EVERSHEDS SUTHERLAND

Helping you navigate the changes

A summary of MLR 2017

Introduction

The Money Laundering, Terrorist financing and Transfer of Funds (Information on the Payer) Regulations 2017 (the "MLR 2017") came into force on the 26 June 2017, repealing the Money Laundering Regulations 2007 ("2007 MLR") and transposed the EU Fourth Money Laundering Directive ("4MLD") into UK law. The 4MLD gives effect to updated recommendations issued by the Financial Action Task Force ("FATF") and the purpose of the MLR 2017 is to ensure that the UK's anti-money laundering ("AML") and counter terrorist financing ("CTF") regime is up to date and effective in seeking to tackle the risk of money laundering ("ML") and terrorist financing ("TF").

The MLR 2017 introduces a number of new and updated requirements on entities which fall within scope of the MLR 2017 ("Relevant Persons"). In addition, the Joint Money Laundering Steering Group ("JMLSG") has updated its AML/CTF guidance and we encourage all regulated entities to ensure they have read the MLR 2017 and the revised JMLSG guidance, so that they are aware of the impact on their business. Supervisory authorities, such as the Financial Conduct Authority ("FCA") and Her Majesty's Revenue and Customs ("HMRC") have also issued, or will be issuing, amended sector specific guidance.

This note summarises key changes brought about by the MLR 2017. This is not a complete guide to all changes but seeks to highlight certain key issues which regulated entities should be giving consideration to. Should you have any questions, please do not hesitate to contact us.

Overview

Policies and procedures

- proportionate to size and nature of the business
- positive obligation to regularly review and maintain
- senior management approval required
- application of group policies in non-EU jurisdictions

Penalties and enforcement

- increased range of offences for which civil and/or criminal penalties can be applied
- new criminal offences
- new civil powers for the FCA and HMRC

Risk assessment

- national level
- sector level
- entity/firm-wide

Internal Controls

- appointed board member/ senior manager responsible for compliance with MLR 2017
- nominated officer
- screening of relevant employees (inc. assessment of knowledge)
- independent audit function
- ownership and management restrictions
- training to including data protection

Reliance

- now applies to all Relevant Persons
- additional requirements for reliance including arrangements for the provision of copy documents and record keeping requirements

Due diligence requirements

- amended definition and scope of a "business relationship"
- emphasis on firm-wide and customer risk assessment
- amended definition of CDD measures
- SDD no longer has automatic application
- EDD required in specified situations, with a focus on risk assessment and high risk jurisdictions
- on-going monitoring requirements

Politically Exposed Persons ("PEPs")

- amended definition to include domestic PEPs
- varying levels of risk and due diligence required for different categories of PEPs
- FCA guidance

Risk assessment

Position under 2007 MLR

Regulation 20 of the 2007 MLR required Relevant Persons to 'establish and maintain' risk-sensitive policies relating to risk assessment and management.

Amended position under MLR 2017

One of the significant changes brought about by the MLR 2017 is the requirement for AML/CTF risk assessments to be conducted at a national, sector and entity level[1]:

- **National risk assessments ("NRA")[2]** – the UK's first NRA was conducted in October 2015 in light of FATF's 2012 Recommendations. The MLR 2017 places the Treasury and Home Office under an obligation to undertake another AML/CTF NRA prior to 26 June 2018 and to keep this up to date. The MLR 2017 state that the NRA should identify areas where enhanced due diligence ("EDD") measures should be applied, identify sectors of lower and greater risk and consider whether any rules made by a supervisory authority (including the FCA and HMRC) are appropriate and relevant to the risk of ML/TF applicable to that sector. The NRA is an important tool in assisting supervisory authorities and Relevant Persons conduct their own more targeted risk assessments.
- **Sector risk assessments[3]** – the MLR 2017 state that supervisory authorities must undertake an AML/CTF risk assessment of the sectors which they supervise. In addition, each supervisory authority must develop and record in writing, risk profiles for each type pf Relevant Person in its sector. Such profiles must be kept under review and up to date and where it would assist Relevant Persons in the sector, be provided to them.
- **Entity/firm-wide risk assessment[4]** – the MLR 2017 now places an obligation on Relevant Persons to take appropriate steps (bearing in mind the size and nature of the business) to identify and assess the risks of ML/TF to which their business is subject, taking into account, where relevant, the findings from the NRA and sector specific risk assessments. Firm-wide risk assessments should take into account risk factors associated with:
  - customers;
  - the countries or geographic areas in which a Relevant Person operates;
  - products or services;
  - transactions; and
  - delivery channels.

