MLD4: Here at last

What does it mean?

December 2015

After many years of negotiation, the fourth Money Laundering Directive (MLD4) and the accompanying revised Funds Transfer Regulation (FTR2) were adopted in May 2015 and made it into the Official Journal of the EU a month later. MLD4 must be implemented in all Member States and in force by 26 June 2017, the same date as FTR2 takes effect. In this article, Emma Radmore looks at the history and drivers behind MLD4, its key provisions and what this means for firms in the UK regulated sector.

History of EU money laundering legislation

The EU made the first Directive – MLD1 – in 1991. This was aimed predominantly at drugs-related offences and introduced obligations on credit and financial institutions to verify the identity of their customers and report concerns of money laundering. This Directive remained the key EU measure for some 10 years. The UK already had in place, and as a result of MLD1 updated, its legislation and industry guidance.

In 2001, MLD2 came along. This expanded MLD1 in terms of both the predicate offences in relation to which money laundering could apply and the businesses covered. Its main aim was to ensure the EU addressed the Financial Action Task Force (FATF) recommendations of the time. The UK implemented MLD2, and went further, by extending its domestic laws to cover a wider scope of participants.

MLD3 followed in 2005. Again, this built on MLD2, extending its scope again, including to cover professionals such as lawyers and accountants within scope. It was MLD3 that introduced the risk-based approach (RBA) to customer due diligence (CDD), and introduced the concept of simplified due diligence (SDD) and enhanced due diligence (EDD). MLD3 was accompanied by a Funds Transfer Regulation (FTR1), which mandated information on the payer and payee to be included in fund transfers.

Drivers for MLD4

10 years after MLD3, we now have MLD4. Many would say the change was long overdue. The relatively long gap since the last revision has meant there were many drivers for change. Key amongst these, and reflected in the recitals to MLD4, were:

Global consistency

The European Commission (Commission) noted the need for international coordination of anti-money laundering (AML) and counter financing of terrorism (CFT) measures and, in particular, that EU AML and CFT laws needed to be compatible with current FATF recommendations.

Breadth of offences covered

Although a broad range of criminal offences could already give rise to criminal property which in turn could be laundered, the Commission saw the need specifically to address manipulation of money derived from serious crime and collection of money or property for terrorist purposes. It also considered that tax crimes relating to direct and indirect tax laws had to be

included.

Businesses covered

Again, each iteration of MLDs has widened the scope of what MLD4 calls "obliged entities" (and what the UK calls the "regulated sector"). In particular, there was significant discussion around when high value dealers for cash should be covered. After significant negotiation, it was decided the threshold above which cash traders should be covered needed to be decreased to €10,000 with the ability for individual Member States to cover lower thresholds.

Changes also bring new products, such as e-money products, within scope and seek to address "directly comparable" professions so there should be no arbitrage between those providing effectively the same service.

Consistency on beneficial ownership checks

An area that desperately needed clarification was the question of what is a beneficial owner, and to what extent they should be identified. MLD4 is to allow Member States to include the greatest range of entities in any beneficial ownership determination and consider appropriate evidential measures as well as absolute thresholds for beneficial owner assessment. Beneficial owner checks should aim to identify the ultimate natural owner.

To ease up-to-date availability of beneficial ownership information, Member States should require entities in their territories to keep up to date information on ownership in a central registry, and to ensure persons with a legitimate right to know beneficial ownership information have access to it. Trustees should be required to hold similar information in registries and disclose it to obliged entities.

Risk-based approach

MLD3 had introduced the risk-based approach, but MLD4 stresses it is critical to apply it. Obliged entities must recognise "per se" high risk situations. The most common situation would involve Politically Exposed Persons (PEPs) – another phrase that had been subject to significant differences in interpretation under MLD3. MLD4's aim is to require that PEPs include those entrusted with public functions both domestically and abroad.

