RTDF N° 3-2016 ◆ Septembre 2016

Revue Trimestrielle de Droit Financier

Corporate Finance and Capital Markets Law Review

Doctrine

Colloque

German-French Symposium on Company Law and Capital Markets Law,
Max Planck Institute for Comparative and International Private Law Hamburg – July 7-8, 2016

Chroniques

Bibliographie

THOMSON REUTERS
TRANSACTIVE

SOMMAIRE

Doctrine

Colloque

German-French Symposium on Company Law and Capital Markets Law,

Max Planck Institute for Comparative and International Private Law Hamburg
July 7-8, 2016

SOMMAIRE

Chroniques

Bibliographie

Comité éditorial

Comité international

Abonnement

✂----------

Revue Trimestrielle de Droit Financier – RTDF : 4 numéros par an : 480,00 € TTC / Étranger : 490,00 €

Prénom & Nom : .....

Profession : ..... Raison sociale : .....

Adresse : .....

Code Postal : ..... Ville : ..... Pays : .....

Tél. : ..... eMail : .....

Bulletin et règlement à retourner à ↓

International Financial and White Collar Crime, Corporate Malfeasance and Compliance

Margot Sève, Ph.D.
Skadden, Arps, Slate, Meagher and Flom LLP

Michel Perez, CAMS, MBA
Labex ReFi US Representative; President MAPI, LLC

This section edited by Margot Seve in Paris and Michel Perez in New York aims at presenting and analyzing legal developments related to cross-border enforcement actions in financial and white collar crime cases. It also focuses on the growth of compliance and corporate governance regulatory standards. Comments and suggestions are welcomed, including articles proposals.
Please email your inputs to margot.seve@skadden.com or michelaperez@gmail.com.

Current and Expected Improvements in EU's Anti-Money Laundering and Counter-Terrorist Financing Framework

Sidne Koenigsberg, JD
Skadden, Arps, Slate, Meagher and Flom LLP

Margot Sève, Ph.D.
Skadden, Arps, Slate, Meagher and Flom LLP[1]

The EU Anti-Money Laundering and Counter-Terrorist Financing ("AML/CTF") framework is currently governed by Directive 2005/60/EC dated October 26, 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing (the "Third AMLD").[2] The implementation of the Fourth AMLD, and its recent proposed amendments by the Commission, will soon enhance EU's counter-terrorism framework. In broad terms, the Fourth AMLD aims at strengthening the EU's defences against money laundering and terrorism financing, ensuring the soundness, integrity and stability of the financial system by aligning the EU framework with the 2012 Revised FATF Recommendations, and enhancing the risk-based approach to anti-money laundering ("AML") compliance and supervision. In 2016, in response to the recent terrorist attacks in Europe and Panama paper revelations, the EU accelerated its calendar with respect to the Fourth AMLD and proposed, as have France and the international community, enhanced AML/CTF measures. In light of the Member States' commitment to implement the Fourth AMLD by the end of the year, and the Commission's recent proposal to amend the Directive, we propose in this article to review the main features of the EU's soon-to-be enhanced AML/CTF framework under the Fourth AMLD.

I. Origin of the Fourth AMLD and Related Measures

Following the publication of the Financial Action Task Force's ("FATF") International Standards on combating money laundering and the financing of terrorism and proliferation in February 2012 (the "2012 Revised FATF Recommendations"), the Commission suggested revising the Third AMLD to harmonize the EU's AML standards with FATF's standards. On June 5, 2015, the Directive (EU) 2015/849 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing (the "Fourth AMLD") was published in the Official Journal of the EU. The Fourth AMLD entered into force on June 25, 2015[3]. Member States were initially required to implement the Fourth AMLD by June 26, 2017.

In response to the Paris terrorist attacks of 2015 and the Panama papers revelations, the EU Commission presented in February 2016 an Action Plan[4] for strengthening the fight against terrorist financing with two main tactics: (i) tracing terrorists through financial movements and preventing them from moving funds or other assets; and (ii) disrupting the sources of revenue used by terrorist organizations, by targeting their capacity to raise funds. The Action Plan announced a number of targeted operational and legislative measures, including a draft legislative proposal to better counter the financing of terrorism and to ensure increased transparency of financial transactions and of corporate entities under the preventive legal framework in place in the Union, namely the Fourth AMLD.

In April 2016, in line with UN Security Council Resolutions 2199(2015) and 2253(2015) calling for measures to prevent terrorist groups from gaining access to international financial institutions, the G20 called on the FATF and the

1 The views expressed in this article are those of the authors only. The authors would like to thank Diane Ngouadje and Alize Dill for the quality of their research.

