



CARNE


WE CONNECT THE DOTS.

ETA: 1h20m
DIRECTION: E

SAIL AREA: 1020 m²
CRUISING SPEED: 11 knots
GROSS TONNAGE: 630

Regulatory Update (Ireland)

Criminal Justice (Money Laundering and Terrorist Financing) (Amendment) Act 2018



On 6th September 2019, the Central Bank of Ireland (“CBI”) issued the Anti Money Laundering and Countering the Finance of Terrorism Guidelines for the Financial Sector (“the Guidelines”) following enactment of the Criminal Justice (Money Laundering and Terrorist Financing) (Amendment) Act 2018. The Guidelines set out the expectations of the CBI regarding factors that Firms should take into account when identifying, assessing and managing Money Laundering (“ML”) and Terrorist Financing (“TF”) risks. The Guidelines no longer include prescriptive / definitive examples of documentation that the CBI consider would satisfy customer identification and verification requirements. Below is a summary of the key changes.

Customer Due Diligence (“CDD”)

◀▶ Timing of CDD

The Guidelines state that whilst Firms can avail of Section 33(5) of the Criminal Justice (Money Laundering and Terrorist Financing) Act 2010 (as amended) (“the CJA 2010”) and identify and verify the customer and beneficial owner(s) as soon as practicable during the establishment of the business relationship, Firms should document and retain their reasons for doing so. However, the Guidelines emphasize that in line with Section 33(6) of the CJA 2010, transactions may not be carried out by or on behalf of the customer and beneficial owner(s) until CDD is complete.

Guidelines also list a number of SDD measures which Firms may apply including but not limited to:

- Adjusting the frequency of CDD updates and reviews of the business relationship, depending on the level of risk associated with that customer and adjusting the frequency and intensity of transaction monitoring, for example by monitoring transactions above a certain threshold only. Where Firms choose to do this, they should ensure that the threshold is set at a reasonable level and that they have systems in place to identify linked transactions that, together, would exceed that threshold. They go on to state that SDD is not a “de facto exemption from CDD”

◀▶ Simplified Due Diligence (“SDD”)

Firms can no longer avail of the exemptions previously contained in Sections 34 and 36 of the CJA 2010 for the application of SDD. SDD may be applied to customers who present a lower risk of ML and TF but firms must record the reason(s) for the application of SDD. The

◀▶ Beneficial Ownership

In all instances, Firms are required to identify beneficial owner(s). In addition, Firms are required to verify the identity of beneficial owner(s) by taking those measures reasonably warranted by a risk-based approach following an assessment of the ML/TF risk presented by the customer.

Ongoing Monitoring

When assessing CDD obligations in relation to the ongoing monitoring of customers, Firms should ensure that they have effective and appropriate ongoing monitoring policies and procedures that are in place, in operation and adhered to by all staff. Such policies and procedures should include but are not limited to the following:

- Periodic reviews of customer, the frequency of which is commensurate with the level of ML/TF risk posed by the customer. Firms should also ensure that staff are provided with specific training on how to undertake a periodic review.



Training

Firms should ensure that the AML/CFT training provided to all staff, senior management and agents includes an assessment or examination during the training session, which should be passed by all participants for the training to be recorded as completed. If the training does not contain an assessment, Firms must be able to demonstrate effectiveness of training and staff understanding.

Politically Exposed Person (“PEP”) Approval

The Guidelines state that the Firm must allocate the responsibility for the approval of PEP relationships and must ensure that the approval of a PEP relationship is conducted by individuals who are appropriately skilled and empowered, and this process is subject to appropriate oversight. Firms should determine the level of seniority for sign off by the level of increased ML/TF risk associated with the business relationship.

Additionally, Firms should verify the source of wealth and source of funds based on reliable and independent data, documents or information.

Risk Factors

Firms should take a holistic view of the ML/TF risk factors they have identified that together, will determine the level of ML/TF risk associated with a business relationship or transaction.

When weighting risk factors, Firms should make an informed judgement about the relevance of different risk factors in the context of a business relationship or transaction.

Risk Assessments

Firms should keep their Business Risk Assessment and assessments of the ML/TF risk associated with individual business relationships and occasional transactions as well of the underlying factors under review to ensure their assessment of the ML/TF risk remains up to date and relevant. Where the Firm is aware that a new risk has emerged, or an existing one has increase, this should be reflected in the Business Risk Assessment as soon as possible. Firms should assess information obtained as part of their ongoing monitoring of a business relationship and consider whether this affects the risk assessment.

The Guidelines do not replace the guidance issued by the European Supervisory Authority (“ESA”) or FATF and therefore Firms should ensure that they are familiar with and have regard to the guidance published by these bodies.

Meeting Your New Obligations

Carne is the premier global provider of fund solutions to the asset management industry. Our risk based approach and technology driven solutions are used by some of the world's biggest investment managers to meet their ongoing risk and regulatory requirements. We offer a range of services that can help you to ensure you meet the new Anti-Money Laundering and Terrorist Financing requirements including:

- Reviewing your policies and procedures and updating them in line with the new requirements of the 2018 Act
- Completing business risk assessments
- Providing training and advice regarding compliance with the new Act
- Carrying out due diligence visits to administrators to whom AML functions are delegated to ensure compliance with the new Act

Carne Contacts

CARNE GROUP

Dave Burns

Global Head of Data Protection, AML and Financial Crime Prevention

T: +353 (1) 489 6829 E: Dave.Burns@carnegroup.com

CARNE DUBLIN

Shane Keyes

Money Laundering Reporting Officer, AML, Data Protection & Financial Crime Prevention

T: +353 (1) 489 6861 E: Shane.Keyes@carnegroup.com

CARNE DUBLIN

John Cronin

Money Laundering Reporting Officer, AML, Data Protection & Financial Crime Prevention

T: +353 (1) 489 6874 E: John.Cronin@carnegroup.com

NEXT GENERATION SOLUTIONS

Carne leverages its global scale and capabilities to deliver innovative next generation solutions aligned to the needs of our clients. Our industry leading technology and risk driven platform, CORR, can help you revolutionise your compliance, risk and operational requirements and provide you with the management information you need to control your business.

Legal disclaimer: The content of this document is for information purposes only and should not be relied upon without first seeking legal advice. Opinions constitute best judgement at the time of publication and are subject to change.