Two other aspects of the risk-based approach MLD4 seeks to clarify are that:

- where senior management approval is needed (for instance, for high risk transactions or relationships), this need not necessarily mean board approval; and
- reliance on others and outsourcing should be allowed but responsibility remains with the obliged entity.

Duties on the European Commission

MLD4 introduces a duty on the European Commission to make cross-border risk assessments. It should identify high risk third countries, require EDD on customers and prohibit reliance on third parties there.

Suspicion reporting

The Commission noted that not all Member States had financial intelligence units (FIUs) and determined each Member State should have an FIU to whom suspicious activity reports (SARs) should be made. It also thought it was necessary to ensure that:

- obliged entities could carry out suspicious transactions before making a SAR if refraining from acting is impossible or likely to frustrate efforts to pursue suspects, but that this should be without prejudice to asset freezing obligations under sanctions laws;
- Member States should protect reporters from threats;
- there is consistency with data protection laws, so disclosures should be limited to what is necessary for proper AML compliance; and
- authorities should provide SAR feedback where possible.

Global compliance

The Commission felt obliged entities should apply MLD4 standards to all branches and subsidiaries and tell their Home State regulator if this is not possible, and that EU-wide operations should comply with standards set in the Home State and be subject to Home State supervision.

Sanctions for breach

The Commission noted a lack of consistency in sanctions for breach and, indeed, that in some Member States there were few or none. It said Member States must have appropriate sanctions for breach – and there should be a minimum standard.

A role for the ESAs

The European Supervisory Authorities (ESAs) are gradually acquiring more powers, to foster consistency in interpretation and implementation of EU measures. The Commission said ESAs should elaborate harmonised technical standards for maximum harmonisation across Member States.

MLD4

Moving on to some of the main elements of the MLD4 text, these themes all come through.

Key Provisions: What is money laundering?

Member States must prohibit money laundering and terrorist financing. MLD4 defines money laundering as when a person intentionally:

- converts or transfers property knowing it to be derived from criminal activity...for the purpose of concealing or disguising its illicit origin or of assisting any person involved to evade the legal consequences of their action;
- conceals or disguises the true nature, source, location, disposition, movement, rights or ownership...of property derived from criminal activity;
- acquires, possesses or uses property knowing on receipt that it derives from criminal activity or participation in it; or
- participates in, associates to commit, attempts to commit, aids, abets, facilitates or counsels any of the above.

Criminal activity includes terrorism, drug trafficking, fraud affecting EU financial interests, corruption and all offences punishable by at least six months' imprisonment (or with a maximum imprisonment of more than one year).

These offences apply regardless of where the activities that generate the property take place.

Terrorist financing is providing or collecting funds, by any means, directly or indirectly, intending or knowing they may be used to carry out terrorist activities or aiding and abetting them.

Scope: Obliged entities

MLD4 lists as obliged entities under it:

- credit and financial institutions (including branches of third-country firms)(these are defined by reference to various sectoral financial services legislation, including banks and non-banks carrying on activities listed in the annex to the fourth Capital Requirements Directive, investment firms, life insurers and intermediaries, collective investment undertakings marketing their units or shares and branches of all these entities);
- auditors, lawyers and similar professionals when carrying out real estate, custody/client money activities, account opening/management, creation of companies, trusts and other vehicles and fund collection;
- other trust and company service providers;
- estate agents;
- any person trading in goods where cash payments of over €10,000 are received; and
- gambling service providers.

Member States have national discretion to exempt low risk gambling service providers except for casinos, and to exempt limited ancillary activities in high-value goods.

What is a beneficial owner?

There has never been true clarity on how to determine who is the beneficial owner of a customer. MLD4 is helpful in setting certain parameters. For a corporate, the beneficial owner will be any natural person with ultimate ownership or control of legal entity. A shareholding or ownership of 25% or more assumes beneficial ownership. In some cases, it will appear there is no beneficial owner: where this is the case, obliged entities should keep proof of the evidence that suggests this, agreed by senior management. Listed entities or those with equivalent transparency can be excepted from the need to assess beneficial ownership.