2 The Third AMLD is part of a broader set of measures, including Commission Directive 2006/70/EC dated August 1, 2006 setting forth implementing measures for the Third AMLD, Regulation 1781/2006/EC dated November 15, 2006 ensuring the traceability of funds by requiring information on the payer to accompany transfers of funds, Regulation 1889/2005/EC dated October 26, 2009 on controls of cash requiring persons entering or leaving the EU to declare cash they are carrying if the value amounts to EUR10,000 or more, and EU Council decision 2000/642/JHA dated October 17, 2000 which organizes cooperation between financial intelligence units.

3 The Fourth AMLD was published alongside Regulation (EU) 2015/847 of the European Parliament and of the Council dated May 20, 2015 on information accompanying transfers of funds (the "Revised Wire Transfer Regulation," together with the Fourth AMLD, the "Fourth AMLD Package").

4 Communication from the Commission to the European Parliament and the Council on an Action Plan for strengthening the fight against terrorist financing, COM(2016) 50 final.

Global Forum on Transparency and Exchange of Information for Tax Purposes to make initial proposals to improve the implementation of the international standards on transparency, including on the availability of beneficial ownership information, and its international exchange.

In May 2016, France voted a draft bill which reinforced France's fight against terrorism financing and **organized crime framework, by implementing** preventive measures to detect and monitor terrorist activities, **as well as criminal law measures enhancing** judicial authority to punish such activities. The law also authorizes the French Government to implement the Fourth AMLD by ordinance (*ordonnance)* within six months, and in particular to reinforce France's framework for transparency regarding beneficial ownership information and information on funds transfers to or from non-cooperative jurisdictions.

As explained below, in July 2016, the Commission published a Directive proposal intended to amend the Fourth AMLD in a way to complement the existing preventive legal framework in place in the Union, set out additional measures to better counter the financing of terrorism, and ensure increased transparency of financial transactions and legal entities. The proposed Directive requires that Members States implement the Fourth AMLD by January 1, 2017, at the latest, a commitment previously undertaken by the Ministers of Finance.

II. Main Features of the Fourth AMLD

While the Third and Fourth AMLD cover similar *ratione materiae* (1) and *ratione personae* (2) perimeters, the Fourth AMLD enhances, on a risk-based basis (3), Customer Due Diligence ("CDD") (4) and internal compliance measures (5), as well as Member States' supervisory/sanctions framework (6).

1. Prohibited Activities

In line with the Third AMLD, the Fourth AMLD requires that Member States ensure that money laundering and terrorist financing are prohibited.

The Fourth AMLD clarifies that, when committed intentionally, the following activities shall be regarded as **money laundering** ("ML"):

- the conversion or transfer of property, when knowing that said property is derived from criminal activity;
- the concealment or disguise of the true nature, source, location, disposition, movement, rights with respect to, or ownership of, property, knowing that such property is derived from criminal activity;
- the acquisition, possession or use of property, knowing, at the time of receipt, that such property was derived from criminal activity; or
- the participation in or attempts to aid any of the preceding activities.

While "criminal activities" previously encompassed all "serious crimes" such as terrorist offences, drug dealing, fraud or corruption, the Fourth AMLD extends this definition to include "tax crimes," a concept which each Member State must define. The inclusion of "tax crimes" within the definition of "criminal activity" is an innovation under the Fourth AMLD putting it in line with the Revised FATF Recommendations.

With respect to **Terrorist Financing** ("TF"), the Fourth AMLD reiterates the definition from the Third AMLD. TF means the provision or collection of funds, by any means, directly or indirectly, with the intention that they should be used or in the knowledge that they are to be used to carry out terrorist offences, offences relating to a terrorist group, offences linked to terrorist activities as well as measures aimed at inciting, aiding, abetting or attempting to commit those offences.

2. Scope

Similar to the Third AMLD framework, the Fourth AMLD applies to the following "Obliged Entities":

- credit institutions and financial services institutions;
- trust or company service providers; estate agents;
- other persons trading in goods, such as dealers in precious metals and stones (only for payments made or received in cash of EUR10,000 or more – as opposed to 15.000 under the Third AMLD);
- providers of gambling services (a broader definition than the Third AMLD's "casino"[5]);
- auditors, external accountants and tax advisors; notaries and other independent legal professionals.

Member States can extend the scope of the Directive to other categories of entities if they are likely to engage in activities that participate in ML/TF activities, and must inform the Commission of such decision.

Member States may exempt providers of gambling services (except casinos) or entities that perform financial activities on an occasional or limited basis with little risk of ML or TF from complying with the Directive's provisions. Member States must also inform the Commission of such decision.

