Anti-money laundering and counter-terrorist financing measures - Norway

5. Preventive measures

Effectiveness and technical compliance

Citing reference:

FATF (2014), "Preventive measures" in *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

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

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.

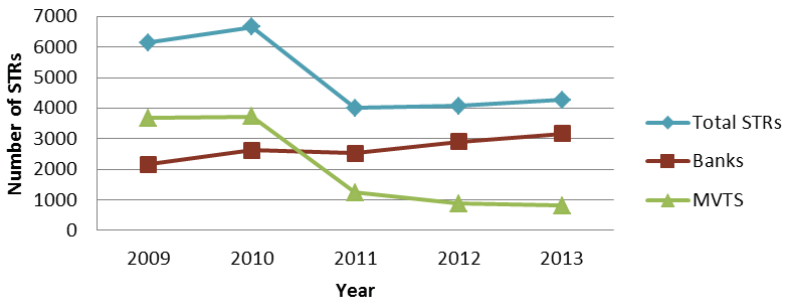
Table 5.2. Number of Reporting Entities

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.

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**.

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