The Fifth EU Money Laundering Directive

HM Treasury consultation on the UK's draft implementing measures

On 15 April 2019, HM Treasury launched its long-awaited first consultation on the UK's implementation measures for the Fifth EU Money Laundering Directive (**MLD5**).[1] MLD5 entered into force as a matter of European law during July 2018, and makes a number of amendments to the Fourth Money Laundering Directive (**MLD4**).[2] EU Member States have until 10 January 2020 to implement MLD5. It is drafted as a minimum-harmonising directive, meaning that EU Member States can apply more stringent requirements than MLD5 if they consider it necessary, and HMT Treasury's implementation proposals will "gold-plate" the baseline provisions of MLD5 in several areas, if they are pursued following the consultation.

The UK government had publicly indicated its commitment to transposing MLD5 prior to issuing this consultation, despite the UK's expected departure from the EU. HM Treasury's consultation proceeds broadly in line with that commitment. This briefing considers the key changes MLD5 will bring about, and the key proposals that have emerged from HM Treasury's consultation.

Overview of MLD5

MLD5 was proposed and negotiated at EU level the context of a number of important developments, in particular a spate of terrorist attacks including the Paris nightclub attack in November 2015, the disclosure of the Panama Papers to investigative journalists in 2015, the European Commission's 2016 Action Plan on the fight against terrorist financing, and several ongoing initiatives within the international Financial Action Task Force (**FATF**), for example with respect to the AML implications of emerging financial technologies. It also picks up a number of points that are understood to have been part of earlier negotiations over MLD4, but were ultimately not included at that time.

MLD5 makes a number of changes to the existing anti-money laundering and counter-terrorism financing regime with the aim of achieving two principal objectives. The first is to improve the transparency of ownership of a number of different types of entity and asset, facilitating firms' due diligence on customers. The second is to disrupt the finances of money launderers and terrorist organisations, by hindering their capacity to raise and transfer funds.

The objectives are met by introducing the following targeted amendments to MLD4:

- extending the scope of those subject to European AML legislation (**obliged entities**) to include, among others, providers of exchange services between virtual (crypto) and fiat currencies as well as custodian wallet providers;
- extending the circumstances in which obliged entities are required to apply certain customer due diligence (**CDD**) measures, for example by reducing the thresholds at which CDD is triggered in relation to prepaid cards;
- clarifying and expanding the circumstances in which firms will be required to carry out enhanced customer due diligence (**EDD**), for example in relation to third countries that are determined by the European Commission to be high-risk countries, and in relation to politically exposed persons (**PEPs**). Member States will for example be required to maintain lists of specific functions that qualify as "prominent public functions" to assist in the identification of PEPs;
- enhancing the powers of - and reinforcing cooperation between - Financial Intelligence Units (**FIUs**) in the various Member States; and
- enhancing access to information on beneficial ownership across the EU and improving transparency, particularly in the ownership of companies, certain trusts and other legal entities, and bank accounts.

It is anticipated that many of the new requirements will ultimately be introduced by way of amendments to the 2017 Money Laundering Regulations (the **MLRs**)[3], however certain other legislation and administrative practices may also change as part of the implementation process.

A further consultation on the draft implementing legislation is expected later in 2019, once HM Treasury has received feedback to the first consultation, and HMRC is expected to consult on changes to the Trusts Registration Service (**TRS**).

---

[1] HM Treasury, Transposition of the Fifth Money Laundering Directive: consultation (April 2019), text available here. The text of MLD5 is available here.
[2] The text of MLD4 is available here.
[3] Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017, text available here.

Electronic money

Whilst general purpose prepaid cards have a number of legitimate uses, not least an important role in contributing to social and financial inclusion, FATF guidance in 2013 pointed to risks around anonymity and prepaid cards that exist at the points of purchase, registration, loading and reloading with funds, and at the point of use. The French authorities reportedly identified prepaid cards as having played a material role in the funding and preparation of the Paris terrorist attacks. The UK's 2017 National Risk Assessment classified e-money as medium risk for AML/CTF purposes.[4]

Low risk e-money products are currently exempted from certain CDD measures (such as identification and verification of the customer and beneficial owner). MLD5 will, however, extend the requirements for CDD in relation to these products. Under MLD5, the circumstances in which CDD will not be required will become more restricted. All of the following conditions must be met before CDD may be reduced:

- the maximum amount that can be stored electronically is €150 (this is a reduction from the current level of €250) or if the amount is only used in UK, €500;
- the payment instrument is not reloadable or has a maximum limit on monthly payments of €150 (reduced from the current €250) which can only be used in the UK;
- the payment instrument may only be used to purchase goods and services;
- the payment instrument is not funded by anonymous e-money; and
- any redemptions in cash or remote payment transactions should not exceed €50 (lowering the threshold from the current €100).

