of this assessment:

- State authorised and registered public accountants: *MLA* s.4-2(1);

- Authorised external accountants: *MLA* s.4-2(2);
- 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 (EUR 5 200): *MLA* s.4-2(3);
- Real estate agents and housing associations that act as real estate agents: *MLA* s.4-2(4);
- Undertakings that, in return for remuneration, provide services corresponding to those referred to in ss.4-2(1) to 4-2(4): *MLA* s.4-2(5);
- Trust and company service providers: *MLA* s.4-2(6); and
- Dealers in movable property, including auctioneers, commission agents, in connection with cash transactions of NOK 40 000 (EUR 5 200) or more or a corresponding amount in foreign currency.

a5.105. With the exception of casinos, the *MLA* and *MLR* cover the categories of DNFBPs as defined by the FATF. The MLR clarifies that due to the nature of their work the following DNFBPs do not have occasional customers: accountants, lawyers and independent legal professionals and real estate agents. They enter into a business relationship with their customers when accepting an assignment from a client: *MLR* s.2. Consequently, provisions regarding occasional customers are not applicable to these groups.

a5.106. Offering gaming activities in Norway is a criminal offence unless they are permitted based on a specific law: *PC* ss.298-299. There are no laws permitting land-based casinos in Norway and therefore they are prohibited, although there are ship- and Internet-based casinos which are not subject to AML/CFT laws. The following Acts allow for specific casino-style gaming activities being offered:

- The *Gamings Act* gives exclusive rights to the state owned entity *"Norsk Tipping"* for the operation of gaming activities and in January 2014, was granted a licence to offer online casino style games. Players are issued an electronic card (one per player) by an e-money company and which are linked to one specific bank account and identification requirements apply. A maximum amount of NOK 10 000 (EUR 1 300) can be stored on the e-card and the amounts which can be used for on-line gambling are limited to NOK 4 000 (EUR 520) per day, NOK 7 000 (EUR 840) per week and NOK 10 000 (EUR 1 300) per month. Gains from internet gambling are credited on the e-card and once they reach a NOK 10 000 (EUR 1 300) threshold, they are automatically transferred to the associated bank account. All transactions on the e-cards are monitored by the e-money company issuing the e-cards.
- The *Lotteries Act* allows for the licensing of lotteries for humanitarian or social benefits, such as bingo, traditional ticket lotteries and gaming on ferries. Based on this Act and corresponding regulations, Norwegian shipping companies in route between Norwegian and foreign ports may be licensed to install slot machines and offer certain casino games, such as roulette and card tables although only in a limited form. So far, one shipping company has been granted such a licence.

a5.107. Even though land-based casinos are prohibited in Norway, as mentioned above, some authorised internet gaming exists since January 2014. This activity is available in the context of a strict framework as outlined above, which limit risk but are not in line with the FATF standards. When foreign cruise ships enter into Norwegian waters, Norwegian laws are applicable to them but there is no enforcement of the gambling requirements or any action taken to close down the games. In addition, foreign companies offer internet gaming in Norway and this activity is not regulated either. As a result, ship- and Internet-based casinos, constitutes a scope issue; however, the existence of only two licenced entities offering casino-style gaming and the existing controls means that this is not given significant weighting for R.22, 23 and 26.

Recommendation 22 – DNFBPs: Customer due diligence

a5.108. In its 3rd MER, Norway was rated PC with these requirements (paragraphs 339-347). The scope issue regarding casinos identified above has an impact on Norway's compliance with c.22.1-3.

a5.109. **Criterion 22.1-5** – The analysis in the implementation of R.10, 11, 12, 15 and 17 above, including the deficiencies identified, equally applies to reporting DNFBPs.

a5.110. **Weighting and conclusion:** The scope issue regarding casinos is minor but the deficiencies identified in R.10-12, 15 and 17 apply here. **Norway is rated PC with R.22**.

Recommendation 23 – DNFBPs: Other measures

a5.111. In its 3rd MER, Norway was rated LC with these requirements (see paragraphs 349 to 354). The 2013 Methodology added tax crimes as a predicate offence for ML which impacts on the reporting obligation.

a5.112. **Criterion 23.1** – The analysis in relation to R.20 above equally applies to reporting DNFPBs. Lawyers, other independent legal professionals, accountants and auditors, and TCSPs are required to report STRs to the FIU. The reporting requirement also applies to dealers in precious metals and stones in relation to cash transactions above NOK 40 000 (EUR 5 200) or their equivalent in foreign currency. This is consistent with the FATF requirements.

a5.113. **Criterion 23.2-4** – The analysis in relation to R.18, 19 and 21 above equally applies to DNFBPs.

a5.114. **Weighting and conclusion:** The scope issue regarding casinos is minor and the deficiencies identified in R.18-19 and 21 apply here. **Norway is rated LC with R.23**.

6. SUPERVISION

Recommendation 26 – Regulation and supervision of financial institutions

a6.1. In its 3rd MER, Norway was rated LC for regulation and supervision of financial institutions and PC with the requirements regarding shell banks which are now incorporated in R.26 (see paragraphs 308 and 319 to 322 in relation to market entry; paragraph 306 in relation to shell banks; paragraphs 308-309 and paragraphs 327 and 330 in relation to supervision and monitoring). R.26 puts an enhanced focus on the risk-based approach to supervision and monitoring.

a6.2. **Criterion 26.1** – The FSA is the competent authority for regulating and supervising Norway's reporting FIs, including for AML/CFT purposes. It has the responsibility to ensure that FIs have adequate policies, procedures and practices in place to comply with AML/CFT requirements: *FS Act ss.2-3*.

a6.3. **Criterion 26.2** – The licensing function for reporting FIs is divided between the MoF and the FSA. Licensing covers both core principles and other reporting FIs, including those providing a money or value transfer service or a money currency changing service (see also R.14 above). All FIs as referred to in the FATF's Glossary are covered by the licensing requirement: *CBA* s.8; *SBA* s.3; *FIA* 3.3,4b.2,4c.2; *STA* s.9.1; *SFA* s.2.1,10.3; *IA* s.2.1; *AIM* s.2.1; and *SRA* s.3.1. Shell banks are indirectly prohibited in Norway by requiring savings and commercial banks to have their registered office and head office in Norway or any other EEA country: *CBA* s.8 and *SBA* s.3.

a6.4. **Criterion 26.3** – Norway has legal and regulatory procedures in place to prevent criminals or their associates from holding a significant or controlling interest, or holding a management function in a reporting FI. Approval from the MoF is required to acquire/dispose of shareholdings in a bank, insurance company, finance company or mortgage company that go beyond defined thresholds (10%, 20%, 25%, 33% and 50%) or would allow the shareholder to exercise significant influence on the management of the credit institution or its business ("qualifying holding"): *FIA* s.2-2. Engaging in financial activities without being licensed or registered is a criminal offence which could lead to a criminal investigation, prosecution and conviction: FIA s.5-1, CBA ss.42-43 and SBA ss.58-59.

a6.5. The FSA conducts fit and proper tests when a reporting FI is granted a license. The FSA assesses the fitness and propriety of the board members, the managing director or other persons directly in charge of a FI (as the key functionaries) to assure proper and adequate management of the entity and its activities: *FSA Circular 5/2012*. This process includes a criminal record check and a self-declaration form. A licence shall be refused if the key functionaries cannot be deemed fit and proper: *CBA* s.8a; *SBA* s.3; *SFA* ss.2-3 and 2-7(1)(2); *FIA* s.2-4 and 3-3; *IA* ss.2-1 and 2-2; and *STA* s.9-9, or, alternatively, the FSA can order an FI to replace a person not deemed fit and proper before issuing the licence. Investments firms, management companies for securities funds, securities register, regulated market, debt-collecting businesses, real estate agents, foreign branches of Norwegian insurance and pensions companies and savings banks are obliged to notify the FSA of any changes in key functionaries, and the FSA will conduct a fit and proper test. However, there is no similar requirement for commercial banks, and all insurance and finance companies, although these entities are required to ensure that the fit and proper requirements are met at all times and the FSA considers this in its supervision activity.

a6.6. **Criterion 26.4** – The FSA's regulation and prudential supervision of banks, investment firms and management companies as well as insurance businesses is centred on the Basel, IOSCO and IAIS core principles and Norway reports that AML/CFT supervision is coordinated with this approach. However, even though Norway states that all core principles FIs are subject to supervision on a risk-sensitive basis, it is difficult to conclude that ML/TF risks are adequately taken into account when determining priorities for AML/CFT supervision as explained below. AML/CFT supervision, including the application of consolidated group supervision, is conducted as part of overall supervision and is supplemented with specific thematic AML/CFT reviews. Insurance companies have been subject to prudential supervision but the first AML/CFT inspection as part of a more general prudential supervision took place during the on-site visit without an AML/CFT specific methodology supporting the inspection. In addition, AML/CFT supervision in the securities

sector has only formed a minor part of the broader on-site inspections.

a6.7. The determination of which FIs should be subject FSA on-sites inspection is to a large extent based on prudential information and not ML/TF risk. The first step for the FSA in the assessment general risks associated with reporting FIs consists of looking at the institutions' specific characteristics, including the licences on the basis they operate, and the market share they represent. This initial assessment is based on information from quarterly reporting by the FIs and information from a broad range of both internal and external sources, such as FSA contacts in the context of licensing and organisational or procedural changes, complaints filed against the FIs, media surveillance, general developments in the markets the FIs operate, and publicly available information on specific FIs. However, the quarterly reports do not generally contain any AML/CFT specific information. The next step consists of identifying the operational risks individual FIs represent as the FSA considers ML/TF risk to be an integral part of the operational risk.