When dealing with a trust, the beneficial owner will be the settlor, trustees, protector, beneficiaries or class of them, and any other natural person with ultimate control over the trust, whether by direct or indirect ownership or otherwise.

What is a PEP?

Again, there have been varying interpretations of the concept of a PEP, with many firms (and their global processes) struggling to understand why a domestic PEP should be treated differently to a foreign one. MLD4 defines a PEP as a natural person who is or has been entrusted with senior specified functions. It includes:

- heads of states and governments' and ministers and their deputies and assistants;
- members of parliament or similar and members of governing bodies of political parties;
- members of high level courts whose decisions are not subject to appeal;
- members of courts of auditors or boards of central banks;
- ambassadors and similar and high ranking forces officials;
- members of the administrative, management or supervisory bodies of state-owned enterprises; and
- directors, deputy directors and board members or equivalent of international organisations.

The definition does not cover middle-ranging or junior officials, but will cover close associates and family members of PEPs. Close associates are persons known to have joint beneficial ownership or another close business relationship with the PEP or to have sole beneficial ownership of an entity known to have been set up for the benefit of the PEP. Family members of a PEP extends to the PEP's spouse (or equivalent), children, spouse (or equivalent) of children, and parents of the PEP.

The role and status of "senior management"

Several parts of MLD4 refer to senior management. As the

drivers and recitals to it relate, this does not necessarily mean the very top management. MLD4 defines "senior management" as an officer with sufficient knowledge of the money laundering and trade finance risk exposure, and sufficient seniority to take decisions affecting risk exposure. It specifically states this person need not be a board member.

Coverage – "business relationship"

MLD4 applies where an obliged entity:

- establishes a "business relationship": which is a business, professional or commercial relationship connected with the professional activities of an obliged entity and expected to have an element of duration;
- carries out an occasional transaction that amounts to €15,000 or more (this threshold stays at €15,000 notwithstanding the reduction in the threshold for coverage of obliged entities), whether by single or linked transaction, or is a "transfer of funds" under FTR2 exceeding €1,000;
- deals in goods in occasional transactions in cash amounting to €10,000 or more, whether in a single or linked transactions;
- provides certain gambling services;
- suspects money laundering or terrorist financing, regardless of whether any exemption might otherwise have applied; or
- doubts the veracity of customer data it has previously obtained.

There are a few derogations from the basic requirement, including, for example, for certain low-value e-money products.

Approach to prevention of money laundering and risk assessments

MLD4 obliges the Commission to assess the risks of money laundering and terrorist financing affecting the internal market and relating to cross-border activities. Its first report must be in place by the implementation date of MLD4 and must include details of the areas of the market that are most at risk, and address sectoral risks and common money laundering strategies. It then has to report at least every two years on its views. Member States then have to implement the Commission's recommendations or explain why they are not doing so. They must apply a risk-based approach when identifying and understanding the risks of money laundering and terrorist financing as well as related data protection concerns. Each Member State must have in place mechanisms to respond to the Commission and inform it of its own assessment and actions.

There is a role also for the ESAs, who must issue an opinion on the risks affecting the EU financial sector by 26 December 2016 and then every two years. Following the various reports, the European Commission will make delegated legislation on high risk third countries.

Requirements on obliged entities

Moving to familiar territory, Member States must require that obliged entities take appropriate steps to identify and assess money laundering and terrorist financing risks, taking into account risk factors relating to customers, geography, products, services, transactions and delivery channels. The steps they take should be proportionate to the size of the entity and must be documented and available to regulators. Obliged entities must also have in place policies, controls and procedures, approved by senior management, designed to mitigate and manage effectively risks identified by the EU, the relevant Member State or the obliged entity: including proportionate internal policies, controls and procedures, including model risk management practices, CDD, reporting, record-keeping, internal control and compliance management. Where it is appropriate to the size of the entity this may include the appointment of a compliance officer at management level, employee screening and an independent audit function. Obliged entities must also monitor and, where necessary, enhance the measures they take.