The MLR 2017 requires that a **written record of the firm-wide risk assessment is maintained** and that Relevant Persons should be prepared to provide this to their supervisory authority if requested.

Part 1 and Annex 4 of the revised JMLSG guidance provides further information on conducting risk assessments.

1 Chapter 2 of the MLR 2017
2 Regulation 16 of the MLR 2017
3 Regulation 17 of the MLR 2017
4 Regulation 18 of the MLR 2017

Eversheds Sutherland comment

"Risk assessment is now a significant part of AML obligations under the MLR 2017, with obligations being imposed on the Government, supervisory authorities and Relevant Persons within the scope of the MLR 2017. Risk assessments will form the basis of compliance with the MLR 2017.

Assessing ML/TF risk within a business is no easy task. A detailed understanding of how ML/TF takes place and is becoming more sophisticated, how it can take place within a particular sector and the risks particular customers pose are vital. MLROs need to ensure that they have a detailed understanding of their business and sector to ensure that their firm's risk assessments are sufficient."

Policies, controls and procedures

Position under 2007 MLR

Pursuant to regulation 20, Relevant Persons were required to establish and maintain appropriate and risk-sensitive policies and procedures in order to mitigate the risk of ML/TF. Such policies and procedures had to provide for EDD, the identification and scrutiny of complex and unusual transactions/patterns of transactions as well as being able to identify customers who were politically exposed persons ("PEPs").

Regulation 15 of the 2007 MLR created obligations on **credit and financial institutions** in respect of any subsidiaries and branches which were located outside of the EEA, essentially requiring them to applying measures which were equivalent to the 2007 MLR standards.

Amended position under MLR 2017

As was the case pursuant to the 2007 MLR, the MLR 2017[5] require Relevant Persons to establish and maintain policies and procedures which mitigate and manage the risks of ML/TF. Such risks should be identified through each Relevant Person's firm-wide AML/CTF risk assessment and should continue to provide for EDD and the identification and scrutiny of complex and unusual transactions/patterns of transactions.

Importantly, the MLR 2017 state that:

- Such policies and procedures must include risk management practices, internal controls, customer due diligence ("CDD"), reliance, record keeping and the monitoring and communication of policies and procedures;
- There is a positive obligation on Relevant Persons to ensure that policies and procedures are regularly reviewed and updated. Relevant Persons must maintain a record in writing of which policies and procedures have been established, any changes made to them as a result of a review and all steps taken to communicate these policies and procedures within the business;
- Policies and procedures must be proportionate to the nature and size of the business;
- Policies and procedures must be approved by senior management (being an officer/employee with sufficient knowledge of the relevant person's ML/TF risk exposure and of sufficient authority to take decisions relating to this) thereby emphasising the importance of senior management responsibility and ownership for ML/TF risks; and
- Money service businesses ("MSBs") which utilise agents are now obligated[6] to ensure that additional measures are taken to assess whether an agent used would satisfy the fit and proper test as set out in regulation 58 of the MLR 2017 and must assess the risk of each agent being used for ML/TF.

The MLR 2017 also imposes specific obligations in the context of group companies[7], stating that parent undertakings are obligated to ensure that the policies and procedure they establish apply to all its subsidiaries and branches, including those situated outside of the UK when it is engaging in any regulated activity. In contrast to the 2007 MLR, these requirements apply to all Relevant Persons and not just credit/financial institutions.

Where a subsidiary is based in a jurisdiction which has AML laws which are not as strict as the UK's the parent undertaking must ensure that its subsidiary applies measures which are equivalent to UK standards. Where the law of the other jurisdiction does not permit the application of such equivalent measures, the Relevant Person in the UK must inform its supervisory authority and take additional measures to handle the risk of ML/TF. In such circumstances, the relevant supervisory authority is required to determine whether such additional measures are sufficient to mitigate the ML/TF risk[8]. If it does not consider it to be so, the supervisory authority has the power to direct the relevant parent undertaking;

- not to enter into a business relationship or to terminate an existing business relationship;
- not to undertake certain transactions;
- to cease operations in the third country; and/or
- to ensure that its subsidiary does not do any of the above.

