EVERSHEDS SUTHERLAND

# Note on the Fifth Money Laundering Directive

What's on the horizon?

# The Fifth Money Laundering Directive (EU 2018/843)

The Fifth Money Laundering Directive (EU 2018/843) (**MLD5**) came into force on 9 July 2018. It amends the Fourth Money Laundering Directive (EU 2015/849) (**MLD4**), and Member States must transpose this into domestic legislation by 10 January 2020.

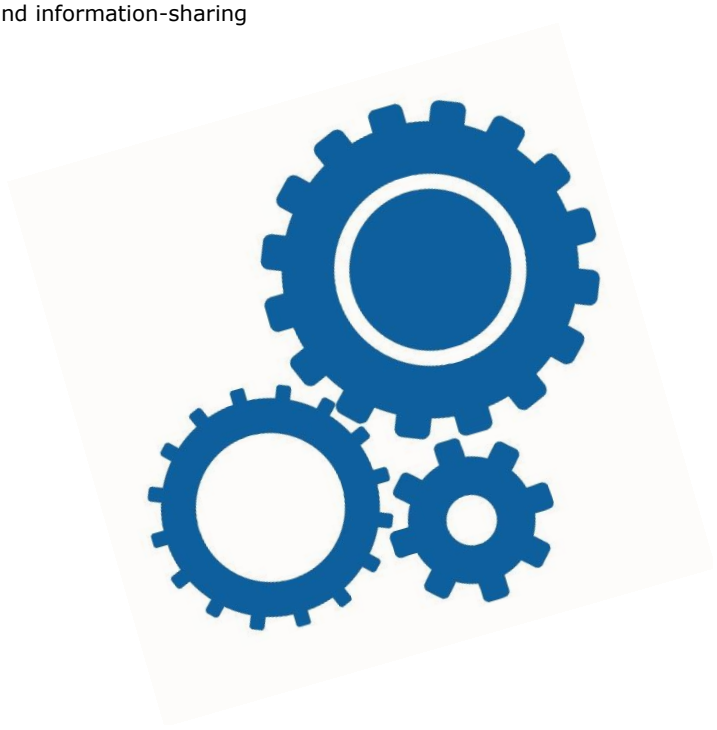
MLD5 was produced following the Paris terrorist attacks and the Panama Papers leak, and is designed to combat terrorist financing, including its use of anonymous payment methods and opaque business structures.

It sets out various 'additional measures to better counter the financing of terrorism and to ensure increased transparency of financial transactions and legal entities', by amending and supplementing MLD4, which came into force on 26 June 2017 and was transposed into UK law via the Money Laundering Regulations 2017.

MLD5 is a minimum harmonising directive, and Member States are able to apply more stringent requirements at a national level if they choose. Although the UK is expected to withdraw from the EU in March 2019, before the deadline for EU Member States to implement MLD5, the current text of the draft withdrawal agreement includes a transitional or implementation period ending on 31 December 2020, during which the UK would be required to implement EU directives (including MLD5). The UK may therefore be obliged to implement MLD5 but, even if not, it may choose to do so.

The key provisions for financial services companies are set out below and fall into three categories:

- provisions focusing on currency and money products
- provisions focusing on high-risk individuals and PEPs
- provisions focusing on information-gathering and information-sharing



# Provisions focusing on currency and money products

## Regulating virtual currency

Under current legislation, virtual currencies are not regulated at an EU level, allowing for their potential misuse by terrorist organisations. MLD5 brings the 'gatekeepers' who control access to virtual currencies into scope.

The definition of 'obliged entities' – i.e. those entities which fall within the scope of MLD4 – is to be extended so that those providers engaged in exchange services between virtual currencies and fiat currencies (virtual currency exchange platforms (**VCEPs**), and custodian wallet providers (**CWPs**) are now within scope. Legal definitions of 'virtual currencies' and 'custodian wallet providers' can be found in Article 1(2)(d) of MLD5, which amends Article 3(18) and (19) of MLD4.

As 'obliged entities' VCEPs and CWPs will be required to implement AML and CTF policies, controls and procedures, including customer due diligence measures and the obligation to report suspicious transactions. They will also need to be registered with local competent authorities – in the UK this will be the FCA.

However, and as the Commission recognises, it is the anonymity of virtual currencies which creates the greatest potential for misuse for criminal purposes. The inclusion of providers engaged in exchange services between virtual currencies and fiat currencies and custodian wallet providers will not, by itself, address the issue of anonymity attached to virtual currency transactions, since a large part of the virtual currency environment will remain anonymous in circumstances where users can currently also transact without such providers.

To combat the risks related to anonymity, national Financial Intelligence Units (FIUs) will now be able to obtain information allowing them to associate virtual currency addresses to the identity of the owner of virtual currency. How this will be achieved in practice is not yet known, although Recital 9 suggests that consideration should be given to the possibility of allowing users to self-declare to designated authorities on a voluntary basis. The question remains as to how many terrorists would accept the proposed opportunity to self-declare.