a6.8. Norway reports that other reporting FIs are also subject to regulation and supervision on a risk-sensitive basis. However, this statement is difficult to accept, especially when it comes to MVTS providers. While MVTS services present by their nature a higher risk, the FSA only monitors AML/CFT compliance via off-site or document based supervision and has not yet undertaken any on-site inspections of authorised MVTS providers. In the context of off-site supervision, MVTS providers are required to file a semi-annual report to the FSA with details on monitoring and reporting of suspicious transactions and, in some instances, information collected as part of the CDD process. In addition, as part of the renewal of MVTS providers' "waiver authorisation", the FSA also assesses the information reported on AML/CFT procedures. Moreover, the FSA does not monitor the AML/CFT compliance of MVTS providers from the EEA which have agents or branches in Norway even though these are subject to the *MLA* (see R.14 above for further details on MVTS). Foreign exchange activities may only be carried out by banks, finance companies and EEA branches of such undertakings: FIA chapter 4a. These activities are supervised as part of the overall supervision of these reporting FIs.

a6.9. **Criterion 26.5** – ML/TF risks play a limited role when determining the frequency and intensity of on-site and off-site AML/CFT supervision. The FSA has limited written documentation to support institution specific ML/TF risk assessments which could form the basis for a classification of reporting FIs based on ML/TF risks even though the FSA recognises the need to lay down the principles for an ML/TF risks classification in writing. While compliance with AML/CFT measures is assessed (for instance, identification of beneficial owners and sources of funds, suspicious transaction reporting), the AML/CFT assessments are mostly part of an overall inspection of the reporting FIs. In addition, in the absence of a reliable formal risk assessment, including a risk assessment of reporting FIs as referred to above, it is difficult to conclude that Norway has a sound basis to decide on the frequency and intensity of on-site and off-site AML/CFT supervision.

a6.10. **Criterion 26.6** – As set out above, the FSA has only limited documentation to support institution specific ML/TF risk assessments, including the ML/TF risk profile of individual FIs. While organisational and procedural changes are a set of factors to be considered for prioritisation of prudential supervision of reporting FIs, the FSA has no specific processes in place to review the assessment of the ML/TF risk profile of individual reporting FIs either periodically or when a major event occurs.

a6.11. **Weighting and conclusion:** The FSA does not undertake AML/CFT supervision on the basis of ML/TF risk (c.26.5) which is a serious deficiency. In addition, the limited supervision of certain sectors (MVTS, insurance and securities) is a concern given the ML/TF risks posed in the MVTS and securities sectors. **Norway is rated PC with R.26**.

Recommendation 27 – Powers of supervisors

a6.12. In its 3rd MER, Norway was rated LC with these requirements (paragraphs 311-9 and 331).

a6.13. **Criterion 27.1** – As indicated in relation to R.26 above, the FSA is Norway's competent authority for regulating and supervising Norway's financial sector entities, including for AML/CFT purposes: *FS Act*, ss.2 and 3. It has the responsibility to ensure that reporting FIs have adequate policies, procedures and practices in place to comply with AML/CFT requirements.

a6.14. **Criterion 27.2** – The FSA has comprehensive inspection and monitoring powers, including the power to conduct on-site inspections and off-site reviews: *FS Act* s.3. There are however no written regulations or guidelines prescribing the procedure that the FSA must follow for on-site inspections, particularly on how to assess compliance with AML/CFT obligations and what actions to take when breaches of AML/CFT legislation are detected.

a6.15. **Criterion 27.3** – The FSA has the power to compel production of or obtain access to reporting FIs' records without the need for a court order. Reporting FIs are obliged to provide the FSA with all the information it requires to conduct these inspections and reviews. If a reporting FI fails to comply with this requirement, then the FSA may impose this disclosure obligation on the reporting FI's officers and employees: *FS Act* s.3. Moreover, a reporting FI's auditor may be ordered to disclose information that appears in the annual financial statements, account forms, staff pay summaries and deduction sheets, auditor's records and auditor's report: *FS Act* s.3a.

a6.16. **Criterion 27.4** – The FSA is authorised to impose a range of sanctions against reporting FIs that do not comply with Norwegian law, including AML/CFT requirements. Depending on the gravity of the failure to comply with AML/CFT requirements, the FSA can impose disciplinary and financial sanctions on reporting FIs and their officers/employees: *FS Act* ss.6 and 10; *MLA* ss.27 and 28. However, apart from coercive fines, financial sanctions can only be imposed if criminal procedures are brought. As explained in more detail in relation to R.35 below, the sanctions provisions both in the *MLA* and the *FS Act* cannot be considered to be proportionate and dissuasive, especially for directors and senior management.

a6.17. **Weighting and conclusion:** The only deficiency is that relating to sanctions (c.27.4). **Norway is rated LC with R.27**.

Recommendation 28 – Regulation and supervision of DNFBPs

a6.18. In its 3rd MER, Norway was rated LC with these requirements (see paragraphs 359 to 376). R.28 puts an enhanced focus on the risk-based approach to supervision and monitoring. The minor scope issue regarding casinos identified above has a negative impact on Norway's compliance with R.28.

a6.19. **Criterion 28.1** – As outlined above in the preamble, casinos are not reporting entities and therefore not subject to supervision for AML/CFT compliance. However, as noted above at paragraphs 251-252, land-based casinos are prohibited and entities offering casino-style gaming on ships and through the Internet are required to be licenced and have strict controls in place to restrict gambling. There are only two such entities currently licenced. Foreign companies also offer internet gaming in Norway but this activity is not regulated. In all cases, there are no legal or regulatory measures in place to prevent criminals or their associates from holding a significant or controlling interest, or holding a management function in the companies offering the casino games which are licensed.

a6.20. **Criterion 28.2** – The FSA is Norway's competent authority for monitoring and ensuring compliance with AML/CFT requirements for real estate agents, and accountants and auditors: *FS Act* ss.2-3. The Supervisory Council for Legal Practice is the AML/CFT regulatory and supervisory authority for lawyers and other independent legal professionals (*CJA* s.225). Norway has no designated competent authority for AML/CFT monitoring and supervision of TCSPs and dealers in precious metals and stones.

a6.21. **Criterion 28.3 –** The FSA has the responsibility to ensure that real estate agents, and accountants and auditors have adequate policies, procedures and practices in place to comply with AML/CFT requirements: *FS Act* ss.2-3. The Supervisory Council for Legal Practice examines lawyers' files and books to determine whether lawyers are complying with their legal obligations, including those related to AML/CFT and specifically verifies that AML/CFT controls are in place: *Regulation for Lawyers* s.4-7. Norway also reports that as a matter of routine, the Supervisory Council looks into suspicions of unlawful activities by lawyers, including ML/TF. TSCPs and dealers in precious metals and stones are currently not subject to any system for monitoring compliance with their AML/CFT obligations.

a6.22. **Criterion 28.4** – *Adequate powers to perform functions:* The FSA's powers to monitor compliance

with AML/CFT obligations are explained in criteria 27.2-3 above. These powers, which include the power to conduct on-site inspections and compel documents, equally apply in relation to real estate agents, and accountants and auditors. The general statutory power to inspect lawyers can be found in the *Regulation for Lawyers* s.4-5. The power of the Supervisory Council to conduct AML/CFT specific controls as part of financial audits is included in the *Regulation for Lawyers* s.4-7.

a6.23. **Measures to prevent criminal ownership or management:** A person who carries out the activity of real estate agent needs to either be licensed by the FSA or be licensed as a lawyer who has specifically provided security (a financial guarantee of minimum NOK 30 million (EUR 3.9 million): *REAA* s.1-2. The FSA assesses the fitness and property of the natural person or, in case of a legal person, of the owner, managing director or other persons directly in charge to assure proper and adequate management of the real estate agent's activities: FSA Circular 5/2012. In addition, applicants must submit a police certificate and meet certain professional criteria. The FSA also licenses external accountants (both natural and legal persons) and conducts fit and proper tests based on the same Circular.

a6.24. Lawyers must be licensed by the Supervisory Council to practise law: *CA* s.218. To obtain a licence, a person must have a law degree and present documentation establishing blameless conduct: *CA* s.220. The Supervisory Council requests the submission of a police certificate that is not older than three months at the time of the application and an auditor must be involved for checking the lawyer's potential compliance with AML/CFT measures (i.e. whether there are routines on control and reporting).

a6.25. **Sanctions in line with R.35 to deal with failure to comply with AML/CFT requirements:** Consistent with what is mentioned in relation to c.27.4 above, the FSA is authorised to impose a range of sanctions against real estate agents, accountants and auditors that do not comply with Norwegian law, including AML/CFT requirements. The FSA can impose disciplinary and financial sanctions on these reporting DNFBPs and their directors, officers, and employees: *FS Act* ss.6 and 10; *MLA* ss.27 and 28. However, apart from coercive fines, financial sanctions can only be imposed if criminal procedures are brought. The Supervisory Council has the power to apply sanctions under ss.27 and 28 of the *MLA* and s.225 of the *CA*. The latter provides the power to give a reprimand, issue a warning or revoke the licence of the lawyer. However, concerns exist with the level of sanctions (see R.35 below).

a6.26. **Criterion 28.5** – The FSA supervises real estate agents and accountants and auditors on the basis of on a risk-sensitive basis, primarily relating to prudential and business conduct risks. Priorities for on-site inspections are mainly set for prudential and other supervision, and are based on external sources of information, such as professional bodies (NARF and DnR), the tax authorities, bankruptcy estates, the police and cases in the media. Accountants and auditors provide some feedback on their AML/CFT measures by answering questions as part of a general semi-annual activities report they file with the FSA but this is not considered to provide a sound basis for an AML/CFT specific risk assessment. The FSA has no specific methodology to assess the ML/TF risks these DNFBPs present or establish their individual ML/TF risk profiles. Although the FSA will give priority to those professionals for who there are clear indications of non-compliance with AML/CFT obligations (based on the self-assessment questionnaire), ML/TF risks are only taken into account to a limited extent when determining which individual reporting entities will be inspected. In addition, AML/CFT supervision is one aspect looked at during both on-site and off-site inspections. While the FSA reports that it also conducts thematic inspections, these do not appear to relate to AML/CFT but rather to accounting or auditing practices. AML/CFT supervision of lawyers is also conducted in a much broader context and the risk-sensitive basis for deciding on the frequency and intensity of supervision is not based on ML/TF risks.

a6.27. **Weighting and conclusion:** The absence of a supervisor for TCSPs and dealers in precious metals and stones is an important scope issue for R.28. In addition, supervision is not carried out on the basis of ML/TF risk, and sanctions are not proportionate and dissuasive. **Norway is rated PC with R.28**.