3. Enhancement of the Risk-Based approach

The risk-based approach (the "RBA") was initially formulated in FATF's 2003 Recommendations, and was implemented by the Third AMLD as a major innovation. Based on the rationale that ML/TF risks are best regulated following risk and mitigation analysis, the RBA entails that the obligations under the Third AMLD and the Fourth AMLD can be enhanced or simplified in light of the risk associated with each Obliged Entity's activities.

The Fourth AMLD revised the RBA by implementing a three-tier risk identification system, where each tier is responsible for identifying ML-TF risks at its own level:

- at the EU level, the Commission, working with EU level banking, insurance and financial supervisory authorities ("ESAs"),[6] shall identify cross-border ML-TF risks and publish reports every two years;

5 "Gambling services" are defined as "services which involve wagering a stake with monetary value in games of chance, including those with an element of skill such as lotteries, casino games, poker games and betting transactions that are provided at a physical location, or by any means at a distance, by electronic means or any other technology for facilitating communication, and at the individual request of a recipient of services."

6 The ESAs are respectively the European Banking Authority ("EBA"), the European Securities Market Authority ("ESMA") and the European Insurance and Occupational Pension Authority ("EIOPA").

- at the national level, Member States shall identify ML/TF risks within their jurisdictions; and
- at the entity level, Obligated Entities shall review their own risks and report them to the relevant national authority.

Using the RBA, Obliged Entities can apply enhanced or simplified CDD measures in certain situations. Where the risk associated with the business relationship or an occasional transaction is low, Obliged Entities may apply simplified customer due diligence measures ("SDD"); conversely, where the risk associated with the business relationship or an occasional transaction is high, Obliged Entities shall apply enhanced customer due diligence measures ("EDD"), meaning that particularly rigorous customer identification and verification procedures will be required.

While the Directive does not set out in detail how Obliged Entities should assess the risk associated with a business relationship or transaction, nor what SDD and EDD measures entail, on October 21, 2015, the Joint Committee of the ESAs issued a consultation paper setting out draft guidelines on the risk factors to be considered and the measures to be taken in situations where SDD and EDD measures are appropriate. The ESAs are required to issue final guidelines addressed to National Competent Authorities ("NCAs") and Obliged Entities by June 26, 2017 at the latest.

4. Customer Due Diligence

CDD requires that an Obliged Entity verify its customers' identities and beneficial owners, review the purpose and intended nature of its clients' business relationship, and conduct ongoing monitoring of the business relationship.

CDD measures are to be implemented in the following circumstances;

- before establishing a business relationship;[7]
- when carrying out an occasional transaction that either amounts to EUR15,000 or more or constitutes a transfer of funds exceeding EUR 1,000;
- when carrying out occasional transactions in cash amounting to EUR 10,000 for persons trading in goods;
- for providers of gambling services carrying out winnings-related transactions amounting to EUR 2,000;
- when there is a suspicion of money laundering or terrorism financing; or
- when the relevant circumstances of a customer change.

Member States can exempt Obliged Entities from certain CDD measures for "electronic money" under strict conditions including when the purpose of the transaction is exclusively for the purchase of goods or services and the amount of the payment instrument is limited (less than EUR 250).

The Fourth AMLD provides that, while Obliged Entities must apply CDD measures, they can determine their extent on a risk-sensitive basis. In doing so, Obliged Entities must take into account, at a minimum, the risk variables set out in Annex I of the Fourth AMLD, such as the purpose of an account or relationship, the amount of assets to be deposited by a customer, the size of the transaction undertaken, or the regularity or duration of the business relationship. Obliged Entities must be able to demonstrate to NCAs that the CDD measures are proportionate to the identified ML/TF risks.

Obliged Entities that cannot satisfy CDD requirements for a new relationship or occasional transaction may not establish the business relationship or carry out the transaction. If an Obliged Entity cannot complete ongoing monitoring of an existing relationship, it must terminate the relationship. In any of these cases, the Obliged Entity must consider making a suspicious transaction report.

Of note, the Fourth AMLD authorizes Obliged Entities to rely on third parties (such as other Obliged Entities), except those established in high-risk third countries, to meet their CDD requirements. However, the ultimate responsibility for meeting those requirements shall remain with the Obliged Entity relying on third party information. In practice, therefore, such reliance must be reasonable and implies that the Obliged Entity will perform some due diligence on the procedures used by the third party on whom it is relying.

4.1. Beneficial ownership

As provided under the current Third AMLD framework, corporate or other legal entities incorporated within EU Member States are required to obtain and hold accurate information on their beneficial ownership and provide information on their beneficial owners as well as their legal owners to Obliged Entities carrying out CDD measures.

