THE TA FORUM
AML Working Group

Anti-Money Laundering Guidance

Introduction

The 2015's 4th AML directive brings Europe's anti-money laundering and counter-terrorist financing laws in line with the 2012 recommendations outlined by Financial Action Task Force ("FATF").

4AMLD ((EU) 2015/849) extends and replaces the previous 2007 EU directive. The purpose of the 4AMLD is to remove any ambiguities in the previous Directive and associated legislation and improve consistency of AML and counter-terrorist financing (CTF) rules across all EU Member States.

Like its predecessor, the aim of 4AMLD is to make it harder for criminals to use the financial system through greater scrutiny and transparency of financial transactions and relationships.

Having come into force in June 2015, EU Member States must transpose the directive into local law by June 2017, after which date affected entities must be fully compliant.

The scope of 4AMLD covers financial institutions ('obliged entities', previously known as 'designated persons') and their clients, including corporates, trusts and other beneficial owners. Areas of focus in 4AMLV include risk-based due diligence, national registers of beneficial owners, record-keeping, politically exposed persons and sanctions.

Key principles

Risk-based due diligence

Obliged entities (e.g. banks, asset managers and other financial institutions) must document the risk assessment before using simplified customer due diligence (CDD) processes. This assessment should be documented and on hand should it be requested. Obliged entities must also engage in adequate monitoring to enable the detection of suspicious transactions. ***Article 16***

Investment providers

Investment providers as the obliged entity are required to document their policies, controls and procedures to mitigate the risk of AML these should include model risk management practices, customer due diligence, reporting, record keeping and internal control and keep these up to date. This should take into account risk factors including customers, countries or geographical areas, products, services, transactions or delivery channels. These should be shared with the TA provider to ensure on boarding controls are in line with the firms policies.

THE TA FORUM
AML Working Group

Beneficial Owner

Obliged entities must establish and document the beneficial owner for corporate entities this means a natural person who ultimately owns or controls a legal entity through direct or indirect ownership. If having exhausted all possible means and provided there are no ground for suspicion, no person with control is identified, the senior management of the entity should be identified as beneficial owners. Firms should record actions taken in trying to establish ownership such as Companies House extracts.

Role of third parties in AML compliance

Obliged entities will still be able to rely on the services of third parties for CDD requirements if arrangements are updated in line with new requirements contained in 4AMLD. ***Article 25***

Where third parties are utilised to verify beneficial owner identities the firms overarching control document should set out the match criteria and sources utilised as part of the search process and set out the score requirements for each risk category.

When placing reliance on a third party, a firm must obtain from that third party the necessary information about the identity of the customer and any beneficial owners and the nature of the business relationship, in addition to having the right to obtain copies of ID documentation and verification on request.

Politically Exposed Persons (PEPs)

Definition clarified and expanded to include prominent political persons in domestic jurisdictions. Also clarifies that enhanced due diligence is required for all transactions involving PEPs. ***Article 3 (9)***

Where third parties are utilised to identify PEPs the firms overarching control document should set out the match criteria and sources utilised as part of the search process and ensure these include domestic PEPs.

Firms must apply risk sensitive monitoring to their PEP clients for at least 12 months after they cease to be a PEP, until that person is deemed to pose no further risk.

Transactional monitoring

Firms 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, which have no apparent economic la or lawful purpose. Firms must also increase the degree and nature of monitoring of the business relationship, in order to determine whether those transactions or activities appear suspicious.

Record-keeping

Personal data shall be deleted five years after end of a business relationship, but this can be extended to a maximum period of 10 years, if provided for by national legislation. ***Article 40 (1)(a)***

Firms must keep a copy of their CDD documents on each customer, and supporting evidence and records of the customer's transactions, in the form of originals or copies that are admissible in legal proceedings for 5 years after the end of the business relationship. On expiry of the retention period firms should ensure they delete personal data.

DPA Disclosures

Firms must include "fair collection notices" to inform clients that they will process data for the prevention of ML and TF.