Recommendation 34 – Guidance and feedback

a6.28. In its 3rd MER, Norway was rated PC with these requirements. Norway took action to address some of the deficiencies identified in the MER and Norway's 4th FUR concluded that Norway had raised its compliance

with the FATF's requirements to a level essentially equivalent to LC (paragraphs 77-81).

a6.29. **Criterion 34.1** – ***Supervisors:*** In June 2009, the FSA issued Circular 8/2009 which contains general AML/CFT guidelines to assist reporting entities with the implementation of the *MLA* and *MLR*. This Circular, which is non-binding and was developed in cooperation with industry organisations, contains no examples of how effective implementation of the key building blocks of Norway's AML/CFT regime, including the application of the RBA and the detection of suspicious transactions, can be achieved. The FSA Circular 13/2006 issued in June 2006, which contains specific and tailored AML/CFT guidelines for auditors and external accountants, has not been updated even though the *MLA* has been substantially changed in 2009. Norway explains that it should be read together with Circular 8/2009. In November 2013, the FSA issued revised guidance on how to comply with the obligations to freeze terrorist related assets.

a6.30. The FSA is to a limited extent involved in AML/CFT education and training covering the entire financial sector, and primarily on an ad hoc and reactive basis. It contributes to the yearly AML/CFT conference which is organised in cooperation with the FIU and the industry association, Finance Norway. While the FSA has contributed to the delivery of presentations and training sessions on legislative issues and trends to the 270 participants, the majority was delivered by the FIU and Finance Norway. The FSA only proactively provides feedback on an ad hoc and limited basis. Norway provided one example of this when, in 2011, the FSA sent a public letter to the boards of financial institutions with a summary report from the thematic inspections in 2010 relating to AML/CFT. This is not a consistent or regular practice. Since November 2007, the FSA and the FIU operate the website www.hvitvasking.no which contains information regarding AML/CFT, including laws and regulations; announcements from the public sector; court decisions; news from the FATF, the EU, the Egmont Group, etc.; and typologies and trends.

a6.31. **FIU:** The FIU has assigned a staff member responsibility for compliance in relation to reporting entities. Feedback is provided on a regular basis both via follow-up from the person responsible for compliance at the FIU and via the analysts in connection with specific cases. In addition, FIU staff give lectures at seminars attended by reporting entities. Because of the diverse audience during these seminars, only general feedback is provided. However, during private sector specific seminars the FIU gives more focused feedback regarding the quality and the use of STRs with the aim to improve their quality. The FIU's IT system *Ask* enables a better structure for follow-up of reporting entities by providing better data for this purpose. *Ask* sends an automatic response to reporting entities confirming receipt of an STR within three days and also sends alerts to reporting entities when an STR they reported is being further analysed. The FIU provided the assessment team with a comprehensive overview of its training activities. For example, the FIU in coordination with the MoJ recently conducted outreach to small and medium sized FIs in the regions as part of the program, *Round Norway*. While this program focused on LEAs, the FIU also visited FIs to raise awareness and give feedback on the importance of filing high-quality STRs. The FIU also operates a "hot line" for reporting entities seeking practical guidance on their reporting obligations.

a6.32. **Law enforcement authorities:** The PST is also engaged in providing feedback on CFT, including typologies, to both public and private sector entities, often in cooperation with the FIU. This feedback is provided both on a case-by-case basis and through participation in training sessions and seminars. When PST gives lectures, it focuses on the importance of financial intelligence and STRs. Norway was unable to provide the assessment team with examples of feedback from other LEAs to the reporting entities.

a6.33. **Weighting and conclusion:** While the FIU and PST provide valuable feedback to reporting entities on STRs and TF issues, an important deficiency is the limited guidance provided by the FSA and lack of proactive engagement with the private sector. **Norway is rated LC with R.34**.

Recommendation 35 – Sanctions

a6.34. Norway was rated LC with these requirements. The main deficiencies were that there was a lack of clarity as to whether or not sanctions (whether civil or criminal) were applicable to directors and senior management, in addition to legal persons.

a6.35. **Criteria 35.1 & 35.2** – The FSA is authorised to impose a limited range of sanctions against reporting FIs (i.e., FIs and DNFBPs other than casinos) that do not comply with AML/CFT requirements. Supervisors may issue orders to reporting entities to cease contravening provisions of the *MLA* and set time limits for doing so. They may also impose "coercive" fines (either single or recurrent fines) on reporting entities that fail to comply with such orders. The MoF has regulation-making authority concerning the imposition of such coercive fines, including their amount, though no regulations have been issued to date. In the absence of any regulations, it is unclear what the amount of those fines would be. The FSA has flexibility to assess what is reasonable and dissuasive, and generally considers that for all laws for which it is the supervisor, that coercive fines of NOK 250 (EUR 32.50) per day per employee are appropriate. However, the lack of transparency of the amounts reduces the dissuasiveness of the fines to reporting entities. In addition, coercive fines can only be imposed on reporting entities, and not on natural persons such as directors and senior management of the entity: *MLA* s.27.

a6.36. There are no administrative penalties for breaches of the *MLA*. However, criminal penalties may apply. Persons (natural and legal) are liable to fines for wilfully or with gross negligence contravening a defined subset of provisions of the *MLA* and, in the case of aggravated circumstances, to imprisonment of up to one year. This is also applicable to the directors and senior management. However, this provision is limited to the contravention of only eight sections of the *MLA: s.28* (being s.5 (RBA), 6-8 (CDD), s.15 (enhanced CDD), s.17-18, 22 (STRs)). These eight sections do not cover some of the fundamental building blocks of Norway's AML/CFT regime, including certain CDD requirements (e.g. timing, third parties and reliance), the obligation to apply on-going monitoring, corresponding banking relationship requirements, internal control requirements, and the tipping-off provisions. In addition, such fines can only be imposed if criminal procedures are brought. The level of fines would be determined by the court taking into account the nature of the offence and the financial position of the person: *PC* s.27.

a6.37. The sanctions provisions of the *MLA* are complemented by the powers in the *FS Act*: s. 4. These include withdrawing, restricting or suspending the licence of the reporting FI, fines and orders to rectify deficiencies. The FSA can order an institution it supervises to correct a failure to discharge its duties as required by law: *FS Act* s.4(7). Contravention of provisions applying to such institutions may also be reported to the relevant prosecuting authority: *FS Act* s.6. Any person, officer or employee of an institution under the FSA's supervision is liable to fines and/or imprisonment up to one year for wilfully or through negligence contravening an order issued by the FSA, and in aggravated circumstances, to imprisonment of up to three years: *FS Act* s. 10. Again, these fines can only be imposed if criminal procedures are brought. This provision equally applies to directors. In addition, the FSA may take into account breaches of the *MLA* by directors and senior management in its assessment of fit-and-proper person requirements.

a6.38. Persons who wilfully violate regulations to implement targeted financial sanctions related to terrorism and TF pursuant to the *Act relating to the implementation of mandatory decisions of the Security Council of the United Nations* are liable to a fine or imprisonment not exceeding three years or both. Persons who negligently violate or negligently contribute to the violation of such regulations are liable to a fine or imprisonment up to six months, or both: s.2.

a6.39. **Weighting and conclusion:** While overall the *MLA* and the *FS Act* provide the FSA with a range of sanctions, these sanctions are not proportionate and dissuasive, especially for directors and senior management. The lack of clarity over the application of coercive fines is a serious concern relating to their dissuasiveness. In addition, the ability to sanction senior management and directors is limited, as administrative sanctions cannot be imposed. Importantly criminal sanctions, while applicable to natural persons, do not cover several of the essential AML/CFT requirements. **Norway is rated PC with R.35**.

7. LEGAL PERSONS AND ARRANGEMENTS

Recommendation 24 – Transparency and beneficial ownership of legal persons

a7.1. Norway was rated as LC with previous requirements relating to legal persons (see 3rd Mutual Evaluation Report (MER) paragraphs 380-396). Since then the FATF standards have changed substantially.

a7.2. **Criterion 24.1** – The following types of legal persons can be created in Norway: (a) Companies – limited companies, public limited companies and European companies[1]; (b) Partnerships – general partnerships, general partnerships with shared liability, and limited partnerships; (c) Societies – house building co-operatives, housing co-operatives and co-operative societies; and (d) Organisations – Foundations, savings banks and associations. The Bronnoysund Register Centre (BRC) provides a guide on its website (www.altinn.no) for starting a business in Norway, including an overview of the types of legal entities that can be created in Norway, their basic features and the creation/registration procedures. The guide also provides information and advice on choosing the appropriate type of entity, but does not indicate how basic and beneficial ownership information can be obtained. The information is available in Norwegian and English.

a7.3. **Criterion 24.2** – Norway has only assessed the ML/TF risks associated with different types of legal persons to a limited extent. The NRA noted some of the vulnerabilities relating to the difficulty of determining beneficial ownership of legal persons in Norway. However, the threats posed by the different types of legal persons and the ways in which they are misused in Norway were not considered.

a7.4. **Criterion 24.3** – Norway has a system of multiple public registries for different types of legal persons, and there is also a central coordinating register that holds key information. Norway requires all companies created in Norway to be registered under the *Business Enterprise Registration Act of 21 June 1985 (BERA)*. All companies must register in the Central Co-ordinating Register, which is governed by the *Central Coordinating Register of Legal Entities Act (CCRA)*. The CCR provides all new companies with a nine-digit organisation number, which is used to identify the legal person in all public business and industry registers. The registry records the required basic information on the company (name, proof of incorporation, legal form/status, address, basic powers and list of directors) which is publicly available.

a7.5. Partnerships and cooperative societies are required to register with the Business Register, and foundations in a separate Foundations register, as outlined below. Other types of societies and organisations are required to register with the Business Register if they conduct business, or if they receive public funding. Any legal person that intends to open a bank account must register in the CCR.

a7.6. In addition to the CCR, the various other registers that hold information related to the basic ownership of legal persons include:

- ***Register of Business Enterprises (Business Register)*:** All Norwegian and foreign business enterprises conducting business in Norway (including companies, partnerships, and sole proprietorships) must register with the Business Register: *s.2-1, BERA*. Norwegian limited companies must submit information on: the articles of association; the date of the company's formation; the company's registered address; the municipality of the business enterprise; the board members; the chairman of the board; the general manager (managing director); the person(s) who represents the enterprise externally; and the person(s) who has the power to sign documents on behalf of the company: *s.3-1a, 3-7, 3-8*. Partnerships in Norway must also register in the Business Register including the partnership's name; names of partners; its objective; board members (if any) and general manager; the names of those empowered to act on its behalf; and the partnership agreement: *ss.3-3, 3-4*. Similarly, cooperative societies must also register with the Business Register:

1 European companies are regulated by the *European Companies Act*, (which applies Council Regulation 2157/2001) and by the *Public Limited Liability Companies Act*. Such companies are treated the same as PLLCs.

