WILLIAM FRY

Financial Regulation Unit

September 2019

Central Bank of Ireland AML/CFT Guidelines for the Financial Services Sector

On 6 September 2019, the Central Bank of Ireland ("**CBI**") published revised 'Anti-Money Laundering and Countering the Financing of Terrorism Guidelines for the Financial Sector' (the "**Guidelines**") to assist regulated entities to comply with their obligations under the recently amended Criminal Justice (Money Laundering and Terrorist Financing) Act 2010 (the "**2010 Act**") (see our Briefing on the 2018 amendments to the 2010 Act here).

This Briefing sets out some of the key legislative requirements under each of the headings below and highlights some of the key guidance in relation to each area.

Overview

The Guidelines outline the CBI's expectations of credit and financial institutions ("**Firms**") when conducting business-wide risk assessments, which involves identifying, assessing and managing money laundering and terrorist financing ("ML/TF") risks — a statutory requirement under the 2010 Act.

The Guidelines are more principles-based than their predecessor which reflects the trend in anti-money laundering legislation to move towards a risk-based approach rather than a "tick the box" approach to mitigating ML/TF risks. For this reason, a Firm's culture, from the board of directors to front-line employees, is highlighted by the CBI in these Guidelines as crucial to meeting the regulator's expectations.

Risk Management

- **Firms are required to apply a risk-based approach when applying ML/TF compliance measures to customers or areas of business**
- **Firms are required to conduct a business-wide risk assessment**

As expected, there is a notable departure from the approach set out in the former Guidelines, which lists various examples of documentation that can be relied upon in the identification of a customer or beneficial owner, together with methods that can be employed to verify that identify and mitigate ML/TF risks. The Guidelines do not contain similar guidance and therefore the process of documenting the identity, and the verification of that identity, is now to be determined on the basis of the business risk assessment. A risk assessment should consist of two distinct but related steps: identifying ML/TF risks relevant to a Firm's business; and assessing the identified ML/TF risks in order to understand how to mitigate those risks.

- **The 2010 Act sets out risk factors that Firms must consider when conducting their business-wide risk assessment and must include considerations of at least the following: the customer, the customer's products and services, the types of transaction carried out, geographic areas and delivery channels**

The Guidelines set out risk factors that may be relevant to consider when a Firm is conducting a business risk assessment – the Guidelines helpfully propose questions and considerations that Firms should consider under each category. For example, in considering the risk presented by any particular customer, the Firm, where appropriate, should have regard to: (i) the customer's business and professional activities; (ii) their reputation insofar as it informs the firm about their financial crime risk; and (iii) whether there is anything suspicious about the customer's behaviour.

The Guidelines explain "geographic risk" and outline what a Firm should know about a customer's or beneficial owner's location, such as whether the relevant jurisdiction has an effective anti-money laundering and counter financing terrorism ("**AML/CFT**") regime and the purpose for the customer/beneficial owner being established there.

With respect to the balancing of risk factors, Firms should take a holistic view and be mindful of financial inclusion. Firms should weigh risk factors dependent on their relative importance.

The Guidelines address the use of IT systems to allocate risk scores to business relationships or transactions and outline expectations about a Firm's management of such a system. Firms should ensure that internal AML/CFT systems and controls can identify emerging risks and lists examples of the sorts of systems and controls that Firms should have in place to identify such risks.

Such risk detection systems should include regular reviews of relevant information sources produced by AML/CFT dedicated bodies, for example, the Financial Action Task Force and the United Nations.

Customer Due Diligence ("CDD")

- **Firms are required to identify the risk level presented by a customer or transaction to determine the level of CDD to be applied**

The requirement for a Firm to identify the risk level presented by a customer reflects the trend contained in MLD4, and the 2018 Act transposing it, towards a "risk-based" approach to CDD. This approach is less prescriptive and seeks to shift the onus of risk identification over to Firms to identify risk levels and document their rationale for prescribing a low or high-risk level to a particular customer or transaction. This approach moves away from the "tick the box" approach to CDD that prevailed in the previous Guidelines.

CDD is "more than just verifying the identity of a customer". A Firm should collect sufficient information to ensure that it knows its customer, persons purporting to act on behalf of the customer and the customer's beneficial owners. In addition, a Firm should know what it should expect from doing business with that customer and be alert to any potential ML/TF risks arising from the customer relationship.

Firms are instructed to document their determination of the level of risk ascribed to any customer or transaction. The Guidelines outline a number of steps for Firms to follow when conducting CDD, such as ensuring there is a timeframe for the Firm's completion of CDD. Firms are obliged to maintain a list of documents that they consider are capable of satisfying CDD and verification requirements.