The Fourth AMLD further enhances the clarity and accessibility of information regarding ultimate beneficial owners of corporate entities and trusts, which the Directive recognizes as a "*key factor in tracing criminals who might otherwise hide their identity behind a corporate structure*."

Similar to the Third AMLD, the beneficial owner for corporate entities is defined under the Fourth AMLD as the natural person who owns or controls the relevant entity, directly or indirectly, through more than 25 % of equity interest (although Member States are allowed to set out a lower threshold) or through control *via* other means. In the absence of the identification of such owner, the natural persons holding the position of senior managing officials in the relevant entity shall be considered as the beneficial owners.

Regarding trusts, trustees of any express trust governed by an EU law are also required to obtain and hold adequate, accurate and up-to-date information on the trust's beneficial ownership. Trustees must disclose their status and provide their beneficial ownership information in a timely manner to Obliged Entities when they form a business relationship, or when they carry out an occasional transaction above a range of EUR 1,000 to EUR 15,000 depending on the relevant transaction.

As an innovation, the Fourth AMLD requires Member States to ensure that the information on beneficial ownership relating to corporate and legal entities is held in a central register located within their territory (for example a commercial register, companies register or public register). Member States shall also ensure that the information on beneficial ownership relating to trusts is held in a central register only when the trust "generates tax consequences," which the Directive does not define. The central register shall be made available to NCAs, FIUs, Obliged Entities

7 Member States may allow verification of the client's identity to be completed during the establishment of a business relationship rather than before the establishment of the relationship, if this is necessary to avoid interrupting the normal conduct of business and where there is little risk of money laundering or terrorism financing.

for CDD purposes, and any person or organization demonstrating a "legitimate interest" on ML/TF issues.[8]

4.2. Simplified Customer Due Diligence

As explained above, where Member States or Obliged Entities identify areas of lower ML and TF risk, they may apply SDD measures. Before applying SDD measures, Obliged Entities shall take into account at a minimum the non-exhaustive factors of lower-risk situations provided in Annex II of the Fourth AMLD, which include risk factors related to customers; products, services, transactions; and geographies. For example, customers that are public administration/entities or companies listed on a stock exchange and subject to disclosure requirements regarding beneficial ownership can benefit from SDD. Transactions involving products like pension schemes or life insurance policies would also benefit from SDD. Finally, customers from third countries having effective AML/CTF systems or having a low level of corruption will also benefit from SDD.

Because the Fourth AMLD does not describe the risk assessment process or the substance of SDD measures, the Joint Committee of the ESAs issued draft guidelines in October 2015 elaborating on the risk factors and measures relevant for SDD. Obliged Entities shall comply with the final guidelines (expected by June 26, 2017 at the latest) on a "comply or explain" basis.

SDD is not an exemption from any of the CDD measures but rather an adjustment of the timing, amount or type of each or all of the CDD measures in a way that is proportionate to the low risk identified. For example, the Joint Draft Risk Factors Guidelines explain that generic SDD measures (*i.e.*, applicable to all sectors) may include, but are not limited to, adjusting the timing of CDD (for example verifying the customer's or beneficial owner's identity during the establishment of the business relationship; or verifying the customer's or beneficial owner's identity once transactions exceed a defined threshold or once a reasonable time limit has lapsed); adjusting the quantity or source of information obtained for identification (for example accepting information obtained from the customer rather than an independent source when verifying the beneficial owner's identity); or adjusting the frequency of CDD updates and reviews of the business relationship or transactions.

Financial Institutions providing retail banking services can also take into consideration as part of their risk assessment process specific factors such as whether the customer is a long-standing client whose previous transactions have not given rise to suspicion or concern; whether the product or service is in line with the customer's risk profile; or whether the customer is a credit or financial institution from a jurisdiction with an effective AML/CFT regime and is supervised for compliance with AML/CTF obligations. Banks can also apply SDD when the product involved in the transaction has limited functionality, such as a fixed term savings product with low savings thresholds, a product where the benefits cannot be realized for the benefit of third persons, or a low value loan facility where the legal and beneficial title to the asset is not transferred to the customer until the contractual relationship is terminated[9].

In low risk situations, banks may also verify the identity of a customer that is subject to a statutory licensing based only on evidence of the customer being subject to that regime (for example a search in the regulator's public register); assume that a payment drawn on a sole or joint account in the customer's name at a regulated credit or financial institution in an EEA country satisfies CDD requirements; accept alternative forms of identity, such as a letter from a government agency; or update CDD information only in case of specific trigger events, such as the customer requesting a new or higher risk product.