Cooperatives Act s12. Information in the Business Register is publicly available: *BER s8-1*.

- ***Register of Company Accounts*:** All Norwegian limited companies, public limited companies, savings banks, mutual insurance companies and petroleum enterprises must submit annual accounts (including the auditor's report) to the Register of Company Accounts within one month of being adopted by the annual general meeting (or by 1 August): *Act Relating to Company Accounts*. The annual accounts must also be accompanied by a list of all shareholders at that time. If the annual accounts are submitted late, the company must pay a default fine, or after six months, the Bankruptcy Court may dissolve the company. The Board of Directors is responsible for ensuring that the annual accounts are accurate. The Register of Company Accounts only confirms that all of the necessary documentation is attached, and that the annual accounts were adopted by the company's annual general meeting. The Register of Company Accounts stores the annual accounts and reports for ten years and makes them publicly available.

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

- ***Corporate Taxation Data Register*:** This register contains information identifying the shareholders of Norwegian legal persons who are obligated to pay tax in Norway. Such information is collected primarily for tax purposes, but is also accessible by authorities once a criminal investigation has begun and there is a cause to suspect that an offence punishable by a sentence of imprisonment for more than six months has been committed. A legal person is obligated to update the information in this register once a year and it is a criminal offence to not give the required information to the tax authorities.

- ***Register of Foundations*:** All foundations must register and provide the name of the founder, the members of the board, the assets of the foundation, and any special rights given to the founder: *s.8 Foundations Act*. Foundations are also required to file a certified copy of the foundation deed: *ss.11-12*. The foundation may not distribute capital or other benefits to the founder.

a7.7. The legislation for the various legal persons requires that they be registered with the BRC within three months of formation. As a result, this means that legal persons can operate for a period of up to three months prior to registration. However, businesses enterprises are required to register with Business Register prior to commencing business activity, although they can provide notification up to 3 or 6 months, depending on the type of legal person, after the creation of the entity: *BERA s.4-1*. Cooperatives are also prohibited from doing business: *Cooperatives Act s.13(1)*. In addition, in practice, legal persons register as soon as possible to be able to open and operate bank accounts and to enter into agreements.

a7.8. **Criterion 24.4** – Norway requires all Norwegian private and public limited companies to establish and maintain a register of all shareholders, including their name, date of birth and address, (or for legal persons: business name, organisation number and address): *Limited Liability Companies Act* (*LLC Act) s.4-2* and *Public Limited Liability Companies Act* (*PLLC Act*) *s.4-4*. The register of shareholders is kept at the company's head office and must be available to the public: *LLC Act s.4-6* and *PLLC Act s.4-5*. Regulations made under the PLLC Act and LLC Act state that the shareholder register held by the company must be accessible to anyone at the company's office during business hours: *Regulations 4 November 1976 no.1*. If the company does not have an office, the shareholder register must be accessible at the company's place of business during business hours. Companies are also required to send a transcript of the shareholders register to anyone requesting such information no later than 14 days after receiving a request.

a7.9. Public limited liability companies (PLLCs) are also required to have a register of shareholders in a security register: *PLLC Act* s.4. Limited liability companies (LLCs) may also decide to establish a register of shareholders in a security register: *LLC Act* s.4-11. Information in the securities register is available to anyone who requests it, directly from the securities register: *Securities Register Act* s.8-2.

a7.10. For partnerships, the partnership agreement must contain the name and address of the partners: *Partnership Act s.2-3*. Cooperative societies are required to have a register of their members: *Cooperatives Act s.14(4*). However, this list is available only to members and there is no legislation or regulations regarding access to information held by the cooperative society. Foundations are required to have a foundation deed which must set out the object of the foundation, the board of directors (unless determined by elections), and any special rights granted to the founder or other persons: *Foundations Act s.9*.

a7.11. **Criterion 24.5** – All legal persons registered in the CCR shall inform the registrar without undue delay of any changes to the information provided. Businesses registered in the Business Register are required to promptly report all changes to information registered with the Register for Business Enterprises by notifying the registrar. Authorities could not indicate the timeframe within which they expect changes to be reported. When the registrar is made aware that the registered information is not correct, then the entity can be fined: *s.4-5 BER Act*. As a first step, the registrar will write a letter to the legal person reminding them of their obligation to update their information. In practice, the registers are updated by legal persons because other public authorities require the information to be reported to them to be the same as that in the registers, for example, in cases of agreements with public authorities. Any updating of information electronically through Altinn has built in automatic checks to ensure that the information is being provided by a registered person connected to the legal person. This registration is also required by financial institutions and others if a person wants to represent a legal person and conduct transactions for it. All changes to the information registered with the Foundation Authority must be promptly reported by providing notification to the registrar. If a foundation is wound up, the registrar must be informed so that the foundation can be removed from the register: *s.8*. There do not appear to be proactive steps taken to verify information on any of the registers, and although company officials must file written declarations setting out the information, there do not appear to be penalties for filing incorrect information.

a7.12. In relation to the information held by companies, transfers of shares in a limited liability company are to be reported to the company: *LLC s.4-7*. The transfers of shares in a public limited liability company are required to be reported forthwith to the securities registry: *PLLC s.4-7*. Authorities could not indicate this timeframe is applied in practice and how this is applied. While there are no direct sanctions for failure to report the shareholder can only exercise his rights when changes in ownership have been recorded in the shareholder registry: *LLC Act* s.4-2 and *PLLC Act* s.4-2.

a7.13. **Criterion 24.6** – Norway uses a combination of mechanisms to ensure access beneficial ownership information. However, the mechanisms used focus on legal rather than beneficial ownership, which would have to be obtained by following the chain of information where this is available.

a7.14. The various registers maintained by the BRC contain a significant amount of information relating to beneficial ownership of companies which is publicly available. The central coordinating register includes information on persons exercising control over the company including the board of directors, the general manager and the person who has the power to sign documents on behalf of the company. For the natural persons identified in these roles, the register includes the personal identity number of Norwegians, or D-number for foreigners, and their identity is cross-checked against the National Population Registry. This means that, where only Norwegian companies with Norwegian ownership are involved, authorities are able to follow the chain of ownership to a natural person who has an identity in the population register.

a7.15. However, where foreign legal persons or arrangements are involved in owning shares in Norwegian companies, beneficial ownership information is not contained in various public registers. This also applies to the information collected and maintained by companies in their shareholder registry, which relates to legal ownership. In such cases, the public registers and the register of shareholders reflect the name, registration number and address of the foreign company. If the Norwegian authorities seek information about a foreign entity's chain of ownership, they would have to ask the foreign entity for that information, or check the business or other register of the home country. The information accessible regarding the foreign company will depend on the information that the home state requires the entity to register about its owners, or which is otherwise obtainable e.g., through international cooperation. As a result, beneficial ownership information on Norwegian companies owned by foreign entities is not available to competent authorities in a timely manner.

a7.16. Competent authorities in Norway also have access to beneficial ownership information held by reporting entities. When undertaking CDD, reporting entities are required to identify and take reasonable measures to verify the identity of the beneficial owner (see R.10 above). This includes lawyers and TCSPs (see R.22 above). However, while reporting entities are required to hold information on beneficial ownership, Norway has not provided information as to whether such information can be obtained by competent authorities in a timely manner, nor whether it is accurate or up-to-date. This is particularly the case where there is a foreign ownership element.

a7.17. Competent authorities have access to the information that companies provide in their annual accounts and which is recorded in the Register of Company Accounts. PLLCs and large LLCs must provide annual accounts to the Register of Company Accounts which includes information on the 20 largest shareholders in the company (for shareholdings greater than 1%): *Accounting Act s.7-42*. For small LLCs, the annual accounts submitted to the Register of Company Accounts must contain information on the 10 largest shareholders in the company: *Accounting Act s.7-42*. Information on shareholders holding less than 5% of shares is not required. However, while this includes legal shareholder information it does not include beneficial ownership information. Companies also have to send in an annual tax return to the tax authorities, which includes ownership information, and any ownership interest (regardless of size) in a company is also registered in the tax authority's shareholder register.

a7.18. Taken together, these mechanisms provide reasonably good information on the legal owners of Norwegian companies and some information relevant to beneficial ownership. However, the focus on legal ownership and the difficulty in obtaining beneficial information on foreign companies means that these other measures do not adequately ensure that beneficial ownership information is available to competent authorities in a timely manner.

a7.19. **Criterion 24.7** – Norway takes limited measures to ensure that the beneficial ownership information, where available, is accurate and up-to-date. The BRC automatically cross-checks the information it receives on individuals with information on the National Registry as noted above. Information on shareholders provided to the tax authority is provided annually and not kept up-to-date. There is no verification of whether information is accurate.

a7.20. **Criterion 24.8** – Both public and private limited companies are required to have the general manager and at least half the members of the board of directors either as Norwegian residents or as citizens and residents of an EEA country: *PLC Act s.6-11 and PLLC Act s.6-11.* This means that Norway does not have a requirement that there is a natural person that is a resident or a Norwegian DNFBP that will ensure that the company they represent can cooperate with authorities by ensuring that all basic and beneficial ownership information is available in Norway. Norway suggests that because the BRC records the name and address of such EEA residents this is an equivalent mechanism, but Norwegian competent authorities would only be able to seek assistance through the normal international cooperation channels, which is different to the possibility to question the Board or general manager in Norway.