5 Regulation 19 of the MLR 2017
6 Regulation 20 of the MLR 2017
7 Regulation 20 of the MLR 2017
8 Regulation 25 of the MLR 2017

Eversheds Sutherland comment

"Over the last 12+ months, the FCA has placed a greater importance on the accountability of individuals within the banking sector, by way of introduction of the Senior Managers and Certification Regime. Whilst the MLR 2017 has broader application than just the banking sector, it builds on this and emphasises the responsibilities of senior management within regulated firms and highlights the need for those in senior positions to take ownership of ML/TF risks within their business.

In an effort to reduce the risk of business being done in high risk jurisdictions, where AML rules may not meet UK standards, supervisory authorities can direct regulated parent undertakings not to enter into specified business or to cease operations in specified third countries entirely, or to ensure their subsidiaries do so."

Internal controls

Amended position under MLR 2017

The MLR 2017 imposes the following obligations, where appropriate having regard to the size and nature of the business[9]:

- In addition to appointing a Nominated Officer, each Relevant Person must appoint one individual who is a member of the board of directors, (or in absence of a board, the equivalent management body) or of its senior management, as the officer responsible for compliance with the MLR 2017. This emphasises again the importance of senior management responsibility and ownership for ML/TF risks. Relevant Persons must notify their supervisory authority of this appointment within 14 days of this being made;
- Relevant Persons must conduct screening of relevant employees and agents both before appointment and at regular intervals during the course of the appointment. The MLR 2017 is clear that screening includes an assessment of the skills, knowledge and expertise of the individual to carry out their functions effectively, as well as an assessment of their conduct and integrity; and
- Establish an independent audit function to assess the adequacy and effectiveness of AML policies and controls, make recommendations in relation to such policies and controls and monitor compliance with the MLR 2017.

Ownership & management restrictions[10]

The MLR 2017 states that no person may be the beneficial owner, officer or manager (or a sole practitioner) of an:

a. Auditor, insolvency practitioner, external accountants or tax advisers;

b. Independent legal professional;

c. Estate Agent; or

d. High Value dealer

Unless they have been approved to hold that position by the relevant supervisory authority. Acting in such a position without the necessary approval will amount to a criminal offence unless an application is submitted before 26 June 2018 and is still to be determined. Supervisory authorities have to approve such applications unless the relevant individual has been convicted of a "relevant offence", which includes offences relating to money laundering, bribery, computer misuse and tax evasion.

Relevant firms must take reasonable care to ensure no-one is appointed to, or continues to act in, these roles without the necessary approvals being in place.

9 Regulation 21 of the MLR 2017
10 Regulation 26 of the MLR 2017

Eversheds Sutherland comment

"The JMLSG guidance notes that it is important that the individual appointed as having responsibility for ensuring compliance with the MLR 2017, the MLRO and the director/senior manager allocated overall responsibility for the establishment and maintenance of systems and controls (where they are not the same person) are all clear as to the responsibilities of each role so that individual's understand their role and so that supervisory authorities can identify and understand where responsibilities lie.

Screening relevant employees is more than conducting criminal record or credit checks. The MLR 2017 specifically state that this includes an assessment of the skills, knowledge and expertise of the individual to carry out their functions effectively, as well as an assessment of their conduct and integrity."

Training

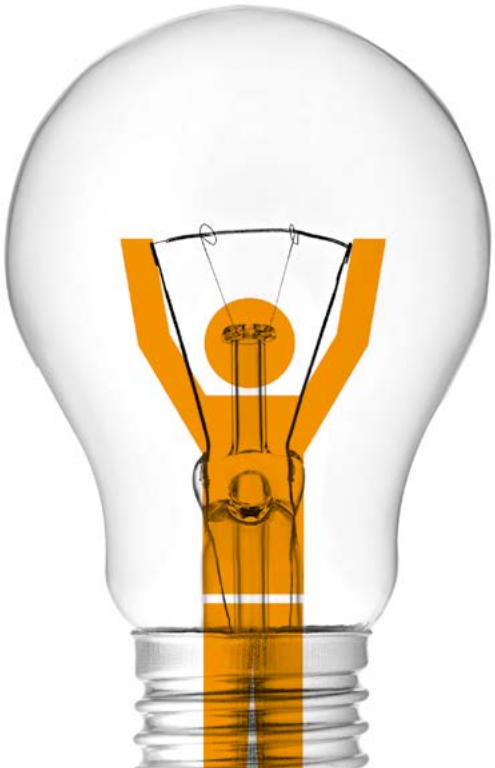
Position under 2007 MLR

Regulation 21 imposed a requirement to make all relevant employees aware of the law relating to ML/TF and to ensure they were regularly given training on how to recognise and deal with transactions/activities which may be related to ML/TF.