4.3. Enhanced Customer Due Diligence

EDD measures do not replace regular CDD measures but must be applied in addition to regular CDD measures to mitigate ML-TF risks appropriately in certain high-risk situations. When assessing ML and TF risks, Member States and Obliged Entities shall take into account, at least, the non-exhaustive factors of potentially higher-risk situations as set out in Annex III of the Fourth AMLD.

For example, with respect to customer risk factors, Obliged Entities shall apply EDD measures when the business relationship is conducted in unusual circumstances; when the legal persons or arrangements are personal asset-holding vehicles; for businesses that are cash-intensive; or when the ownership structure of the company appears unusual or excessively complex given the nature of the company's business. EDD measures shall also be applied when one of the following product/service/transaction risk factor is identified: private banking; products or transactions that might favor anonymity; non-face-to-face business relationships or transactions; or payment received from unknown or unassociated third parties. Finally, Obliged Entities shall also apply EDD measures when dealing with certain country risk factors, such as when dealing with countries that are identified by credible sources as having significant levels of corruption or other criminal activity; countries subject to sanctions or embargos; or countries providing funding for or support to terrorist activities.

Similar to SDD, the Joint Draft Risk Factors Guidelines set out general principles to manage high risk situations, as well as an indicative list of generic EDD measures such as increasing the quantity of information obtained about the customer's and beneficial owner's identity and the intended nature of the business relationship, increasing the quality of such information, or increasing the frequency of CDD reviews. With respect to credit institutions, the Joint Draft Risk Factors Guidelines contain sector-specific risk factors that banks should consider alongside the factors of potentially higher-risk situations set out in Annex III to the Fourth AMLD, including customer risk factors, product/services/transaction risk factors, and country risk factors. For example, if the customer is reluctant to provide CDD information or appears deliberately to avoid face to face contact; if the product involves an unusually high volume or large value of transactions; if the transaction involves new delivery channels that have not been tested yet; or if the customer has significant personal or business links to high risk countries.

The Fourth AMLD also lists specific instances that Obliged Entities shall always treat as high risk: (i) when the customer, or the customer's beneficial owner is a politically exposed person; (ii) when entering/maintaining correspondent banking relationships with a third country respondent institution; (iii) when dealing with natural persons or legal entities established in High Risk Third Countries as identified by the EU Commission; (iv) when transactions are

8 While "legitimate interest" is not defined in the Fourth AMLD, it was meant to include investigative journalists and NGOs.

9 See the Joint Draft Risk Factors Guidelines. https://www.eba.europa.eu/documents/10180/1240374/JC+2015+061+(Joint+Draft+Guidelines+on+AML_CFT+RFWG+Art+17+and+18).pdf.

complex or unusually large without obvious economic or lawful purpose.

Dealings with politically exposed persons is one of the specific instances identified under the Fourth AMLD that creates as a high risk situation where Obliged Entities must apply EDD.[10] The requirement to apply EDD measures, which was limited to foreign PEPs only under the Third AMLD, is expanded under the Fourth AMLD to apply to domestic PEPs, in line with the 2012 Revised FATF Recommendations. Upon identifying that a customer or beneficial owner is a PEP, Obliged Entities shall, in addition to CDD measures, obtain senior management[11] approval for establishing or continuing business relationships with PEPs, take adequate measures to establish the source of wealth and source of funds that are involved in the business relationships or transactions with such persons, and conduct enhanced and ongoing monitoring of those business relationships. [12]

With respect to correspondent banking relationships[13] with respondent institutions from third countries, EU financial institutions shall, in addition to CDD measures, apply specific EDD measures such as gathering sufficient information about the respondent institution on its business, reputation and the quality of its supervision; assessing the respondent institution's AML/CTF controls; and obtaining approval from senior management before establishing new correspondent relationships. Obliged Entities are prohibited from entering into, or continuing, a correspondent relationship with a shell bank.

Further, in contrast to the Third AMLD, the Fourth AMLD establishes a new third country policy based on a black list of countries deemed "non-equivalent" due to "strategic deficiencies" in their AML/TF regime. Any funds transfer flowing to or from high risk countries, or natural persons or legal entities established in high risk third countries, as identified by the Commission, shall trigger the application of enhanced customer due diligence measures.[14]

The Fourth AMLD does not set out exactly what the EDD measures entail in respect of dealings with natural or legal persons established or residing in a High Risk Third Country. The Draft Guidelines provides an indicative list of generic EDD measures such as collecting information on the customer's and beneficial owner's family members; and establishing that the source of wealth and funds involved are not ML/TF proceeds.