a7.21. **Criterion 24.9** – There are no provisions in Norwegian law which require the registries or companies to keep records for five years after the date on which the legal person has been dissolved. However, in the case of bankruptcy of a legal person, the court appointed liquidator will submit a final report to the court, which will hold this information. In addition, all bankruptcies are reported to the Register for Bankruptcies which stores information on the legal person. For companies, this includes information on shareholders who have a shareholding of more than 20% in the five years before bankruptcy. This information is never removed from the registry (see *Debt Settlements and Bankruptcy Act* and related regulations, and *Archive Act*. It is available to competent authorities but is not publicly available. Finally, reporting entities are required to retain records of the documents used to verify the data required to be obtained under *MLA* s.7&8 (customer identification, beneficial ownership information and information on purpose and use) for 5 years after the completion of occasional transaction or termination of the customer relationship: *MLA* s.22.

a7.22. **Criterion 24.10** – The information held in registries and by companies is publicly available, and Norwegian competent authorities responsible for investigating ML, associated predicate offences and TF have the powers needed to obtain access to all necessary documents and information for use in those

investigations (see R.31 below). In particular, the Central Coordinating Register facilitates this since it records all the key information in a single location.

a7.23. **Criterion 24.11** – There are no bearer shares in Norway. In addition, warrant or subscription rights may not be held in bearer form in Norway. The rights are accorded to the person or entity which is recorded in the entity's register for these types of rights.

a7.24. **Criterion 24.12** – There is specific provision in the *PLLC Act* whereby traded shares of public limited companies listed on an exchange may be held by a trustee (nominee) but only in certain situations. This is only for foreign companies that so invest, and several conditions apply. Norwegian law permits the buying and selling of shares of public limited and limited companies (that are registered in the Securities register) through a nominee for foreign investors with safeguards in place. However, Norway did not provide any information to demonstrate that prohibitions are in place for the use of nominees outside of this arrangement. Under the provisions, a bank or another share manager (such as a securities firm or management company for securities) who is licensed by the FSA to act as a nominee may act as a nominee for foreign shareholders: *PLLC Act s.4-10*. Such a nominee may be registered as the owner on behalf of the foreign shareholder. However, the register of shareholders (which must be publicly available) must include the nominee's name and address, and state that he/she is a nominee of the shares: *PLLC Act s.4-10(2)*. Additionally, the nominee's license sets out conditions requiring the nominee to maintain information identifying the beneficial owner and to give all information concerning the beneficial owner of the shares to the authorities or the company upon request: *PLLC s.4-10(4)*. While these requirements are valuable, they only apply to formal nominees and apply only in very limited circumstances. As noted in recent studies e.g., *The Puppet Masters (World Bank)*, criminals often use formal and informal nominee relationships to launder their proceeds. There are no other measures in place to prevent the misuse of nominee shareholders or directors.

a7.25. **Criterion 24.13** – Failure to comply with the duty to register with the Central Registry is an infringement of the *CCRA* and may be subject to administrative sanctions: *CCRA s.16*. Failure to register with the Business Register is an infringement of the *BERA* and may be subject to administrative sanctions: *BERA s.10-4*. Failure to provide notification of changes to information held by the Business Register is sanctioned by administrative sanctions: *BERA s.4-5*. The sanctions for breaches of the *BERA* and *CCRA* increase per week. It starts at NOK 500 (EUR 65) in the first week for the first eight weeks, NOK 1 000 (EUR 130) the next ten weeks and NOK 1500 (EUR 195) the following eight weeks. The maximum penalty is NOK 26 000 (EUR3 380). Such a failure is also criminal offence and can be subject of sanctioned by fine of up to NOK 26 000 (EUR 3 380) or the company can be deprived of the right to carry on business, or prohibited from carrying it on in certain forms: *Penal Code s.48a*. The level of fines for breaches of registration requirements is relatively low and is not dissuasive. The possible restrictions on operations of legal persons appear to be a dissuasive sanction. However, it is difficult to determine the dissuasiveness of the sanctions available as they have rarely been applied for failure to register or for failure to notify of changes to information held by the registers. Failure to comply with the requirements in the *LLC Act* and *PLLC Act* can be punishable by administrative sanctions and, in aggravating circumstances, imprisonment of up to one year: *LLC Act s.19-1* and *PLLC Act s.19-1*.

a7.26. There are no direct sanctions for the failure of registered entities to provide access to ownership information, although other sanctions may apply for failure to comply with requests for information from competent authorities e.g., entities under the FSA's supervision that fail to provide information requested by the FSA may be subject to a daily fine: *Act relating to the Supervision of Financial Institutions, s.10*.

a7.27. **Criterion 24.14** – Norway is able to provide international cooperation through a range of mechanisms (see below R.37-40). The basic information held on the registries and companies is publicly available or available to the public on request. The information held by the Business Register is available in English through either the BRC website, or by contacting the BRC. This may assist foreign counterparts to access basic information on legal persons. In particular, the FIU often provides foreign counterparts with the links and information on access to allow them to access this information directly. Norwegian businesses may also be registered with the European Business Register. Information held in the European Business Register is available in a range of languages. In addition there is information available on private websites such as www.purehelp.no.

a7.28. **Criterion 24.15** –Norway does not specifically monitor the quality of assistance it receives from other countries in response to requests for basic and beneficial ownership information. Individual agencies are aware of the quality of the assistance they receive but, no information was provided on this.

a7.29. **Weighting and conclusion:** While significant information on beneficial ownership of Norwegian companies is available to authorities in a timely manner when purely Norwegian ownership is involved, this is not the case when Norwegian companies have elements of foreign ownership. **Norway is rated PC with R.24**.

Recommendation 25 – Transparency and beneficial ownership of legal arrangements

a7.30. In its 3rd MER, Norway was not rated against these requirements as it was not applicable to countries that did not recognise trusts or other legal arrangements. However, there are substantial new requirements in relation to legal arrangements in R.25 including obligations that apply to all countries. Norway is not a signatory of the 1992 Hague Convention on the law applicable to trusts and the Norwegian legal system does not provide for the creation of trusts or other legal arrangements, though foreign trusts or other legal arrangements are not prohibited. Trusts and other legal arrangements formed overseas can and do operate through persons that are trustees and who reside or otherwise act for the trust in Norway.

a7.31. **Criterion 25.1 & 25.2** – c.25.1(a)-(b), and c.25.2, are not applicable as the Norwegian legal system does not provide for the creation of trusts or other legal arrangements. Measures taken to require professional trustees (lawyers or TCSPs) to keep CDD and transaction records are described in R.22 above.

a7.32. **Criterion 25.3** – There is no legal obligation on trustees to disclose their status to reporting entities. However, as part of the CDD requirements, reporting entities are required to identify any persons acting on behalf of a customer, on the basis of a valid proof of identity using a document, issued by an authorised body, and which contains the representative's full name, signature, photograph and personal ID number: Art.7. They should, for control purposes, explicitly ask customers whether they are "acting" for someone else (see R.10 and 22 above). Accordingly, while not explicitly referring to trustees, the normal CDD requirements could in some way help ensure that trustees disclose their status to reporting entities. However, it is unclear whether this obligation on reporting entities would require the disclosure of their status by a trustee in practice, and this issue is not addressed in the guidance.

a7.33. **Criterion 25.4** – There seems to be no provisions in Norwegian law or regulation which would prevent the disclosure of information regarding a legal arrangement.

a7.34. **Criterion 25.5** – The general powers of law enforcement, prosecution and judicial authorities apply to information regarding trusts and legal arrangements where information is held in Norway. In criminal investigations, the police authorities have the powers they need to give access to beneficial ownership information held by reporting entities (see R.31 below). This includes information held by TCSPs and other DNFBPs such as lawyers, and the CDD information held by reporting FIs. Law enforcement agencies also have access to the records kept by trustees pursuant to the *Bookkeeping Act*. Records must be kept if there is a Norwegian tax or VAT liability.

a7.35. **Criterion 25.6** – Normal provisions for cooperation with competent authorities in other countries apply to requests for shareholder or beneficial ownership information, with neither restrictions nor special measures applied (see below R.37-40). However, this does not necessarily mean that such information is accessible to foreign counterparts in practice. No information was provided that shows the authorities rapidly provide international cooperation on information relating to trusts and other legal arrangements that may hold assets in Norway or where the trustee is located in Norway.

a7.36. **Criterion 25.7 & 25.8** – Although the Norwegian legal system does not provide for the creation of trusts, Norway does not place any obligations (or associated sanctions) on trustees of foreign trusts to ensure that they disclose their status to reporting entities or to give access to information held by them in relation to the trust. The only possibility is that deliberately providing incorrect information for the purpose of obtaining

an unlawful gain and thus causing loss or risk of loss may amount to fraud; however this is very indirect and may only be applicable in certain factual cases.

a7.37. **Weighting and conclusion:** The majority of the criteria do not apply to Norway as it does not have trust law. However, there are no obligations on trustees to disclose their status to financial institutions. This is an important deficiency as foreign trusts operate in Norway and have been identified in ML cases. **Norway is rated PC with R.25**.

8. INTERNATIONAL COOPERATION

Recommendation 36 – International instruments

a8.1. In the 3rd Mutual Evaluation Report (MER) Norway was rated LC with the requirements to sign, ratify and implement international conventions (due to deficiencies in the ML offence and preventive measures) and PC concerning the TF Convention and UNSCRs (due to deficiencies in relation to the UNSCRs). Norway has made progress in addressing the ML offence and the UNSCRs are dealt with in R.6.

a8.2. **Criterion 36.1** – Norway is a party to the Vienna, Palermo, Merida and Terrorist Financing Conventions. Norway is not a party to the Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and on the Financing of Terrorism (2005), although it has signed and ratified the predecessor Strasbourg Convention (1990). However, Norway ratified the Council of Europe Convention on Cybercrime (2001) on 30 June 2006.

a8.3. **Criterion 36.2** – Norway has fully implemented the relevant articles of the Vienna, Palermo and TF Conventions by addressing the remaining deficiencies identified in the 3rd MER concerning the ML offence and preventive measures. It should be noted that the Convention requirements do not encompass all the FATF requirements. Norway has also implemented the Merida Convention.

a8.4. **Weighting and conclusion: Norway is rated C with R.36**.