Amended position under MLR 2017

The scope of training required under the MLR 2017 has been widened to include data protection[11]. The requirement for training to take place regularly continues and the JMLSG guidance notes that Relevant Persons should take into account the nature and size of their business, as well as the extent of ML/TF risks to which the business is subject (as per its firm-wide risk assessment), when determining how often training should be provided.

The MLR 2017 also explicitly requires Relevant Persons to maintain a record in writing of the measures taken to ensure compliance with training requirements under the MLR 2017. As such, if they do not have so already, Relevant Persons should ensure they have suitable training records established.



11 Regulation 24 of the MLR 2017

Eversheds Sutherland comment

"Data protection training, which is relevant to the implementation of the MLR 2017, must now be provided to relevant employees."

Customer Due Diligence ("CDD")

Position under 2007 MLR

Regulation 7 required the application of CDD when a Relevant Person:

- established a business relationship;
- carried out an occasional transaction;
- suspected ML/TF;
- doubted the veracity or accuracy of documents/data/information previously obtained for the purposes of CDD; and
- at other appropriate times, applying a risk-sensitive approach.

A "business relationship" was defined as "a *business, professional or commercial relationship between a relevant person and a customer, which is expected by the relevant person, at the time when contact is established, to have an element of duration*".

CDD measures were defined as:

- identifying and verifying the identity of customers on the basis of documents, data or information obtain from a reliable and independent source;
- identifying beneficial owners (where applicable) and taking adequate measures on a risk-sensitive basis to verify this identity; and
- obtaining information on the purpose and intended nature of the business relationship.

Amended position under MLR 2017

Regulation 27 of the MLR 2017 replicates the requirements of regulation 7 under the 2007 MLR in respect of when CDD must be conducted. However, the following differences apply:

- CDD must also be conducted when a Relevant Person engages in an occasional transaction which amounts to a transfer of funds exceeding 1,000 Euros;
- The MLR 2017 adds an additional limb to the 2007 MLR definition of a "business relationship", requiring the relationship between a customer and Relevant Person to "arise out of the business of the Relevant Person" – a change in definition which should not pose too many challenges going forward;
- Trust and service company providers should note that a "business relationship" now includes one where the Relevant Person is asked to form a company for its customer, even if this is the only transaction carried out for that customer;
- Estate agents should note that in contrast to the position under the 2007 MLR, the new MLR 2017 specifically states that they are considered to be entering into a business relationship with a purchaser as well as a seller, at the point when the purchaser's offer is accepted by the seller;
- The way CDD measures are implemented must be determined by reference to the Relevant Person's firm-wide AML/CTF risk assessment, as well as its assessment of risk associated with a given customer (annex 4-II of the JMLSG guidance provides some examples of risk factors relating to customers).
- CDD measures now mean:
  - identifying the customer and verifying their identity (unless the identity is already known and has previously been verified) using documents/information from a reliable source which is independent of the person being verified;
  - assessing and where appropriate obtaining information on the purpose and intended nature of the business relationship or occasional transaction;
  - where the customer is a body corporate – obtaining the corporate's name, company/registration number and registered office address and if different, its principal place of business (and verifying this information);
  - where the customer is a body corporate which is not listed on a regulated market, Relevant Persons must also take reasonable measures to identify and verify the law to which the customer is subject, its constitution (i.e. its articles of association or other governing documents) and the full names of the board of directors (or equivalent management body) and the senior persons responsible for operations. Relevant Persons must also identify beneficial owners and take reasonable measures to verify their identity; and

12 Regulation 30 of the MLR 2017

- where a person purports to act on behalf of a customer, the Relevant Person must verify that they are so authorised and must identify that person and verify their identity on the basis of documents or information which is independent of that person and the customer.

– CDD must be conducted in respect of existing customers when the Relevant Person becomes aware of circumstances which affect the risk assessment of a customer (for example, their identity, or the identity of a beneficial owner, changes, a transaction is not consistent with previous transactions, the purpose or nature of the business relationship changes etc.)