There is an additional duty on Member States to ensure that policies are appropriate across branches and subsidiaries of obliged entities.

CDD requirements

MLD4 contains a number of outright bans, specifically that there can be no anonymous accounts or passbooks, and that they should take measures to prevent the misuse of bearer shares and bearer share warrants.

MLD4 requires CDD measures to comprise:

- identifying the customer and verifying its identity on the basis of documents, data and information from a reliable and independent source (and verifying the identity and authorisation of any person acting for the customer);
- identifying the beneficial owner and taking reasonable measures to verify its identity so the obliged entity is satisfied it knows who the beneficial owner is, including taking reasonable measures to understand the ownership and control structure of the customer;
- assessing and obtaining information where appropriate on the purpose and intended nature of relationship; and

- ongoing monitoring, including scrutiny of transactions to ensure they are consistent with the obliged entity's understanding of the customer, and its business and risk profile, including where necessary the source of funds and checking that information is up to date.

Entities should apply CDD to all customers on a risk-sensitive basis, and MLD4 gives guidance that this should entail considering at least the variables listed below and being able to show that the measures taken are appropriate:

- the purpose of the account or relationship;
- the level of assets to be deposited and size of transactions;
- the regularity or duration of the relationship; and
- including due diligence on beneficiaries of insurance or investment policies at the appropriate time.

Generally, entities should ensure CDD takes place before the establishment of the relationship or before the transaction takes place, although this can happen as soon as possible afterwards, if necessary, and if the entity determines the relationship or transaction is low risk. Accounts can be opened so long as transactions cannot take place. If entities cannot complete their CDD, they should not carry on business with the customer, and should consider making a SAR.

Entities should apply CDD to existing customers on a risk-sensitive basis.

SDD

If a Member State or obliged entity identifies lower risk areas, then SDD may be permitted. Any assessment should take into account:

- customer factors: for example, listed public companies subject to disclosure requirements that have adequate disclosure of beneficial owners, public administrations or enterprises, customers in other Member States or third countries having effective AML/CFT controls or low corruption and criminal activity levels; and
- product, service, transaction or delivery channel risk factors: for example, low premium life insurance, wage-deduction based pensions, defined and limited purpose products.

Regardless, however, of whether SDD is appropriate, entities must still monitor relationships and transactions so as to detect any suspicions of money laundering or terrorist financing and report accordingly. The ESAs are to issue Guidelines by 26 June 2017 to confirm risk factors and appropriate measures relevant to SDD.

EDD

MLD4 is also fairly prescriptive about EDD. It notes that specific EDD may be appropriate for specific situations. In particular, it notes the need for it when dealing with natural persons or legal entities in high risk third countries. However, if the relevant persons are branches or subsidiaries of the obliged entity and comply fully with the obliged entity's policies this may not be necessary. In principle, entities should consider all complex and unusually large transactions and patterns, and when assessing whether to carry out EDD should take into account at least:

- customer factors: for example, involvement of a high risk country, unusual circumstances, use of asset-holding vehicles, presence of a nominee shareholder, cash-intensive businesses, or excessively complex structures;
- product, service, transaction or delivery channel factors: private banking, products favouring anonymity, non-face to face transactions, payments from unknown or unassociated third parties, new products and practices may all indicate the need for EDD; and
- geographical factors: countries with ineffective AML/CTF, or known to be corrupt, subject to sanctions or embargoes, known to support terrorism or have terrorist organisations operating there again are likely to indicate the need for EDD.

Specific considerations will apply to cross-border correspondent relationships. If an obliged entity wishes to enter into such a relationship, it must ensure it has a good understanding of the business and all necessary AML/CFT controls. The relationship must have senior management approval, be documented and the entity must have in place measures to ensure the respondent has carried out CDD on anyone with direct access to accounts.