Recommendation 37 - Mutual legal assistance

a8.5. In its 3rd MER, Norway was rated LC with requirements relating to mutual legal assistance. The main deficiency was the application of dual criminality to requests relating to ML/TF activities not fully criminalised in Norway.

a8.6. **Criterion 37.1** – Norway does not have a separate mutual legal assistance act and the legal basis is found in different laws and regulations, such as the *Extradition Act* (*EA*) in Chapter V, the *Courts of Justice Act* in Chapter 2, and the *Regulations relating to International Cooperation in Criminal Matters, December 2012* (*Regulations on International Cooperation*). Norway's laws (e.g., *PC* and *CPA*) may be employed fully in response to foreign requests and may be used to the same extent as in domestic cases. The legal framework in relation to mutual legal assistance does not differentiate between categories of offences and is in principle the same for ML, predicate offences and TF. Norway may provide assistance irrespective of the existence or applicability of a treaty: *EA* s.26(3).

a8.7. **Criterion 37.2** – The *Regulations on International Cooperation* (ss.3 and 10) and the *EA* s.23a designate the MoJ as the central authority for mutual legal assistance. In addition, requests can be sent directly to judicial authorities from Nordic and EU countries (s.3a-d) pursuant to the *European Convention on Mutual Assistance in Criminal Matters* and the *Convention on Mutual Assistance in Criminal Matters between Member States of the European Union*. The MoJ maintains a case management system called *Websak*. However, this records only requests made through the MoJ and not those made directly from or to other authorities. When Norway is notified of urgent cases, incoming requests may be transmitted through formal channels and through Interpol. Requests for assistance in criminal matters are prioritised: *Regulations on International Cooperation* s.5.

a8.8. **Criterion 37.3** – The system for providing mutual legal assistance to Nordic countries is straightforward and not subject to unduly restrictive conditions. The system for mutual legal assistance to EU or Schengen countries is also very streamlined as it allows for direct law enforcement to law enforcement assistance. In all cases involving mutual legal assistance requests from non-Nordic countries (where coercive measures are being sought), dual criminality applies.

a8.9. **Criterion 37.4** – There is no rule under Norwegian law that a mutual legal assistance request must

be refused if the offence is considered to involve fiscal matters, or due to secrecy or confidentiality.

a8.10. **Criterion 37.5** – There are no specific confidentiality requirements relating to the information in mutual legal assistance requests. However, judicial authorities such as the MoJ, courts and LEAs have confidentiality requirements under their own internal or national security protocols.

a8.11. **Criterion 37.6** – Where the measure sought is not a coercive measure, there is no requirement for dual criminality: *EA* s.23a(5). There is also no dual criminality requirement even if coercive measures are required if the mutual legal assistance request originates in a Nordic country.

a8.12. **Criterion 37.7** – Where dual criminality is required for mutual legal assistance, it is sufficient that the conduct underlying the offence is criminalised in both Norway and the requesting country. A difference in the classification of the offence does not affect the dual criminality principle: *EA s.24*. For Nordic countries no dual criminality is required. There is a deficiency with the TF offence since the collection of funds in the knowledge that they are to be used by a terrorist organisation or an individual terrorist (for any purpose) is not criminalised as a stand-alone offence. However, the underlying conduct is criminalised as an attempt to make funds available to terrorists or terrorist organisations (*PC* s.147b), or as an attempt to provide financial or material support to terrorist organisations when the organisation has taken steps to realise the purpose by illegal means: *PC* s.147d. Therefore, given that the conduct is criminalised, the deficiency with the TF offence does not apply to R.37 as the classification of the offence does not affect dual criminality requirements.

a8.13. **Criterion 37.8** – The underlying basis for the mutual legal assistance system in Norway is that a request from a foreign country should be handled in the same way and using the same means as if it were an investigation being carried out by a Norwegian authority. The result of this is that law enforcement authorities may use their powers to obtain information based on their enabling legislation or the *CPA* when executing a request from abroad.

a8.14. **Weighting and conclusion:** The deficiency in the TF offence has a spill-over effect as it may limit assistance due to dual criminality requirements. **Norway is rated LC with R.37**.

Recommendation 38 – Mutual legal assistance: freezing and confiscation

a8.15. In its 3rd MER, Norway was rated PC for confiscation assistance. The main deficiencies were that Norway must start its own domestic proceedings to allow for confiscation in situations other than those covered by the Vienna and Strasbourg Conventions.

a8.16. **Criterion 38.1** – Where a foreign state (that is not a signatory to the Vienna, Strasbourg or Merida Convention) requests Norway to execute a foreign freezing/seizing/confiscation order (including NCB confiscation), Norway can recognise the order, but cannot give effect to it without starting its own proceedings. Regarding confiscation, this could delay any action taken. If a foreign country is a signatory to the Conventions, there is no requirement for Norway to start its own proceedings. In other cases, Norway would need to provide mutual legal assistance, which does not need a treaty, and open its own proceedings.

a8.17. **Criterion 38.2** – Norway's laws do not refer to the enforcement of foreign NCB confiscation requests. Norway considers that NCB confiscation could be available pursuant to a foreign request under *PC s.34*. As noted under R.4 above, although not entirely clear, it appears that some form of NCB confiscation may be possible, but with stringent preconditions. Extended confiscation requires a criminal conviction: *PC* s.34a. Property can be confiscated without a conviction (both domestically and pursuant to a request) when there is a risk that it could be used to commit a crime, or when the owner is unknown or has no known residence in Norway: *PC* s.37b&c.

a8.18. **Criterion 38.3** – There are no formal pre-existing arrangements for coordinating seizure and confiscation actions with other countries, but Norway has a series of national contact points which allow it to co-ordinate appropriately. As with domestic confiscation, there is no specific mechanism through which Norwegian authorities manage certain types of property that has been frozen, seized or confiscated. The LEA that seizes the property is responsible for managing the property, including disposal.

a8.19. **Criterion 38.4** – The MoJ may decide to share confiscated assets with other countries: *PC* s.37d.

a8.20. **Weighting and conclusion:** The restriction on the ability to expeditiously enforce a foreign confiscation order, and the lack of a mechanism to manage confiscated property are minor deficiencies. **Norway is rated LC with R.38**.

Recommendation 39 – Extradition

a8.21. Norway was rated LC in its 3rd MER for requirements concerning extradition. The main deficiency was the effect of the deficiencies in the ML/TF offences on extradition due to dual criminality requirements.

a8.22. **Criterion 39.1** – Any person who is charged, accused or sentenced by a foreign state for a punishable act, and who is in Norway, may be extradited and ML/TF are extraditable offences: *EA* s.1. Extradition with other Nordic countries is governed by the *Convention on the Nordic Arrest Warrant* of 16 November 2012. Extradition to all other countries is regulated in the *EA*, and may only take place if there is dual criminality and the offence is punishable under Norwegian law with imprisonment for more than one year: *EA* s.3. This means that the limitation in the TF offence has an effect on extradition. There are clear procedures for timely execution of extradition requests, and judicial authorities use case management systems. However, cases handled directly by law enforcement agencies through Nordic arrest warrants are not recorded.

a8.23. **Criterion 39.2** – Norway does not extradite its nationals to non-Nordic countries. When extradition is refused because the person in question is a Norwegian national, the case will (upon request) be forwarded to the Prosecution Authority. If considered appropriate, proceedings may take place, including transmission of information relating to the offence.

a8.24. **Criterion 39.3** – Where dual criminality is required for extradition (i.e. with non-Nordic countries), it is necessary that the conduct underlying the offence has been criminalised in both Norway and the requesting country. A difference in the classification or denomination of the offence does not affect the dual criminality principle: *EA* s.3. There is a deficiency with the TF offence since the collection of funds in the knowledge that they are to be used by a terrorist organisation or an individual terrorist (for any purpose) is not criminalised as a stand-alone offence. However, Norway has advised that the underlying conduct will always be criminalised as an attempt to make funds available to terrorists or terrorist organisations (*PC* s.147b), or as an attempt to provide financial or material support to terrorist organisations when the organisation has taken steps to realise the purpose by illegal means: *PC* s.147d. Therefore, given that the conduct is criminalised, the deficiency with the TF offence does not apply to R.39 as the classification of the offence does not affect dual criminality requirements.

a8.25. **Criterion 39.4** – Simplified procedures for extradition are in place for states such as Norway which are parties to the *Schengen Convention*. This allows the direct transmission of extradition requests between the appropriate ministries. Further, if the subject consents to extradition, the extradition request may be decided and processed by the Public Prosecutor: *EA* s.17a(1). For Nordic states, requests for extradition are forwarded directly between the prosecuting authorities, and there can be a simplified decision regarding the arrest warrant if the person sought consents to the surrender.

a8.26. **Weighting and conclusion:** The deficiency in the TF offence has an effect as it may limit Norway's ability to provide assistance when dual criminality is required. **Norway is rated LC with R.39**.