The MLR 2017 is clear that where CDD cannot be conducted, the Relevant Person must not establish a business relationship, must terminate an existing relationship and must not conduct any transaction through a bank account on that customer's behalf. The MLR 2017 does set out some examples of where CDD can be conducted after a business relationship is established[12]. If Relevant Persons rely on these exemptions they should fully document the reasons for doing so.

Eversheds Sutherland comment

"The MLR 2017 broadens the scope of CDD, narrows the application of SDD and emphasises the need for risk-based EDD in certain circumstances, with a real focus on business being done in, or with customers based in, high risk jurisdictions."

"Regulation 43 of the MLR 2017 requires regulated and un-regulated corporate entities to notify Relevant Persons, of which they are customers, of changes to their CDD information, including beneficial owners, within 14 days of the corporate becoming aware of the change. Failure to comply will be a criminal offence."

Beneficial ownership

Position under 2007 MLR

The 2007 MLR required that the beneficial owner of customers be identified (and verified on a risk basis). The 2007 MLR provided a definition of "beneficial ownership" but did not contain any means for identifying beneficial ownership.

Amended position under MLR 2017

Further information regarding the definition of "beneficial ownership" is provided for in the MLR 2017, with specific information regarding trusts and similar arrangements being specifically set out in the regulations.

Corporate and other legal entities are now required to maintain adequate, accurate and current information on their beneficial ownership in a central register. However, we note that regulation 28 of the MLR 2017 specifically states that Relevant Persons cannot rely solely on these registers as a means of identifying and verifying beneficial owner details.

In contrast to the 2007 MLR, which stated the beneficial owners of trusts were individuals who benefited at least 25% of the property in the arrangement or any person who exercised control over at least 25% of the property in the arrangement, the MLR 2017 removes the 25% threshold and states that the beneficial owner is the:

- settlor;
- trustees;
- beneficiaries;
- any class of persons in whose main interest the trust is set up; and
- any individual who has control over the trust (which is subsequently defined in regulation 6(2) of the MLR 2017).

Eversheds Sutherland comment

"Recent focus on issues such as the Panama Papers highlighted the use of complex ownership structures, such as overseas trusts and companies, as potential tools to evade scrutiny for money laundering purposes, making the identification of beneficial owners difficult for regulated entities. Enhanced measures pursuant to the MLR 2017 attempt to address this and place obligations on regulated entities to delve further into the ownership of such complex structures."

Simplified Due Diligence ("SDD")

Position under 2007 MLR

Pursuant to the 2007 MLR, SDD could be conducted if a customer, product or transaction fit within specified criteria set out in the regulations.

Amended position under MLR 2017

In a significant departure from the 2007 MLR, and as part of the risk based approach emphasised within the MLR 2017, "automatic" SDD requirements are no longer applicable. Instead, if a Relevant Person wishes to apply SDD for a specific customer/transaction it must consider various risk factors (examples of which are set out in the MLR 2017) in determining whether SDD is appropriate[13]. The MLR 2017 states that SDD will only be appropriate if the Relevant Person is able to determine on a risk basis that the business relationship or transaction presents a low risk of ML or TF.

Importantly, SDD does not mean that CDD can be dispensed with altogether. Instead, it means that the extent of the CDD measures applied can be adjusted to reflect the lower risk. The JMLSG guidance provides further information on risk factor guidelines and what SDD measures could be applied (see Annex 5-III), which include adjusting:

- the timing of CDD;
- the quantity of information obtained for identification and verification (for example using only one document);
- the quality or source of information used for identification and verification; and
- the frequency of CDD updates and transaction monitoring.

13 Regulation 36 of the MLR 2017

Eversheds Sutherland comment

"The application of SDD is no longer automatic to specific customers, products or transactions. Instead it requires an assessment of risk (utilising firm-wide AML/CTF risk assessments) and an adjustment to the extent of the CDD measures which Relevant Persons should apply. When SDD is applied, the reasons for doing so should be fully documented."

Enhanced Due Diligence ("EDD")

Position under 2007 MLR

Regulation 14 required Relevant Persons to apply EDD on a risk-sensitive basis and in certain specific situations (for example, when a customer was not physically present for identification purposes or when a business relationship or occasional transaction was conducted for a PEP).