As well as reducing the thresholds at which CDD becomes necessary, MLD5 introduces a new restriction on the acceptance by financial institutions within the EU of anonymous prepaid cards issued outside the EU. Financial and credit institutions acting as acquirers operating in Member States will only be permitted to accept payments carried out with anonymous prepaid cards issued in non-EU countries where those countries have equivalent AML/CTF law. HM Treasury recognises that the changes to the thresholds and usage of pre-paid cards may significantly increase firms' compliance costs and is seeking feedback on this. Another key question for stakeholders concerns the changes (if any) financial institutions and credit institutions will need to make to their systems in order to detect whether anonymous card issuers located in non-EU states are subject to requirements in their national legislation that are equivalent to EU requirements.

Cryptoassets

The online accessibility, cross-border reach and pseudo-anonymous nature of cryptoassets are all features that make them attractive for criminal purposes and HM Treasury expects that, as accessibility of such assets increases, the risk of their use in money laundering, terrorist financing and other criminal activities (such as fraud, scams and cyber-theft) is also likely to grow.

MLD5 brings custodian wallet providers and cryptoasset exchanges within the scope of the AML/CTF regime, which will require them to register with the relevant UK supervisor (likely to be the FCA), perform customer due diligence, monitor transactions and report suspicious activity. However, MLD5 contains a definition of "virtual currencies" that is narrower than the definition of cryptoassets used by the UK's Cryptoassets Taskforce (the **Taskforce**). HM Treasury is seeking views on whether the MLD5 definition may need to be changed to incorporate the three types of cryptoasset identified by the Taskforce (namely, exchange tokens, security tokens and utility tokens), so as to capture within the AML/CTF regime all relevant activity involving all three types of cryptoasset.

HM Treasury is also considering whether the identified risks warrant it gold-plating the MLD5 requirements, which apply only to cryptoasset exchanges providing exchange services between cryptoassets and fiat currencies, to capture other services, namely:

- crypto-to-crypto exchange service providers;
- peer-to-peer exchange service providers;
- cryptoasset Automated Teller Machines;
- issuance of new cryptoassets, for example through Initial Coin Offerings; and
- the publication of open-source software (including non-custodian wallet software and other types of cryptoasset-related software).

Care will need to be taken that any gold-plating by the UK does not give rise to legal uncertainty and/or have a chilling effect on technological innovation.

The MLD5 definition of virtual currency is limited to "means of exchange", whereas HM Treasury considers that activity involving security tokens and utility tokens should also be captured in AML/CTF regulation. This may represent over-reach particularly as it is admitted that security tokens amount to a "specified investment" under the Financial Services and Markets Act 2000 (Regulated Activities) Order 2001 – which would typically already bring them within AML/CTF regulation. As for utility tokens (which can be redeemed for access to a specific product or service), it must be asked whether these present an AML risk, as any definition of cryptoassets which seeks to capture tokens is likely to be very broad in scope and may give rise to unintended consequences. In particular, we foresee difficulties for cryptoassets which initially fall into one

[4] The 2017 National Risk Assessment is available here.

category for AML purposes but where changing use by the market means that the characteristics of the asset changes this category at a later point.

Further, proposed gold-plating in relation to services related to cryptoasset exchange may include the regulation of providers of such services that publish *open-source software* (which includes, but is not limited to, non-custodian wallet software and other types of cryptoasset related software). Again, care will need to be taken not to render unwieldy the scope of restrictions on publishing open-source software in the UK, particularly given the international nature of software development and sharing.