Recommendation 40 – Other forms of international cooperation

a8.27. In its 3rd MER, Norway was rated C with these requirements (see paragraphs 440-450). Norway is a party to the EEA Agreement and transposes and implements EEA relevant Acts adopted at EU level.

a8.28. **Criterion 40.1** – As a matter of policy, Norway's competent authorities give priority to rapid exchange of information with international counterparts in combating ML, associated predicate offences and TF. Norwegian legislation allows for a wide range of information exchange with foreign authorities, and there

is no legal impediment for information to be exchanged both spontaneously and upon request.

a8.29. **Criterion 40.2 – Supervisors:** The FSA has the authority to exchange information with foreign counterparts. Under the *FSA Regulations*, the FSA may assist foreign supervisory authorities that make inquiries related to the ordinary discharge of their supervisory functions and powers: *FS Act* s.4(3). There is nothing that would prevent the FSA from using the most efficient means to cooperate. All information sent and received is registered, safeguarded and processed internally according the *Archives Act* and an encrypted mail solution is used when deemed necessary.

a8.30. **FIU:** The FIU has a sound legal basis for the exchange of information with its foreign counterparts: *MLA* s.30 and *Police Registry Regulation* s.52-5. There are no impediments that would prevent the FIU from using the most efficient means to cooperate. Where possible, information is sent and received via the Egmont Secure Web which provides for a clear and secure channel for the transmission and execution of requests. Most of the FIU's information exchange takes place with other Egmont members. All exchange of information with foreign counterparts is registered in the FIU's database *"Ask"*.

a8.31. **LEAs:** LEAs are permitted to internationally exchange information which is not related to a specific criminal case: *PA* s.24. There is nothing that would prevent LEAs from using the most efficient means to cooperate. Disclosure of information to foreign LEAs takes place via "*Indicia"*, which is a clear and secure gateway. There are clear processes in place to safeguard the information received in criminal cases: *Regulations on International Cooperation*. The protection of the information received is also governed by the *Police Information Registration Act*. The PST can exchange information with foreign police and intelligence authorities, which are approved by the MoJ: *PA* s.17. When the PST investigates cases with international connections, it establishes contacts with foreign counterparts and with Norwegian liaison officers. Intelligence information which is needed as evidence always needs to be confirmed via a formal request through legal channels. The PST gives high priority to foreign requests for information.

a8.32. **Customs authorities:** The Customs Authority is allowed to share information with other countries' customs and excise administrations: *CA* ss.4, 12-1 and chapter 15. The Enforcement Department in the Norwegian Directorate of Customs and Excise administers all incoming and outgoing requests for assistance, including when they come through customs regions. All cases are registered in an electronic case-handling system which is regularly scrutinised to ensure that cases are dealt with in a timely manner. Urgent requests are given priority. Exchange of information with foreign customs authorities is mostly executed by post and e-mail but in urgent cases, is made by phone or e-mail. The absence of a secure gateway to exchange information is an issue for the secure transmission and execution of requests.

a8.33. **Criterion 40.3 – Supervisors:** The FSA does not need an MOU to assist foreign supervisory authorities, though it has established bi-lateral MOUs when requested. The FSA has bi-lateral MOUs with some European countries; the Reserve Bank of India; the US' Securities and Exchange Commission; and the Central Bank of Russia. The FSA also exchanges information based on multi-lateral MOUs, such as the Nordic MOUs which also provide for supervisory cooperation in relation to supervision of particular financial groups. The FSA also closely cooperates with the three European supervisory authorities to support effective regulation and effective supervision across the single EU internal market.

a8.34. **FIU:** The FIU does not need an MOU to be able to exchange information with foreign counterparts, but can sign MOUs upon request. The FIU exchanges information based on the Egmont principles of information exchange which require confidentiality and reciprocity, and these principles are covered in the MOUs it signs.

a8.35. **Law enforcement authorities:** Norway has been a member of Interpol since 1931 and has entered into several agreements with the EU concerning police cooperation. In 2001, Norway signed a cooperation agreement with Europol and has a Norwegian liaison officer at Europol. Communication between the Norwegian police and Interpol and Europol takes place via KRIPOS. Norway has entered into an agreement to the Schengen cooperation in 1999 and to the Prüm Convention (Schengen III agreement) and focusses on combating terrorism. In addition, police are heavily involved in the Nordic Police and Customs Cooperation and have entered into bi-lateral agreements with Russia, Bulgaria and Romania.

a8.36. **Customs authorities:** In addition to customs' mutual assistance agreements (Protocol 11 of the

Agreement on the EEA and the Nairobi Convention), Norwegian customs authorities concluded MOUs with Poland (1990), the Russian Federation (1997) and the Netherlands (1998). Norwegian customs authorities also extensively engage in the Nordic Police and Customs Cooperation referred to above. There is nothing what prevents the customs authorities to provide assistance to foreign counterparts in this regard.

a8.37. **Criterion 40.4** – There are no general impediments which would prevent Norwegian competent authorities from providing feedback regarding assistance received, if so requested. Norwegian authorities report to provide feedback to foreign counterparts upon a specific feedback request from the counterpart and provided some FIU specific examples to support this statement.

a8.38. **Criterion 40.5** – Competent authorities do not refuse requests for cooperation solely on the ground that the request is considered to involve fiscal matters nor do they refuse international cooperation on the grounds of secrecy laws or confidentiality requirements. In general, exchange of information is not made subject to unduly restrictive conditions and in on-going proceedings, international cooperation can be provided, unless the assistance would impede the proceeding. Norway reports that the majority of its cooperation agreements allow for the use of information for tax purposes. Finally, cooperation is not dependent on the nature or status of the requesting counterpart authority.

a8.39. **Criterion 40.6** – Competent authorities strictly protect the information received from their foreign counterparts. The FIU and the FSA will only pass on information obtained from foreign counterparts based on express prior consent. LEAs are obliged to keep confidentiality: s.61a *PCA*, s.24 *PA*. Information received from foreign counterparts regarding criminal investigations is mostly obtained by letter rogatory where the question of using the information in court is part of the agreement. When the police obtain information from foreign counterparts which is not specifically related to a criminal investigation, the information is never passed on without prior consent. Customs authorities only pass information to other authorities than the police when prior consent is received: s12-1 *CA*.

a8.40. **Criterion 40.7** – Competent authorities maintain appropriate confidentiality with regard to requests for information received, consistent with privacy and data protection requirements and with confidentiality rules that are applied to information received from domestic sources. Information exchanged should also be subject to confidentiality by the requesting foreign authority. In general, foreign authorities may only pass on information received from Norway with explicit prior approval. Competent authorities will not exchange information if the requesting counterpart cannot assure effective protection of information, including prior authorisation.

a8.41. **Criterion 40.8** – The FSA may assist foreign supervisory authorities with the discharge of their supervisory functions and can use its power to conduct inquiries on their behalf, including in relation to information held by reporting entities. There is no restriction regarding the type of information to be exchanged and it is in a position to exchange regulatory, prudential and AML/CFT information. The FIU can use its powers to collect additional information based on a request from a foreign counterpart; however, as mentioned in relation to R.29 above, this information does not extend to information to be collected from financial institutions, unless the request matches a specific STR. LEAs are authorised to conduct investigations on behalf of foreign counterparts as outlined above.

a8.42. **Criterion 40.9** – See c.40.2 above. The information provided may only be used for intelligence purposes and not as part of a criminal investigation.

a8.43. **Criterion 40.10** – The FIU provides feedback in accordance with the Egmont criteria for feedback between FIUs. Feedback is provided in cases where the counterpart FIU actively seeks feedback, for instance by attaching a feedback form to the information provided.

a8.44. **Criterion 40.11** – The FIU has a wide range of powers to collect information from financial, administrative and police powers and is able to exchange this information with its foreign counterparts.

a8.45. **Criterion 40.12** – As noted in relation to c.40.2, the FSA has the authority to exchange information with foreign counterparts in relation to the ordinary discharge of their supervisory functions and powers: *FS Act* s.4(3). This includes with respect to the exchange of information for the supervision of AML/CFT

requirements.

a8.46. **Criterion 40.13** – As indicated above in relation to c.40.8, the FSA can legally exchange information domestically available to it, including client specific information, with its foreign counterparts in the EEA. However, as explained in relation to c.40.2, the FSA can only exchange information with certain counterpart supervisors established outside the EEA. The proportionality principle is not a factor that determines the extent to which the FSA responds to foreign requests.

a8.47. **Criterion 40.14** – When relevant for AML/CFT purposes, the FSA is in a position to exchange: (i) regulatory information; (ii) prudential information; and (iii) AML/CFT information. See also c.40.8.

a8.48. **Criterion 40.15** – In addition to conducting enquiries on behalf of foreign counterparts, the FSA may authorise foreign counterparts to conduct inquiries themselves in Norway in order to facilitate group supervision. The Nordic supervisory authorities have signed more detailed MOUs in relation to the supervision of particular financial groups.

a8.49. **Criterion 40.16** – Information received by the FSA from foreign supervisory authorities may only be passed on with the consent of the authority concerned and only for the purposes for which the consent was given: *FSA Regulations* s.3.

a8.50. **Criterion 40.17** – LEAs are permitted to internationally exchange information for both intelligence and investigative purposes as long as the information is not used in the context of a specific criminal case: *PA* s.24. This extends to domestically available information related to ML, predicate offences or TF, including the identification and tracing of the proceeds or instrumentalities of crime.

a8.51. **Criterion 40.18** – LEAs are able to use their domestic powers to conduct enquires and obtain information on behalf of a foreign counterpart based on multilateral or bilateral agreements in place. As indicated in relation to c.40.3 above, Norway extensively cooperates with foreign counterparts based on multilateral agreements in the context of Interpol, Europol, the Schengen agreement and the Prüm Convention. Such cooperation with foreign counterparts is coordinated by Norway's KRIPOS. Finally, in the context of the Nordic Police and Customs Cooperation, liaison officers of Denmark, Sweden and Norway are located around the world. The PST is able to use all of its powers, including coercive measures which also cover undercover operations, when multilateral or bilateral agreements are in place.

a8.52. **Criterion 40.19** – LEAs participate in cooperative investigations with foreign competent authorities, especially the Nordic countries. These cooperative investigations are conducted consistent with chapter 8 of the Agreement between the Nordic countries' law enforcement agencies on police cooperation. A similar arrangement exists within Europol and police authorities participate in that context. Norway reports that the PST has participated in joint investigations into TF offences.

a8.53. **Criterion 40.20** – Indirect exchange of information with foreign non-counterparts is permitted. The FIU often reaches out to foreign counterparts to support on-going investigations within ØKOKRIM. When doing so, it provides the necessary background information to allow its counterparts to make a clear distinction between co-operation sought for the FIU's intelligence purposes and information requested for purely investigative purposes. The information received from a foreign FIU will only be shared with domestic LEAs if the Norwegian FIU receives a formal consent from its counterpart.

a8.54. **Weighting and conclusion:** Competent authorities are generally able to provide a wide range of direct and indirect international assistance, with only minor deficiencies. **Norway is rated LC with R.40**.