Nonetheless the stated intention is that these measures will help to prevent terrorist groups from feeding money into the EU financial system, or within virtual currency networks by 'concealing transfers or by benefiting from a certain degree of anonymity on those platforms'.

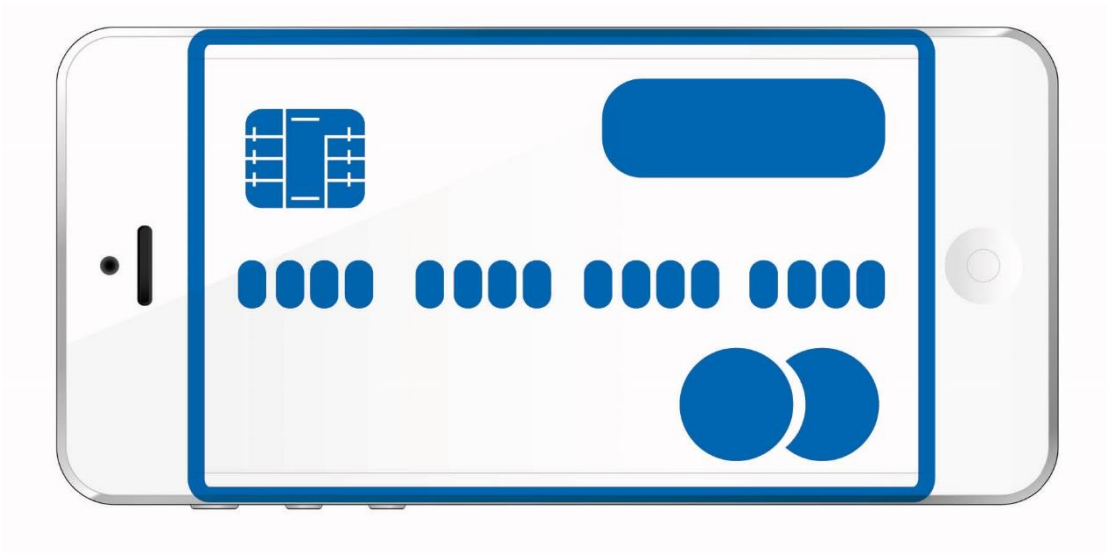
## Limiting exemption for electronic money products

The Commission has identified the use of anonymous reloadable and non-reloadable prepaid cards as a feature in the financing of recent terrorist attacks which must be addressed. Under Article 12 of MLD4, Member States can allow firms to benefit from an exemption to the normal requirements to conduct customer due diligence (**CDD**) for electronic money products. However, to minimise misuse of these products, the existing EUR250 threshold is to be lowered to EUR150 in respect of pre-paid instruments. There is a maximum limit of EUR 50 for redemption in cash, cash withdrawal of the monetary value or amount paid per remote payment transaction, above which limit the existing customer due diligence exemption will no longer apply.

Further new provisions require that firms acting as acquirers only accept payments carried out with anonymous pre-paid cards issued *outside* the EU where those cards comply with requirements equivalent to those set out in Article 12(1) and (2) of MLD4. As MLD5 is a minimum harmonising directive, Member States may decide not to accept payments carried out using anonymous pre-paid cards at all.

## Restrictions on anonymity

Credit and financial institutions will no longer be allowed to keep anonymous safe-deposit boxes. MLD5 also requires such institutions to conduct customer due diligence (**CDD**) measures on the owners and beneficiaries of existing anonymous safe-deposit boxes.



# Provisions focusing on high risk jurisdictions and individuals

## High risk third countries

Under Article 18 of MLD4, once a country is designated by the EU Commission as having strategic money laundering or terrorist financing deficiencies, firms are obliged to apply enhanced customer due diligence (**EDD**) measures to manage and mitigate the risk. To streamline this process between Member States, Article 1(11) of MLD5 contains a prescriptive list of EDD measures that must be applied by firms, including obtaining additional information on the customer and beneficial owner, obtaining senior management approval for establishing or continuing the business relationship and carrying out enhanced monitoring. These are to be considered as a minimum set of requirements to be applied by all Member States.

MLD5 also requires firms to apply one or more 'additional mitigating measures' to persons and legal entities carrying out transactions involving high risk third countries, as set out in Article 18a(2) of MLD4.

In addition to the requirements being imposed on firms, Member States will also be obliged to take one or more of a list of measures relating to high-risk third countries. These measures include refusing the establishment of subsidiaries, branches or representative offices of 'obliged entities' from the relevant country, requiring increased supervisory examination of local branches and subsidiaries, and requiring firms to review, amend or terminate correspondent relationships with respondent institutions in the relevant country.

## Identifying politically exposed persons (**PEPs**)

MLD5 contains a series of new measures relating to the identification of PEPs, including a new obligation on Member States to create, and keep up-to-date, a list of the functions that qualify as 'prominent public functions' for the purposes of the PEP definition found within Article 3(9) of MLD4 .