CDD and Enhanced Due Diligence (EDD)

This is an area where firms are likely to see significant changes. MLD5 seeks to clarify and harmonise CDD and EDD requirements across Member States. Whilst the general approach remains risk-based, the new directive will in practice introduce a number of more prescriptive requirements, addressing some of the widely drafted provisions (particularly around EDD) that were included in MLD4 that have been criticised in the past for creating uncertainty. In particular, MLD5 seeks to clarify what firms will be expected to collect during standard CDD, where firms will need to carry out EDD, and the type of information that must be obtained during EDD, particularly for business relationships or transactions "involving" high risk third countries. The criteria the Commission must apply when determining high risk third countries are being tightened. MLD5 will also strengthen requirements to obtain senior management approval with respect to such business relationships and transactions. The new requirements will be wider than current EDD requirements, which (in short) apply to business relationships or transactions with a person established in a high risk third country. HMT is seeking feedback on use of a broad definition for the term "involving". MLD5 will also clarify the circumstances where UK authorities will have power to take mitigating measures with respect to high risk third countries (for example by prohibiting firms in scope from establishing branches in those countries). Member States will also be required to maintain lists of specific functions that qualify as "prominent public functions" to assist in the identification of PEPs.

In addition to proposals for MLD5 implementation, HM Treasury is also seeking feedback on proposed changes to the MLRs to address some of the recommendations of the FATF's Fourth Mutual Evaluation Report on the UK regime, published in December 2018.[5] FATF considered that the UK requirement to identify and verify the names of senior managers of bodies corporate is not absolute (the MLRs require only reasonable measures to be taken) and so HM Treasury proposes to amend the MLRs to make the requirement mandatory. FATF also recommended that relevant persons (that is, obliged entities) should be "*required to understand the nature of their customer's business and its ownership and control structure*".[6] HM Treasury seeks input on the extent to which firms are already gathering this information as part of their CDD procedures.

Information about the beneficial ownership of companies

The key changes that MLD5 will make in this area relate to:

- Member States' central registers for beneficial ownership information for companies (in particular, requirements as to the adequacy, accuracy and currency of information held on such registers are being reinforced); and
- the legal requirements on companies to hold information about their own beneficial ownership so this is available for due diligence purposes.

As expected, HMT has taken the view that the UK's current Persons of Significant Control (**PSC**) regime already meets most of MLD5's requirements in this area, but it is consulting on ways in which discrepancies identified in PSC information can be reported to Companies House, so they can be dealt with.

Two possible options put forward by HM Treasury in the consultation are a possible requirement on firms to report issues they find during their due diligence, and a possible requirement on the authorities to identify discrepancies during their work. Either might help the UK meet the requirement in MLD5 for mechanisms to ensure that the information held on the central register is "*adequate, accurate, and current*".[7]

Changes to the Trust Registration Service

The **TRS** is a register maintained by HM Revenue & Customs (**HMRC**) containing details of those involved with express trusts which have a UK tax consequence (that is, where the trust is liable to pay income tax, capital gains tax or other specified UK tax). The TRS was put in place during 2017 to meet a requirement introduced in MLD4. Information on it is currently accessible to law enforcement and FIUs but not the general public.

MLD5 expands the number of trusts that will need to be entered on national central registers. The impact for the UK is that registration under the TRS will be required for:

- UK resident express trusts (whether not they have a UK tax consequence);
- non-EU express trusts acquiring UK land or property either on or after 10 March 2020;
- non-EEA express trusts entering a new business relationship with a UK obliged entity on or after 10 March 2020; and
- overseas and non-express Trusts that are liable for UK tax (whether or not they are express trusts or have UK trustees).

---

[5] The FATF's December 2018 report is available here.
[6] See Criterion 10.8 of FATF's December 2018 Mutual Evaluation Report for the UK (at page 194).
[7] See MLD5, Recital (25).

Further, MLD5 will widen access to TRS to those with a "legitimate interest" (including some members of the public), and will reinforce the requirement on trustees to provide information about their trusts to facilitate due diligence.

HM Treasury is consulting on categories of UK trust that are likely to fall within the newly expanded regime (and which accordingly will need to be registered within TRS). It does not intend to create a definitive list, but instead to place the onus on trustees and their agents to determine whether their trust is captured.