Finally, Obliged Entities are required to examine, as far as reasonably possible, the background and purpose of all complex and unusually large transactions, and all unusual patterns of transactions having no apparent economic or lawful purpose. Pursuant to the Draft Guidelines, transactions are deemed unusual if they are larger than what would normally be expected, or are very complex compared to similar transactions. Upon identification of unusual transactions, Obliged Entities shall take measures to understand the background and purpose of these transactions (such as establishing the source and destination of the funds); and monitor the business relationship and subsequent transactions more frequently and with greater attention to detail.

5. Compliance-related Obligations under the Fourth AMLD

5.1. Reporting Obligations

Similar to previous AML directives, the Fourth AMLD provides that each Member State shall establish a financial intelligence unit (the "FIU") to detect, prevent and effectively combat ML and TF. The purpose of FIUs is to establish links between suspicious transactions and underlying criminal activity. FIUs shall be responsible for receiving and analyzing suspicious transaction reports (the "STR") and other information relevant to ML or TF, in order to address specific transactions as well as larger ML/TF trends. The Fourth AMLD innovates by requiring that FIUs shall be operationally independent and autonomous in carrying out their tasks.

Similar to the Third AMLD, Obliged Entities must report all suspicious transactions, including attempted transactions, to the FIU (*e.g.* Tracfin in France, the UK Financial Intelligence Unit (UKFIU) in the UK), regardless of the amount of the transaction. The Fourth AMLD categorically prohibits Obliged Entities from performing transactions which they know or suspect to be related to proceeds of criminal activity or TF until they have informed the FIU or complied with any specific instruction from the FIU or the NCAs in compliance with relevant national laws.

Obliged Entities and their directors and employees shall not disclose to customers the fact that information is being, will be or has been transmitted to an FIU. This "tipping off" prohibition does not apply to disclosure to the competent authorities or disclosure for law enforcement purposes.

10 Politically Exposed Persons are natural persons who are or have been entrusted with prominent public functions including the following: heads of state, heads of government, ministers and deputy or assistant ministers; members of parliament or similar legislative bodies; members of the governing bodies of political parties; members of supreme courts, constitutional courts or other high-level judicial bodies whose decisions are not subject to further appeal, except in exceptional circumstances; members of courts of auditors or the boards of central banks; ambassadors, chargés d'affaires and high-ranking officers in the armed forces; members of the administrative, management or supervisory bodies of state-owned enterprises; directors, deputy directors and members of the board or equivalent function of an international organization.

11 "Senior management" means an officer or employee with sufficient knowledge of the institution's money laundering and terrorist financing risk exposure and sufficient seniority to take decisions affecting its risk exposure, and need not, in all cases, be a member of the board of directors.

12 Note that EDD measures extend to PEPs' family members and close associates. Where a person is no longer a PEP, Obliged Entities must, for at least 12 months, consider the continuing risk posed by that person, and apply risk-sensitive measures until such person is deemed to pose no further risk.

13 Defined by the Directive as "*the provision of banking services by one bank as the correspondent bank to another bank as the respondent, including providing a current or other liability account and related services (like cash management, international funds transfers, cheque clearing, payable-through accounts and foreign exchange services); or the relationships between and among credit institutions and financial institutions including where similar services are provided by a correspondent institution to a respondent institution, and including relationships established for securities transactions or funds transfers.*"

14 By a Delegated Act of July 14, 2016, the Commission issued a list of high risk third countries organized into three categories: (i) high risk third countries which have provided a written high-level political commitment to address the identified deficiencies and have developed an action plan with FATF (Afghanistan, Bosnia and Herzegovina, Guyana, Iraq, Lao PDR, Syria, Uganda, Vanuatu, Yemen), (ii) high risk third countries which have provided a high-level political commitment to address the identified deficiencies, and have decided to seek technical assistance in the implementation of the FATF Action Plan (Iran) (iii) and high risk third countries which present ongoing and substantial money laundering and terrorist financing risks, having repeatedly failed to address the identified deficiencies and which are identified by FATF Public Statement (Democratic People's Republic of Korea).

Notaries, other independent legal professionals (including lawyers), auditors, external accountants and tax advisors are exempted from reporting obligations only to the strict extent that such exemption relates to privileged and confidential information (namely information received in the course of ascertaining the legal position of their client, or information received in the course of performing their task of defending or representing that client in judicial proceedings)

These professionals will also not be considered as having "tipped off" their clients if they sought to dissuade a client from engaging in illegal activity.

Finally, Member States shall ensure that individuals (including employees and representatives of the Obliged Entity) who report suspicions of ML/TF (either internally or to the FIU) are protected from being exposed to threats or hostile action, and in particular from adverse or discriminatory employment actions.[15]

5.2. Training, Policies & Procedures and Document Retention

The Fourth AMLD articulates the minimum required elements of an Obliged Entity's AML-CTF compliance program.