With respect to PEPs, obliged entities must have in place risk management systems to determine whether there is a PEP and, if so, get senior management approval for dealings with the PEP, put in place adequate measures to check sources of wealth and funds and conduct enhanced ongoing monitoring. Moreover, they should apply these measures for at least a year after the person ceases to be a PEP, and apply them to family members or known close associates of PEPs. Where appropriate, they must determine whether beneficiaries of a policy are PEPs and, if so, inform senior management of this before

paying out and conduct enhanced scrutiny of the business relationship.

Reliance on others

MLD4 allows reliance on others to carry out CDD, but the obliged entity remains responsible, hence this remains a dangerous option. In any event, reliance is possible only if the relevant third party applies measures consistent with MLD4 and is supervised in doing so. MLD4 requires the obliged entity to obtain basic CDD evidence from the third party and ensure it can have access to more if it needs it. Reliance on group company CDD is permitted provided the group policy complies with MLD4.

Beneficial ownership information

MLD4 requires all legal entities to provide information on their beneficial ownership and for Member States to ensure this is held in a central register which is accessible to obliged entities for CDD purposes. Member States must also require trustees to hold details of trust settlors, trustees, protectors, beneficiaries or other natural persons exercising control.

Reporting

MLD4 places requirements on Member States to establish FIUs, and on an obliged entity to report where it knows, suspects or has reasonable grounds to suspect that funds, regardless of the amount involved, are the proceeds of criminal activity or related to terrorist financing. Obliged entities must not carry out transactions which they know or suspect to be related to proceeds of criminal activity or terrorist financing until a report has been made and only then in compliance with their FIU's instructions.

MLD4 states that disclosure of information in good faith will not be a breach of any restriction on disclosure of information imposed by any means and will not impose any liability on the reporter. It further requires that obliged entities must not disclose the fact of a report to any person, other than to the competent authorities, or to other institutions, or the group, under certain circumstances. However, entities may seek to dissuade the client from illegal activity.

Record-keeping

MLD4 requires firms to keep CDD and transaction records for at least five years from the end of the business relationship.

Sanctions and penalties

Member States may impose criminal sanctions, but must impose administrative penalties at least for breaches of MLD4 requirements on CDD, suspicion reporting, record-keeping and internal controls.

The sanctions they impose must include:

- a public statement;
- a cease and desist order;
- withdrawal or suspension of relevant authorisation;
- temporary ban on individuals;
- a maximum fine of twice the benefit or €1 million.

FTR2

FTR2 sets out the rules on information on payers and payees that accompanies fund transfers. It applies to transfers of funds in any currency, which are sent or received by a payment service provider (PSP) or intermediary established in the EU, subject to some exceptions.

FTR2 imposes duties on each of the:

- PSP of the payer;
- PSP of the payee – to detect missing information;
- intermediary PSPs – to ensure all relevant information is retained within the transfer and to have in place effective procedures to detect missing information.

Member States may make breach a criminal offence and must impose administrative sanctions for it.

ESA consultations

As required by MLD4, the ESAs are consulting on guidelines. There are two sets:

Risk Factors Guidelines

These Guidelines look at CDD and factors credit and financial institutions should consider when assessing the ML/TF risk associated with individual business relationships and occasional transactions. They will apply to regulators and obliged entities.

The Guidelines take a familiar form for UK entities used to the Joint Money Laundering Steering Group Guidance, even including a statement to remind obliged entities that sanctions compliance is not subject to the risk – based approach.

Title I covers the subject matter, scope and definitions. The Guidelines are addressed to credit and financial institutions as well as authorities, and state that the authorities are to use the guidelines when assessing adequacy of firms' procedures. While the Guidelines cover ML and TF risks, compliance with the sanctions regime is outside their scope.