Member States are also required to ask each international organisation accredited in their territories to create, and keep updated, a list of prominent public functions at that organisation.

These lists are to be sent to the Commission and may be made public, and so will only contain the name of the PEP function, and not the name of the PEP individual currently fulfilling that function. Additionally, the Commission will create, and keep updated, an equivalent list of the functions that qualify as 'prominent public functions' in EU-level institutions and bodies.

## Monitoring of existing customers

The risk-based approach to CDD under MLD4 has been enhanced to ensure that certain clearly specified categories of existing customer are monitored on a regular basis. Firms will have to apply CDD measures at appropriate times, to existing customers, on a risk-sensitive basis, or:

- when the relevant circumstances of a customer change;
- when the firm has any legal duty in the course of the relevant calendar year to contact the customer for the purpose of reviewing any relevant information relating to any beneficial owners; and
- if the firm has had this duty under Council Directive 2011/16/EU (which provides for the mandatory automatic exchange of information in the field of taxation)

# Provisions focusing on information gathering and information sharing

## Developments in CDD measures

New provisions under MLD5 in this area reflect the Commission's view that MLD4 should be updated to take account of the new legal framework covering electronic identification and authentication, relevant when opening bank accounts (the eIDAS Regulation). This new legal framework complements the MLD4 objective that parties to a transaction or payment should be properly identified and verified.

MLD4 is therefore to be amended to provide that identifying the customer and verifying their identity on the basis of documents, date, or information obtained from an independent or reliable source includes, where available, any:

- electronic identification means;
- relevant trust services as set out in the eIDAS Regulation; and
- any other secure, remote or electronic identification process regulated, recognised, approved or accepted by the relevant national authorities

Similar MLD5 provisions amend other areas of MLD4:

- Article 1(14) of MLD5 amends Article 27(2) of MLD4 (third party reliance);
- Article (1)(25)(a) of MLD5 amends Article 40 of MLD4 (record keeping); and
- Article 1(44)(b)(i) of MLD5 amends Annex III to MLD4 (a non-exhaustive list of factors and types of evidence of potentially higher risk)

## National central mechanisms

Member States will be obliged to establish a central automated mechanism, such as a central register or data retrieval system, which enables financial intelligence units (**FIUs**) and other competent authorities to identify holders and controllers or bank and payment accounts, and safe deposit boxes, held by credit institutions within their jurisdiction.

The information that must be accessible and searchable will include: (i) the name and unique identification number of the customer and, where applicable, the beneficial owner, (ii) the IBAN number, (iii) the date of account opening and closing (for bank and payment accounts), and (iv), for safe deposit boxes, the name of the lessee, their unique identification number and the duration of the lease. As the explanatory memorandum to MLD5 sets out, firms will be obliged to file or upload this information into the central mechanism periodically, although the frequency with which the data needs to be updated is yet to be determined.

Access to this register will be limited, and provided on a 'need to know' basis, but will be 'directly accessible in an immediate and unfiltered manner' to FIUs. The EU Commission is due to report to the EU Parliament and Council by 26 June 2020 in relation to connecting the national central mechanisms through the European Central Platform.

## Access to beneficial ownership information

Following the Panama Papers, the EU Commission made clear that it considered that improvements were needed to remedy transparency issues. MLD5 therefore expands and strengthens the beneficial ownership regime of MLD4. The access right to the information on the existing register will be extended to any member of the general public, in addition to competent authorities, FIUs and obliged entities, so that third parties can ascertain beneficial ownership throughout the EU. Member States will be permitted to make this access subject to online registration and payment of a fee.

Additionally, MLD5 contains a new discrepancy reporting requirement, whereby entities must report any discrepancies they find between the information they hold, and the information on the beneficial ownership register. The requirement to hold beneficial ownership information is to be extended to trusts (and other legal arrangements with similar structures). This information will also be held in the central registry, but access to it will require demonstration of a legitimate interest.

## New powers for FIUs

The Commission's view is that FIUs' unfettered access to information is essential to ensure that flows of money can be properly traced and illicit networks and flows can be detected at an early stage. MLD4 has therefore been amended to align the requirements relating to FIUs' access to information with the Financial Action Task Force standards, to further enhance their effectiveness and efficiency. FIUs will now be able to request, obtain and use information from any obliged entity, even in situations where no prior suspicious activity report has been submitted.

## Collaboration

Prudential information about firms, such as information on the fitness and properness of directors and shareholders, internal control mechanisms, governance and risk management, is often key for adequate ML and CTF supervision, and vice versa. The EU Commission felt that information sharing and collaboration in this area ought not be hampered by legal uncertainty and therefore under MLD5 prudential supervisors and AML/CTF supervisors are required to exchange confidential information, as set out in new articles dealing with:

- professional secrecy
- disclosure of confidential information
- cooperation of supervisors

These clarifications are designed to ensure cooperation between competent authorities and other authorities bound by professional secrecy, so that the exchange, dissemination and use of information is not fettered by differences between national laws.

**eversheds-sutherland.com**



LON_LIB1#19461324