Obliged Entities must set up policies, controls and procedures must encompass model risk-management practices, customer due diligence, reporting, record-keeping, internal control, compliance management and employee screening. An independent audit function within Obliged Entities must also test the internal policies, controls and procedures.

Obliged Entities that are part of a group must implement group-wide policies and procedures (including data protection policies and policies and procedures for sharing information within the group for AML-CTF purposes).

Obliged Entities must also ensure that their employees are aware of the provisions adopted pursuant to the Fourth AMLD. Obliged Entities shall provide ongoing training programs to their employees to help them recognize operations which may relate to ML or TF, and explain to employees how to proceed in such cases. Obliged Entities are required to maintain up-to-date information on the practices of money launderers and financers of terrorism and on indications leading to the recognition of suspicious transactions. Obliged Entities shall identify the member of their management board responsible for compliance.

Policies and procedures shall be implemented at the level of branches and majority-owned subsidiaries in Member States and third countries. The NCA of the home Member State of the Obliged Entity is responsible for supervising the Obliged Entity's application of group-wide AML-CTF policies and procedures; this could involve on-site visits in establishments based in another Member State.

Finally, Obliged Entities are required to retain specific documents (including a copy of the documents and information necessary to comply with the CDD requirements, as well the evidence necessary to identify the relevant transactions) for a period of five years, after the end of the business relationship with the customer or after the date of an occasional transaction. Upon expiry of the five year retention period, Obliged Entities are required to delete personal data, unless otherwise provided for under national law. Note that, with respect to data protection, Obliged Entities shall process personal data for the purposes of the prevention of ML or TF only. The Fourth AMLD specifies that the processing of personal data for any other purposes, such as commercial purposes, is prohibited.

6. Supervision and Sanctions

The supervision and enforcement of AMLD provisions is the reponsbility of "National Competent Authorities" ("NCAs"). Although the Fourth AMLD does not define NCAs, they are to be understood as referring to all public authorities with designated responsibilities for combating ML/TF. The 2012 Revised FATF Recommendations clarify that competent authorities include, among others, the FIU (such as Tracfin in France), authorities that have the function of investigating and/or prosecuting money laundering and terrorist offences (such as the prosecutor's office in France), and authorities that have AML/CTF supervisory or monitoring responsibilities aimed at ensuring compliance by Obliged Entities (such as, in France, the Prudential and Resolution Supervisory Authority (ACPR) for the banking and insurance sectors, and the Financial Markets Authority (AMF) for investment firms).

NCAs must have on-site and off-site access to all relevant information on the specific domestic and international risks associated with customers, products and services of Obliged Entities. NCAs must base the frequency and intensity of on-site and off-site supervision on the risk profile of Obliged Entities and on the risks of ML and TF in that Member State.

With respect to sanctions for non-compliance, Member States shall lay down rules on administrative sanctions. Member States are further required to ensure that Obliged Entities can be held liable for breaches of relevant national provisions, and that NCAs have all the supervisory and investigatory powers necessary to exercise their functions and impose sanctions.

As an innovation, administrative sanctions are to be imposed by NCAs, at a minimum, to breaches that are **serious, repeated, systematic**, or a combination thereof, of the requirements on CDD, suspicious transaction reporting, record-keeping, and internal controls.[16] In all these cases, Member States are required to apply specific minimum administrative sanctions, including a maximum administrative pecuniary fine of at least twice the amount of the benefit derived from the breach where the benefit may be determined, or at least EUR 1,000,000. Decisions imposing administrative sanctions shall be published by the NCAs on their official website.

Sanctions are increased for credit institutions, who can be fined at least EUR 5,000,000 or 10 % of the total annual turnover. Natural persons can be fined a maximum admin-

15 Recital 41 to the Fourth AMLD explains that there have been a number of cases of employees reporting suspicions of ML or TF being subjected to threats or hostile action. As a result, Member States should be aware of the problem and do whatever they can to protect individuals, particularly in respect of their personal data and their rights to effective judicial protection and representation.

16 The other administrative sanctions and measures that can be applied by NCAs include a public statement identifying the natural or legal person and the nature of the breach, an order requiring the natural or legal person to cease the conduct and to desist from repetition of that conduct, a withdrawal or suspension of the Obliged Entity's authorization (where applicable), and a temporary ban against any person discharging managerial responsibilities in an Obliged Entity, or any other natural person held responsible for the breach, from exercising managerial functions in Obliged Entities.

istrative fine of at least EUR 5,000,000. It is important to note that the Fourth AMLD does not restrict liability under the Fourth AMLD to members of the management body, but extends it to any other natural persons who are responsible for the breach of the relevant provisions, such as the Head of Compliance.