Amended position under MLR 2017

As was the case under the 2007 MLR, EDD must be applied on a risk-sensitive basis in any situation which presents a higher risk of ML or TF. The MLR 2017 sets out 7 specific circumstances in respect of which EDD must be applied. These include:

- Any case which a Relevant Person identifies, using its firm-wide risk assessment, that a customer or transaction gives rise to a high risk of ML/TF. The MLR 2017 sets out factors which should be considered in making such a determination, including customer, product, service, transaction and delivery channel risk factors. The JMLSG guidance (Annex 5-IV) has further information regarding suggested risk factors for EDD;
- Any transaction with a person established in a high risk third country. The European Commission will now publish, from time to time, a "black list" of "high-risk third countries". Relevant Persons will be required to apply EDD in relation to any transaction or business relationship with a person who is established in a high-risk jurisdiction;
- Correspondent relationships with a credit or financial institution;
- Where a Relevant Person identifies that a customer or potential customer is a PEP or is a family member or known close associate of a PEP;
- Any case where a customer has provided false or stolen identification documents or information and the Relevant Person proposes to continue dealing with that person;
- Any case where the transaction is complex and unusually large or where there is an unusual pattern of transactions; and
- In any other case which by its nature can present a higher risk of ML/TF.

The MLR 2017 sets out 4 examples of EDD measures:

1. Seeking additional independent, reliable sources to verify information provided;
2. Taking additional measures to understand better the background, ownership and financial situation of the customer, and other parties to the transaction;
3. Taking further steps to be satisfied that the transaction is consistent with the purpose and intend nature of the business relationship; and
4. Increasing the monitoring of the business relationship, including greater scrutiny of transactions.

Eversheds Sutherland comment

"Although the procedures to follow where EDD is applicable have not greatly altered under the MLR 2017 it is important to note the automatic applicability with any party which is established in a high risk country. As of July 2017, this included; Afghanistan, Bosnia & Herzegovina, Iran, Iraq, Syria, Uganda, Democratic People's Republic of Korea, Vanuatu and Yemen"

Politically Exposed Persons ("PEPs")

Position under 2007 MLR

Regulation 14(4) of the 2007 MLR stated that senior management approval was required before any Relevant Person entered into a business relationship, or conducted an occasional transaction, on behalf of a PEP. In addition, adequate measures had to be taken to establish source of wealth and source of funds.

The definition of a PEP meant that only foreign PEPs were applicable for the purposes of the 2007 MLR.

Amended position under MLR 2017

Senior management approval and the requirement to establish source of funds and source of wealth remain, however, regulation 35 of the MLR 2017 sets out wider definitions and requirements in relation to PEPs:

- The definition of PEPs has been expanded to include domestic PEPs;
- Regulation 35(14) lists examples of "prominent public functions" for the purpose of identifying PEPs;
- Relevant Persons must have appropriate risk management systems and procedures, taking into account the firm-wide ML/TF risk assessment, to identify customers and/or beneficial owners who are PEPs or a family member or known associate of a PEP and to manage the risks associated with these relationships. The JMLSG guidance makes it clear that a "proportional, risk based and differentiated approach" to relationships with PEPs and transactions involving PEPs must be taken, depending where they are assessed on the scale of risk. A one-size-fits-all approach to PEPs will not be sufficient;
- EDD should be applied to PEP relationships, the extent of which should be assessed by the Relevant Person.

The revised JMLSG guidance makes it clear that when approving PEPs, senior managers should ensure they have considered the ML/TF risk posed by the particular PEP and how the relevant person will manage that risk.

The FCA has a duty to provide guidance on PEPs including how varying risks associated with different categories of PEPs should be addressed. The guidance was issued on 6 July 2017.[14]

14 https://www.fca.org.uk/publication/finalised-guidance/fg17-05.pdf

Eversheds Sutherland comment

"Relevant Persons should be careful to ensure that the EDD carried out in relation to PEPs is proportionate. The 4MLD is clear that refusing to establish a business relationship or carry out a transaction with a person solely based on their status as a PEP will not be acceptable and the Financial Ombudsman may assess complaints from PEPs, family members and known close associates who have suffered from financial exclusion."

Reliance

Position under 2007 MLR

Regulation 17 enabled Relevant Persons to rely on other specified Relevant Persons to apply CDD measures, provided that they consented to being relied upon. Where reliance was exercised the Relevant Person remained liable for compliance with the 2007 MLR requirements.

Only the following Relevant Persons could be relied upon:

- credit or financial institutions who were authorised persons;
- auditor, insolvency practitioner, external accountant, tax adviser or independent legal professional which were supervised by designated supervisory authorities;
- any of the above in another EEA state who were supervised for AML purposes; or
- any of the above in a non-EEA state which were subject to equivalent AML requirements.