HM Treasury is also consulting on a number of administrative issues which are of real practical significance to the future operation of TRS, in particular the deadlines for registration, penalties for late registration, and the extremely important issue of how access to the information on TRS will be governed (particularly what will count as a "legitimate interest").

A further technical consultation is expected to be published by HMRC in due course.

National register of bank account ownership

MLD5 requires Member States to establish centralised automated mechanisms, such as a register or data retrieval system, as an efficient means to get timely access to information on the identity of holders of bank and payment accounts (identified by IBAN) and safe-deposit boxes, their proxy holders, and their beneficial owners.

HM Treasury is proposing to meet this requirement in the UK by establishing a National Register of Bank Account Ownership and requiring credit institutions and payment institutions to submit information to the register on a weekly basis (to the extent the information is new or has changed).

HM Treasury also seeks feedback on the costs and benefits to law enforcement agencies of gold-plating MLD5 requirements by requiring the following additional entities to submit information to the register:

- UK incorporated credit and payment institutions that issue credit cards;
- e-money issuers that issue prepaid cards; and
- credit unions and building societies that issue accounts without an IBAN.

HM Treasury is inviting feedback on the envisaged scope of information to be included register across different categories of account/product and on its proposed approach to allow access to the information to meet the MLD5 requirement that the register be "*directly accessible in an immediate and unfiltered manner to national FIUs*", and be "*accessible to national competent authorities for fulfilling their obligations under this Directive*"[8].

Pooled Client Accounts

HM Treasury is taking the opportunity in the consultation to gather more information from stakeholders on practical difficulties they have experienced in implementing the AML/CTF framework that applies to pooled client accounts (**PCAs**), by which a firm will hold and move money on behalf of its underlying customers. The default position for CDD is that a bank should conduct CDD on both the immediate account-holding customer (for example a law firm) and on its underlying clients. However, the PCA framework in the MLRs enables simplified due diligence (**SDD**) to be carried out by a bank in circumstances where the business relationship between the bank and the customer is considered low risk for ML/TF, the account-holding customer is itself subject to obligations under the MLRs and the bank is satisfied firstly that the customer has conducted CDD on its clients (the underlying owners of the account monies) and also that the customer will provide that information if requested.

HM Treasury is aware that the requirement to demonstrate that a relationship is low risk can prove difficult in practice. Another issue is that, given that the PCA framework requires the customer to be subject to obligations under the MLRs, the MLRs are not explicit on the CDD that should be carried out where the customer is not MLR-regulated. HM Treasury is interested in views on what CDD obligations should be placed on the banks should the PCA framework be extended to non-MLR-regulated businesses.

Other matters

HM Treasury is consulting on some other matters including technical amendments beyond the scope of this briefing. These relate in particular to enforcement powers, information sharing and cooperation, registration requirements, complex network structures, criminality checks, new technologies and group policies.

Next steps

Responses to the first consultation are due to go to HM Treasury by 10 June 2019. Addleshaw Goddard has been working on a response to the consultation – any clients interested in discussing it with us / providing input into it are invited to make contact with their usual AG contacts as soon as possible.

---

[8] New Article 32a, MLD4, as inserted by Article 1(19), MLD5.

If you have any questions, please do not hesitate to contact your usual AG contact or one of the lawyers listed below:

David Ellis, Partner	020 7160 3352	david.ellis@addleshawgoddard.com
Steven Francis, Partner	020 7160 3949	steven.francis@addleshawgoddard.com
Michelle de Kluyver, Partner	020 7788 5101	michelle.dekluyver@addleshawgoddard.com
Brian McDonnell, Partner	020 7160 3175	brian.mcdonnell@addleshawgoddard.com
Nichola Peters, Partner	020 7160 3370	nichola.peters@addleshawgoddard.com
David Pygott, Partner	020 7788 5123	david.pygott@addleshawgoddard.com
Richard Small, Partner	020 7160 3004	richard.small@addleshawgoddard.com
William Robertson, Managing Associate	020 7160 3398	william.robertson@addleshawgoddard.com
Jennifer Cutting, Associate	020 7788 5111	jennifer.cutting@addleshawgoddard.com
Sara Evans, Principal Knowledge Lawyer	020 7160 3045	sara.evans@addleshawgoddard.com