Fifth Money Laundering Directive

Summary of changes to UK AML law

28 February 2020

On 10 January 2020, the Fifth Money Laundering Directive (EU) 2018/843 (5MLD) came into force. On 20 December 2019, the UK government laid before Parliament its implementing legislation, the Money Laundering and Terrorist Financing (Amendment) Regulations 2019 (MLR 2019), which amends the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (MLR 2017, and together with MLR 2019, the MLRs).

5MLD expands the scope of businesses to which the UK's anti -money laundering regime applies (for example, to tax advisors, letting agents and crypto-asset exchanges), as well as amending a number of the substantive requirements. Many businesses will have made amendments in readiness for the anticipated changes. Nonetheless, with financial crime prevention at the top of the agenda for UK, European and international regulators, it is important to ensure that a firm's policies and procedures are fully compliant with the finer details contained in the recently published MLRs.

This article sets out a brief summary of the changes for relevant persons under MLR 2019.

Relevant persons

MLR 2019 extends the list of relevant persons falling within scope of the MLRs to include:

- those providing material aid or assistance on tax matters;
- letting agents;
- art market participants; and
- cryptoasset exchange providers and custodian wallet providers.

Policies

MLR 2017 requires relevant parent companies to establish, maintain and flow down to all of its subsidiaries (whether incorporated in the UK or elsewhere) group-level policies, controls and procedures on:

- data protection; and
- sharing information for the purposes of preventing money laundering with other members of the group.

MLR 2019 amends this second bullet to include policies "on the sharing of information about customers, customer accounts and transactions." The other record -keeping and review requirements contained in MLR 2017 will also apply to these policies.

Training

If a relevant person uses agents to help with preventing, identifying or mitigating the risk of money laundering in its business, it must ensure that these agents:

- are made aware of the law on AML and data protection; and
- receive regular AML training.

E-Money thresholds for customer due diligence (CDD)

Under MLR 2017, certain low-risk e-money products were exempted from CDD requirements. MLR 2019 reduces these thresholds so that the exemption only applies where all of the following conditions are met:

- the maximum amount that can be stored electronically is EUR150 (previously EUR250);
- the payment instrument used in connection with the electronic money is not reloadable or has a maximum limit on monthly payments of EUR150, which can only be used in the UK (previously EUR250);
- the payment instrument is used exclusively to purchase goods and services;
- anonymous e-money is not used to fund the payment instrument; and any redemptions in cash, or remote payment transactions, do not exceed EUR50 per transaction (previously EUR100).

MLR 2019 also prohibits financial institutions from accepting payments which are carried out using anonymous prepaid cards issued in non-EU countries unless those non-EU cards meet requirements that are equivalent to the EU's AML rules for those products. This requirement comes into force on 10 July 2020.

CDD

MLR 2019 clarifies that relevant persons may use electronic identification to complete CDD, providing that the chosen means is secure from fraud and misuse and provides an appropriate level of assurance that the person claiming their identity is in fact that person.

MLR 2019 adds another situation in which relevant persons must apply CDD measures: where the relevant person has any legal duty in the course of the calendar year to contact an existing customer for the purpose of reviewing any information which:

- is relevant to the risk assessment for that customer; and
- relates to the beneficial ownership of the customer, including information which enables the relevant person to understand the ownership or control structure of a legal person, trust, foundation or similar arrangement who is the beneficial owner of the customer.

The other changes to the CDD regime are also focused on beneficial ownership. Below are some examples:

- Where a customer is a body corporate and the beneficial owner cannot be identified, relevant persons must instead take all reasonable measures to verify the identity of the senior managing official. The relevant person must keep records detailing all actions it took to do this and any difficulties encountered in doing so.
- Where a customer is a legal person, trust, company, foundation or similar legal arrangement, the relevant person must take reasonable measures to understand the ownership and control structure of that legal person, trust, company, foundation or similar legal arrangement.
- Before entering into a new business relationship with a company subject to beneficial ownership registration requirements (i.e. the PSC regime), the relevant person must collect from the company either:
  - proof of the company's registration on the PSC Register; or
  - an excerpt of the PSC Register.
- Where the relevant person identifies a discrepancy between the beneficial ownership information available in the PSC Register and the beneficial ownership information provided by the company in the course of CDD, it must report this to Companies House.

Enhanced customer due diligence (EDD)

MLR 2017 requires relevant persons to conduct EDD in cases where:

- a transaction is complex or unusually large, or there is an unusual pattern of transactions; and
- the transaction or transactions have no apparent economic or legal purpose.

MLR 2019 splits out these criteria into three alternative limbs.

5MLD extends the existing requirement to carry out enhanced monitoring of any business relationship or transaction with a person “established in” a high -risk third country so that it covers any relationship or transaction “involving” a high-risk country. However, MLR 2019 clarifies that in the UK, “involving” means:

- a business relationship with a person established in a high-risk third country; or
- a transaction subject to CDD anyway, to which either party is established in a high-risk third country.

For these purposes, being “established in” a third country means:

- in the case of a legal person, being incorporated in or having its principal place of business in that country, or, in the case of a financial institution or a credit institution, having its principal regulatory authority in that country; and
- in the case of an individual, being resident in that country, but not merely having been born in that country.

High-risk third countries remain those identified by the European Commission as such, although 5MLD broadens the assessment criteria, suggesting that the list will likely increase.

MLR 2019 contains a number of additional requirements for business relationships or transactions involving a party established in a high-risk country including:

- obtaining additional information on:
  - the customer and on the customer’s beneficial owner(s);
  - the intended nature of the business relationship;
  - the source of funds and wealth of the customer and the customer’s beneficial owner(s); and
  - the reasons for the intended or performed transactions.
  - obtaining senior management approval for establishing or continuing the business relationship; and
  - carrying out enhanced ongoing monitoring of the business relationship by increasing the number and timing of controls applied, and selecting patterns of transactions that need further examination.

National register of bank account and safe deposit box ownership

Under MLR 2019, the UK has until 10 September 2020 to establish a centralized automated mechanism – such as a central registry or electronic data retrieval mechanism – which allows for the identification of natural and legal persons holding or controlling bank accounts, payment accounts or safe deposit boxes in the UK.

Credit institutions or safe custody services providers must respond fully and rapidly to requests from law enforcement authorities or the Gambling Commission. Customer records must be kept for five years after the closure of the account or safe deposit box.