Table of Acronyms

3AMLD	EU 3rd Anti-Money Laundering Directive
AA	Auditors Act
AC/AML Project	Anti-corruption and Money Laundering project
Action Plan 2000	Norwegian Government's Action Plan for Combating Economic Crime 2000
Action Plan 2004	Norwegian Government's Action Plan for Combating Economic Crime 2004
AEAA	Authorisation of External Accountants Act
Al-Qaida Regulations	Regulation on sanctions against Al-Qaida of 22 December 1999
AML	Anti-money laundering
AMLD	EU Anti-Money Laundering Directive
ANSC	Association of Norwegian Stockbrokers Companies
BERA	Business Enterprise Registration Act
BNI	Bearer Negotiable Instruments
BRC	Bronnoysund Register Centre
C	Compliant
CA	Customs Act
CBA	Commercial Banks Act
CCR	Central Coordinating Register for Legal Entities
CCRA	Central Coordinating Register for Legal Entities Act
CDD	Customer due diligence
CFT	Counter-terrorist financing
CJA	Court of Justice Act
Circular 9/2004	FSA Circular 9/2004 of 15 April 2004
CLA	Courts of Law Act
COE Corruption Convention	Council of Europe Criminal Law Convention on Corruption
Control Committee	Control Committee for Measures to Combat Money Laundering
Control Committee Regulations	Regulation on the Control Committee for Measures to Combat Money Laundering
CPA	Criminal Procedure Act
CRA	Currency Register Act
CRR	Currency Register Regulations
Customs	Directorate of Customs and Excise
DGPP	Director General of Public Prosecutions
DNFBP	Designated non-financial businesses and professions
DnR	Norwegian Institute of Public Auditors
DOB	Date of birth
DPA	Data Protection Authority
DPP	Director General of Public Prosecutions
EA	Extradition Act
ECHR	European Court of Human Rights
EEA	European Economic Area
Egmont Principles for Information Exchange	Egmont Principles for Information Exchange Between Financial Intelligence Units for Money Laundering Cases

TABLE OF ACRONYMS

EU	European Union
EU Extradition Convention	European Convention on Extradition
EUR	Euros
FATF	Financial Action Task Force
FCA	Financial Contracts Act
FIA	Financial Institutions Act
FIU	Financial intelligence unit
FNH	Norwegian Financial Services Association
FSA	Financial Supervisory Authority (Kredittilsynet)
FS Act	Financial Services Act
FSA Regulations	Regulations concerning the exchange of information with supervisory authorities from countries within and outside the EEA
FT	Financing of terrorism / terrorist financing
HSH	Federation of Norwegian Commercial and Service Enterprises
FUR	Follow-up report
IA	Insurance Act
ISA	International Standards on Auditing and related services
IOPS	International Pension Supervisors Group
IT	Information technology
KRIPOS	National Criminal Investigation Service
LEA	Law Enforcement Agency
LLC Act	Limited Liability Companies Act
LC	Largely compliant
MFA	Ministry of Foreign Affairs
ML	Money laundering
MLA	Money Laundering Act
MLA Prep. Works	Preparatory Works of the Money Laundering Act
MLR	Money Laundering Regulations
MoF	Ministry of Finance
MoJ	Ministry of Justice and Public Security
MOU	Memorandum/memoranda of understanding
MVTS	Money or value transfer service (i.e. money remitter / alternative remittance service)
N/A	Non Applicable
NARF	Norges Autoriserte Regnskapsføreres Forening (Association of Authorised Accountants)
NAST	National Authority for Prosecution of Organised and Other Serious Crime
NBA	Norwegian Bar Association
NC	Non-compliant
NCB	Non-conviction based
NEA	Nordic Extradition Act
NHO	Confederation of Norwegian Business and Industry
NIPA	Norwegian Institute of Public Auditors
NMFA	Norwegian Mutual Fund Association

NOK	Norwegian Kroner
NPD	National Police Directorate
NRA	National Risk Assessment
OECD Bribery Convention	OECD Convention on Combating Bribery of Foreign Public Officials in International Business Transactions
ØKOKRIM	National Authority for Investigation and Prosecution of Economic and Environmental Crime
PA	Police Act
PAA	Public Administration Act
Palermo Convention	United Nations Convention against Transnational Organised Crime (2000)
PC	Partially compliant
PC	Penal Code
PCCC	Police Computer Crime Centre
PEP	Politically exposed person
PLLC Act	Public Limited Liability Companies Act
PF	Proliferation financing
POB	Place of birth
Police Academy	National Police Academy
Police Directorate	National Police Directorate
Population Register	Norwegian Population and Employer Register
Prosecution Authority	Government body responsible for conducting criminal prosecutions (headed by the Director General of Public Prosecutions)
PSP	Payment services provider
PST	Norwegian Police Security Service
PSD	EU Payment Services Directive
RBA	Risk-based approach
RCA	Regulations to the Customs Act
REAA	Real Estate Agency Act
REBA	Real Estate Business Act
Reg.1102	Regulation no.1102 of 30 November 1998 concerning exchange of information with supervisory authorities from countries within and outside the EEA
Regulations on International Cooperation	Regulations relating to International Cooperation in Criminal Matters
Reporting DNFBP or Reporting Designated Non-Financial Businesses and Professions	All non-financial businesses or professions that are obligated to comply with the Money Laundering Act and Regulations
Reporting entity	All entities that are obligated to comply with the Money Laundering Act and Regulations
Reporting FI or Reporting Financial Institution	All financial institutions that are obligated to comply with the Money Laundering Act and Regulations
RFA	Regulations for Advocates
ROK	Advisory Council for Combating Organised Crime
SBA	Savings Banks Act
SFA	Securities Funds Act

TABLE OF ACRONYMS

S/RES/	United Nations Security Council Resolution
SRB	Self-regulating body
SSB	Statistics Norway
STA	Securities Trading Act
STR	Suspicious transaction report
Strasbourg Convention	Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime 1990
Supervisory Council	Supervisory Council for Legal Practice
Taliban Regulations	Regulation on sanctions against Taliban of 8 November 2013
Tax Bulletin	Tax Directorate Bulletin of 5 November 2003
Tax Directorate	Directorate of Taxes
TCSP	Trust and company service provider
Terrorist Financing Convention	United Nations Convention for the Suppression of the Financing of Terrorism (1999)
UN	United Nations
UNCAC	United Nations Convention Against Corruption
UNCTC	United Nations Counter Terrorism Committee
UNSC	United Nations Security Council
USD	United States Dollars
Vienna Convention	United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances 1988

ANNEX:

OVERVIEW OF REGISTERS AND DATABASES USED FOR AML/CFT[1]

Name of Register	Description	Access
FIU database ('Ask')	This is the computer system and register for the FIU. 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. This is maintained by the FIU.	FIU
Register of Cross Border Transactions and Currency Exchange (Currency Register)	This contains all cross-border transactions and currency exchanges reported by financial institutions. This is maintained by Customs.	Customs, tax authorities, police and FIU, FSA, labour and social welfare dept, SSB.
STRASAK	This is the register for the processing of criminal cases, used for registration of information in relation to reports and investigations. STRASAK provides an overview of criminal cases progress, and contains information on both legal motions and in which phase a case has reached until finalisation or conviction. The register provides an overview of the procedure and process for all criminal cases. In STRASAK the object is cases, not persons.	LEAs
Indicia	The police intelligence register used for investigation and prevention of crimes. It is possible to register a wide range of information about suspects, including information about third parties relevant to the suspect.	LEAs
FSA Register	This contains information on all entities (enterprises and individuals) under the FSA's oversight.	FSA
Central Coordinating Register	Contains all relevant information reported to the BRC in line with registration requirements.	Public
Register of Business Enterprises (Business Register)	All Norwegian and foreign business enterprises conducting business in Norway (including companies, partnerships, one-man businesses) must register with the Business Register and are provided a registration number. This is maintained by the BRC.	Public

1 This table includes those registers most relevant to AML/CFT. Other registers which may also be relevant, though which were not discussed on-site, include the following: Police *DNA Registry* and *Photo Registry*; *Passport Register*; *Fingerprint Register*; *Land Register*; *Register of Mortgaged Moveable Properties*; *VAT Register*; *Register of Employers*; and *Register of Bankruptcies*.

ANNEX: OVERVIEW OF REGISTERS AND DATABASES USED FOR AML/CFT

Name of Register	Description	Access
Register of Company Accounts	All Norwegian limited companies, public limited companies, savings banks, mutual insurance companies and petroleum enterprises are obliged to submit their annual accounts (including the auditor's report) and a list of shareholders to the Register of Company Accounts annually. This is maintained by the Tax Authority.	Public
Securities register	Norwegian public limited liability companies (PLLCs) must set up their register of shareholders in a Securities Register that is maintained in Norway. Limited liability Companies (LLCs) may choose to register their shareholders with the Securities register. This is maintained by the Tax Authority or entities on their behalf.	
Corporate Taxation Data Register	This register contains information identifying the shareholders of Norwegian legal persons who are obligated to pay tax in Norway. This is maintained by the Tax Authority.	LEAs; Public (if apply and s.t. conditions
National Population Register	Contains information on all Norwegian citizens and their personal identification number given at the time of birth or citizenship, as well as foreigners who have been granted a D-number. This is maintained by the Tax Authority.	LEAs and competent authorities
Register of Foundations	All foundations are required to be registered which includes the name of the founder, the members of the board, the assets of the foundation, and special rights given to the founder. This is maintained by the BRC.	Public
Registration with the Foundation Collection Control	This is a voluntary registration process for Norwegian NPOs. This is maintained by the Foundation on Collection Control.	Public
Register of NPOs	This is a voluntary register maintained by the Tax Authority to be eligible for tax exemptions. Entities must be registered in the Central Coordinating Register for Legal Entities. This is maintained by the BRC.	Public

www.fatf-gafi.org

December 2014

Anti-money laundering and counter-terrorist financing measures - Norway
Fourth Round Mutual Evaluation Report

In this report: a summary of the anti-money laundering (AML) / counter-terrorist financing (CFT) measures in place in Norway as at the date of the on-site visit (27 March to 1 April 2014). The report analyses the level of compliance with the FATF 40 Recommendations and the level of effectiveness of Norway's AML/CFT system, and provides recommendations on how the system could be strengthened.