Title II covers assessing and managing risk. It sets out how firms should carry out business-wide risk assessments to help them understand where they are exposed to ML/TF risk. It embellishes on MLD4 in requiring firms to assess risks against products, jurisdictions, customers, and transaction and delivery channels. It states firms should use the findings of the business-wide assessment to decide appropriate levels and type of CDD. It stresses the importance of taking a holistic

view, and of identifying all relevant risk factors. It deals also with monitoring and review of risk assessments to ensure they are regular, tested and kept up to date, and notes also the importance of understanding whether the risk associated with any particular relationship changes.

The Guidelines say that, when identifying ML/TF risk, entities should take account of various sources of information. They should always consider European Commission, national, regulatory and FIU assessments and information from their initial CDD, and the Guidelines make suggestions on other sources to consider.

In terms of risk factors, the Guidelines cover:

- customer risk: the business, reputation, behaviour of customers and beneficial ownership;
- country and geographical risk: where customer and its beneficial owner is based, does their main business, and have personal links. The Guidelines also say firms should look not only at FATF and Moneyval assessments but also at sanctions, bribery and other similar concerns;
- products, services and transactions risk: assessments should look at transparency, complexity and value; and
- delivery channels risk: including considering whether the transaction is face to face, and whether it uses introducers or intermediaries.

When assessing ML/TF risk firms should take a holistic view and weight risk factors appropriately. They should make an informed judgement based on different factors, which are likely to vary between products and customers. Entities must devise their own methods for categorising business relationships and occasional transactions, and the Guidelines note that there may be alternatives to the basic low, medium, or high risk categorisation.

The Guidelines also address risk management, setting out situations where SDD or EDD may apply. They stress the requirements of MLD4 in always applying measures to assess source of wealth and funds when dealing with PEPs and the need for senior management approval, as well as the resultant need to apply enhanced ongoing measures.

This part of the Guidelines also addresses:

- correspondent relationships, and the need to apply EDD and adjust it on a risk-sensitive basis;
- unusual transactions, and the need to have policies to detect and assess whether there is a suspicion;
- high risk jurisdictions and situations, and the need to decide what measures to apply and when;
- derisking, and the fact that nothing requires firms to refuse business with entire categories of customer; and
- regular monitoring and review, and record-keeping of reviews and changes.

Title III provides sector-specific guidelines dealing with potential risks for:

- correspondent banks;
- retail banks;
- e-money issuers;
- money remitters;
- wealth management;
- trade finance providers;
- life insurers; and
- investment managers.

Risk-based Supervision guidelines

These are Guidelines to apply to regulators on the characteristics of a risk-based approach to AML and TF supervision and the steps to be taken when conducting supervision on a risk-sensitive basis.

They require regulators to establish and maintain an effective model for risk-based supervision, requiring them to:

- collect information and identify money laundering and terrorist financing risk factors;
- assess risks;
- act on the risk assessment; and
- monitor and follow up the assessment,

so they understand the business of the subject of their assessment.

What does it all mean?

Clearly, the laws of all Member States will need to change in time for MLD4. Some more than others. The UK already has advanced laws on AML and CFT and will probably be among the jurisdictions that make the fewest changes, especially as it is already pressing ahead with its beneficial ownership registry.

.

Contacts

Emma Radmore
Managing Associate
D +44 20 7246 7206
emma.radmore@dentons.com

Andrew Cheung
Partner
D +44 20 7320 6437
andrew.cheung@dentons.com

© 2015 Dentons. This publication is not designed to provide legal or other advice and you should not take, or refrain from taking, action based on its content. Attorney Advertising. Please see dentons.com for Legal Notices. Dentons is a global legal practice providing client services worldwide through its member firms and affiliates. Dentons UKMEA LLP is a limited liability partnership registered in England and Wales under no. OC322045. It is authorised and regulated by the Solicitors Regulation Authority. A list of its members is open for inspection at its registered office: One Fleet Place, London EC4M 7WS. Any reference to a "partner" means a person who is a partner, member, consultant or employee with equivalent standing and qualifications in one of Dentons' affiliates.