With respect to the use of technology to conduct CDD, the Guidelines note that the 2010 Act is technology neutral. Where a Firm chooses to employ RegTech solutions, Firms remain responsible for ensuring compliance with ML/TF legislation.

Firms may rely on third parties to carry out CDD provided that a number of criteria are met, such as having a clear contractual agreement in place that allocates obligations between the parties and ensuring that the outsourced provider can provide the requisite CDD information to the Firm in a timely manner. The Guidelines are very clear that in such circumstances, responsibility for ensuring compliance with the 2010 Act remains with the Firm.

- **Firms must monitor on an on-going basis any business relationship that it has with a customer to the extent reasonably warranted by the risk of ML/TF**

The Guidelines set out expectations relating to the gathering of information on beneficial ownership and processes to be followed when establishing new business relationships. The Guidelines explain that the Firm should identify what information is required by the Firm in order to satisfy itself that it has the requisite knowledge to adequately monitor a customer's activity and be able to identify unusual transactions.

Firms must have effective policies that: specify 'trigger events' associated with their customers that are indicative of a heightened ML/TF risk; provide for periodic reviews; provide for politically exposed persons ("**PEP**") screening; and provide for proactive utilisation of customer contact as an opportunity to update CDD. Trigger events and the monitoring programme in general must be well-documented and well-established. Staff should also be trained in how to undertake periodic reviews.

- **Firms may apply simplified customer due diligence ("SDD") measures when reasonably warranted by the low level of ML/TF risk**

As the 2010 Act (as amended) no longer provides for specific circumstances when SDD can be applied, SDD should only be applied on the basis of a business risk assessment i.e. Firms may adjust the amount, timing or type of each or all the SDD measures to be undertaken that are commensurate with the low level of ML/TF risk attributable to that customer or business as identified by the Firm.

- **Firms are required to undertake enhanced customer due diligence ("EDD") in certain situations, such as when the customer, or a relevant beneficial owner, is a PEP**

The Guidelines specify that Firms should apply risk proportionate levels of EDD measures where the ML/TF risk so warrants. The Guidelines are prescriptive in specifying the various EDD measures that should be applied by Firms, such as, seeking additional documentation, including the customer's source of wealth, and additional information about the customer's business. The Guidelines outline the policies and procedures a Firm should have in place which include: how to determine whether a customer or beneficiary is a PEP; how to manage PEP relationships; third party reliance in relation to PEPs; the allocation of responsibility for the approval of PEP relationships and approval by senior management; and enhanced on-going monitoring of PEPs. Similarly, when dealing with customers from high-risk third countries or other high-risk situations, Firms should make an informed decision about which EDD measure are appropriate for each high-risk situation.

- **Firms are required to undertake EDD when establishing corresponding relationships with respondent institutions outside the EU**

The Guidelines refer to the expanded definition of "correspondent relationships" under the 2010 Act. The Guidelines make clear that a "corresponding relationship" may exist where there is no underlying third party customer – for example, between firms acting on a principal-to-principal basis. Firms are enabled to apply differing levels of CDD to correspondent relationships in accordance with the Firm's own risk assessment.

Governance

- **Firms are obliged to adopt policies and procedures to facilitate the detection of ML/TF**
- **Firms that are part of a group, or Firms that operate a branch, a majority-owned subsidiary or an establishment outside the State, are required to implement group-wide ML/TF policies and procedures**

The Guidelines are prescriptive in setting out the CBI's expectations surrounding ML/TF risk management by different layers of governance within a Firm. The CBI has frequently commented on the importance of a culture of compliance and expects Firms to be proactive in bringing matters to the CBI's attention.

Senior management, including the board of directors, are responsible for managing the identified ML/TF risks by demonstrating active engagement with the mitigation of those risks.

A Firm's AML/CFT policies and procedures should be maintained, supplemented by guidance, demonstrate compliance with all legal and regulatory compliance and have clearly defined processes in place for their review.

The Guidelines specify the roles and responsibilities of senior management, the MLRO, the Risk Officer (where relevant) and the Compliance Officer (where relevant). Roles should be clearly defined and documented.

The Guidelines also specify that there should be appropriate governance and oversight in relation to business-wide risk assessments; policies and procedures; reporting lines; senior management meetings and AML/CFT resourcing. Discussions at senior management meetings which concern AML/CFT should be evidenced and recorded appropriately. Similarly, records and appropriate evidence should be maintained in relation to decisions regarding PEPs and correspondent relationships.