III. Recent Development and Next Steps

In July 2016, pursuant to its Action Plan prompted by the 2015 Paris terrorist attacks and the Panama papers revelations, the Commission published a Directive proposal intended to amend the Fourth AMLD in a way to complement EU's existing preventive legal framework.[17] The Commission explained that "*the globally interconnected financial system makes it simple to hide and move funds around the world, by quickly and easily setting up layer upon layer of paper companies, crossing borders and jurisdictions and making it increasingly difficult to track down the money. Money launderers, tax evaders, terrorists, fraudsters and other criminals are all able to cover their tracks in this way*."

The Commission's Directive proposal amends the Fourth AMLD by strengthening the following points:

- Apply enhanced due diligence measures towards high risk third countries;
- Bring virtual currency exchange platforms under the scope of the Directive;
- Strengthen transparency measures applicable to prepaid instruments, such as prepaid cards, by lowering thresholds for identification from €250 to €150 and expanding customer verification requirements;[18]
- Enhance the powers of Financial Intelligence Units and facilitate their cooperation by further aligning the rules for such Units with the latest international standards;[19] and
- Give Financial Intelligence Units swift access to information on the holders of bank-and payment accounts, through centralised registers or electronic data retrieval systems.[20]

In addition to amending the Fourth AMLD, the Commission is also to publish, as part of its Action Plan, a Directive on criminal offences and sanctions for money laundering by the end of the 4th quarter 2016, and an assessment with regards to a possible European system complementing the existing EU-US Terrorist Finance Tracking Program agreement. Indeed, as explained in the Action Plan, while all Member States have criminalised money laundering, there are differences between Member States as to the definition of money laundering and the sanctions applied. These differences create obstacles in cross-border judicial and police cooperation to tackle money laundering, and have a direct relevance to action against terrorist financing. The objective of the Commission's proposal will be to introduce minimum rules regarding the definition of the criminal offence of money laundering (applying it to terrorist offences and other serious criminal offences) and to related sanctions.

In the French context, the implementation in June of France's anti-terrorism law reinforced France's national counter terrorism financing framework,[21] by limiting the circulation of important sums of money, limiting the amount of money stocked on prepaid cards, and reinforcing the traceability of transactions processed using prepaid cards. TRACFIN, France's FIU, is now also authorized to provide information to financial institutions on individuals, companies or transactions raising high TF risks, so that banks can apply enhanced monitoring measures regarding the designated persons/transactions. To facilitate evidence gathering at customs, the law further sets forth for a presumption of illegal origin of the funds when material, legal or financial circumstances pertaining to the import, export or clearing of funds cannot be explained by any motive other than hiding the origin of the funds. The new law also revises France's criminal procedure by offering new investigatory tools to judges and prosecutors, such as night raids and wiretapping. Finally, as explained above, the June 2016 law authorizes the French Government to implement the Fourth AMLD within six months. France's implementation of the Fourth AMLD in national law will be presented and discussed in this Review under this section when completed.

17 Proposal for a Directive of the European Parliament and of the Council amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing and amending Directive 2009/101/EC.

18 As explained in the Commission's Action Plan, the terrorists who committed the attacks in Paris on 13 November 2015 reportedly used prepaid cards to pay for hotel rooms.

19 As explained by the Commission, centralised registers at national level allow for identification of all national bank accounts belonging to one person, or other similar mechanisms such as "central retrieval systems." They are used by law enforcement authorities to facilitate financial investigations, including those relating to terrorism financing. The establishment of these centralised registers or electronic data retrieval systems in all Member States will rapidly provide FIUs (or other competent authorities) with information on the identity of holders of bank and payment accounts. In parallel, the Commission will look into the possibility of a distinct legal instrument to broaden the scope for accessing these centralised bank and payment account registers for other purposes (*e.g.* law enforcement investigations, including asset recovery, tax offences) and by other authorities (*e.g.* tax authorities, Asset Recovery Offices, other law enforcement services, Anti-corruption authorities). Any initiative would have to be accompanied by appropriate safeguards, in particular as regards data protection, and conditions of access.

20 As indicated by the Commission, FIUs play an important role in identifying the financial operations of terrorist networks across borders and in detecting their financial backers. International standards now emphasise the importance of extending the scope of and access to information available to FIUs (that information is currently limited in certain Member States by the requirement that a prior Suspicious Transaction Report has first been made by an Obliged Entity). The Commission proposes to amend the Fourth AMLD to enhance the access to information available to FIUs.

21 Loi n° 2016-731 du 3 juin 2016 renforçant la lutte contre le crime organisé, le terrorisme et leur financement, et améliorant l'efficacité et les garanties de la procédure pénale.