Reporting of Suspicious Transactions

- **Firms are required, when the requisite suspicion arises, to submit a suspicious transaction report ("STR") to An Garda Síochána and the Revenue Commissioners**

The CBI has frequently stated the importance of STRs and has described STRs as playing a "pivotal role" in the fight against ML/TF.

Firms are instructed to consider attempted transactions, as well as completed transactions, when assessing potentially suspicious transactions. There is no minimum monetary threshold that is too low to raise suspicions.

The Guidelines set out a non-exhaustive list of examples of incidents that might raise suspicions, such as, the occurrence of unnecessarily complex transactions or those that do not appear to make economic sense.

The Guidelines define what "as soon as practicable" means in the context of the time by which the CBI expects STRs to be submitted, as well as operational internal reporting procedures that Firms must have in place. Firms should retain the information that gave rise to the Firm's suspicion, and document information pertaining to the Firm's decision to either discount a suspicion that was raised or to proceed to file an STR with the authorities.

STRs are submitted to the Financial Intelligence Unit ("**FIU**") of An Garda Síochána via the goAML application and the same should be submitted to the Revenue Commissioners by mailing a hard copy of the submitted STR from the goAML application.

The Guidelines also refer to the offence of "tipping-off" and state that Firms should include details of this offence in policies and procedures together with advice on how to handle unusual transactions and requesting additional due diligence information without committing the offence of "tipping-off".

Training

- **Firms must ensure staff are instructed on the law relating to ML/TF and are provided with ongoing training to identify a transaction or activity that may relate to ML/TF and to know how to proceed once such a transaction or activity is identified**

The CBI has highlighted the importance of well-trained staff as a "critically important control" for Firms in the detection and prevention of ML/TF risks. Training should be tailored to the nature, scale and complexity of the Firm's operations and should be proportionate to the level of ML/TF risk faced by the Firm and the Guidelines explain how Firms can achieve training compliance. Staff should be trained in relation to the Firm's AML/CFT policy.

Training may be outsourced but the outsourcing Firm is responsible for ensuring that the service provider is itself appropriately trained in several areas including the ML/TF law applicable to the Firm.

Record Keeping

- **Firms are required to retain records in relation to business-wide risk assessments, customer information and transactions**

Firms are advised to also retain records in relation to the following: internal and external STRs; investigations and STRs; details of reliance on third parties to undertake CDD; minutes of relevant senior management meetings; and AML/CFT training and ongoing monitoring of customers.

International Financial Sanctions

- **Firms are obliged to comply with EU Council Regulations concerning sanctioned individuals or entities**
- **Firms must report any transaction with a sanctioned individual or entity to the CBI and immediately freeze any relevant account/stop the transaction immediately**

The Guidelines outline the various sanctions frameworks that apply to Firms, namely, the EU Sanctions regime and the United Nations Sanctions regime and provide information on where to find up-to-date sanctions lists. True sanctions hits should be reported directly to the CBI.

Firms should have effective screening systems in place to detect any activity with sanctioned persons or entities and such screening procedures should be appropriate to the nature, size and risk of the Firm's operations.

Looking forward

The proposed financial services Guidelines provide useful clarity in addressing AML/CFT requirements under the recently amended 2010 Act.

With the Council of the European Union's recent 'AML Action Plan' which calls on European Central Banks to further monitor AML compliance, and the recently amended AML legislation, AML/CFT will remain an enforcement priority of the CBI throughout 2019 and beyond.

How can William Fry help?

William Fry can assist Firms in relation to:

- reviewing internal policies and procedures, and contracts, to ensure they comply with current AML/CFT legislation;
- reviewing and updating Firm processes in carrying out CDD;
- providing training and advice with regards to AML/CFT compliance; and
- AML/CFT inspections and regulatory enforcement action.

Contact Us

For more information, please contact Shane Kelleher, Louise McNabola or your usual William Fry contact.

Shane Kelleher
Partner,
Head of Financial Regulation Unit

+353 1 639 5148
shane.kelleher@williamfry.com

Lisa Carty
Partner,
Litigation & Dispute Resolution

+353 1 639 5386
lisa.carty@williamfry.com

John Larkin
Partner,
Insurance & Reinsurance

+353 1 639 5224
john.larkin@williamfry.com

Patricia Taylor
Partner,
Asset Management & Investment Funds

+353 1 639 5222
patricia.taylor@williamfry.com

John Aherne
Partner,
Asset Management & Investment Funds

+353 1 639 5321
john.aherne@williamfry.com

Louise McNabola
Senior Associate,
Banking & Finance

+353 1 639 5196
louise.mcnabola@williamfry.com