Amended position under MLR 2017

Regulation 39 of the MLR 2017 widens the categories of persons that can be relied upon for CDD purposes so that it includes all other Relevant Persons who are subject to the MLR 2017. However, a Relevant Person is not permitted to rely on another other Relevant Person established in a high risk jurisdiction (as identified by the European Commission).

In order to rely on another Relevant Person the person seeking to rely must:

- obtain from the third party all the information it needs to satisfy CDD;
- enter into arrangements which permit them to obtain copies, immediately upon request, of any identification and verification data/documents in respect of the customer or beneficial owner; and
- enter into arrangements which require the person being relied upon to maintain records for a period of time which is in keeping with the MLR 2017.

Eversheds Sutherland comment

"It will come as a welcome development in the non-bank sector, that the ability to rely on regulated entities has been expanded."

On-going monitoring

Position under 2007 MLR

Regulation 8 required Relevant Persons to conduct ongoing monitoring of business relationships. This involved:

- scrutinising transactions undertaken to ensure they were consistent with the customer's business and risk profile; and
- keeping documents, data and information obtained for CDD up to date.

Amended position under MLR 2017

In keeping with the theme of having risk-sensitive process in place, the JMLSG guidance states that Relevant Persons should have on-going monitoring measures established which are commensurate with assessed risk of ML/TF.

Regulation 27(11) of the MLR 2017 specifically states that Relevant Persons must conduct on-going monitoring of business relationships by scrutinising transactions and undertaking reviews of existing records and ensuring that they are kept up to date. The extent of these ongoing obligations should be determined by a Relevant Person's firm wide ML/TF risk assessment. Enhanced on-going monitoring must be applied to high risk customer relationships.

Importantly the MLR 2017 makes it clear that applying SDD to a customer or transaction does not remove the obligation to conduct on-going monitoring, although the level and extent of this may vary in order to reflect the lower level or ML/TF risk which has been assessed.

Eversheds Sutherland comment

"It should be remembered that the formulation of monitoring processes should be directly mapped to each Relevant Person's AML risk assessment, both firm-wide and at a customer level."

Civil and criminal penalties

Position under 2007 MLR

The 2007 MLR provided that the FCA or HMRC could impose a financial penalty, of such amount as it considered appropriate, for breaches of specified parts of the 2007 MLR.

The 2007 MLR provided that failure to comply with certain aspects of the regulations amounted to a criminal offences which, if found liable, Relevant Persons could face a fine and/or a term of imprisonment not exceeding two years.

Amended position under MLR 2017

The MLR 2017 enables the FCA or HMRC to impose financial penalties for a broader range of breaches of the MLR 2017. In addition, they can also:

- publish a statement censuring a Relevant Person if it is satisfied that the Relevant Person has contravened a relevant requirement on him; and/or
- prohibit an individual from holding an office or position involving responsibility for taking decisions about the management of the Relevant Person."

The MLR 2017 also enable the FCA to cancel or suspend a Relevant Person's authorisation/permission, or apply restrictions on such permissions, for a period which does not exceed 12 months.

The MLR 2017 also set out factors the FCA and HMRC must consider when determining what disciplinary action to take.

The MLR 2017 provides for the commission of criminal offences for a broader range of failures to comply with the MLR 2017 and creates new criminal offences of:

- prejudicing a criminal investigation; and
- knowingly or recklessly making a false or misleading statement in purported compliance with the MLR 2017.

Eversheds Sutherland comment

"The FCA and HMRC can now impose financial penalties for a broader range of breaches of the MLR 2017, as well as publishing statements censuring Relevant Persons and prohibiting individuals from holding certain functions within a Relevant Person."

Contacts

Zia Ullah
Partner

T: +44 16 1831 8454
ziaullah@eversheds-sutherland.com

Neill Blundell
Partner

T: +44 20 7919 4533
neillblundell@eversheds-sutherland.com

Leonie Tear
Principal Associate

T: +852 2186 3271
leonietear@eversheds.com

Lindsey Roberts
Senior Associate

T: +44 161 831 8199
lindseyroberts@eversheds-sutherland.com

Emma Gordon
Partner

T: +44 20 7919 4931
emmagordon@eversheds-sutherland.com

Saira Choonka
Principal Associate

T: +44 20 7919 0801
sairachoonka@eversheds-sutherland.com

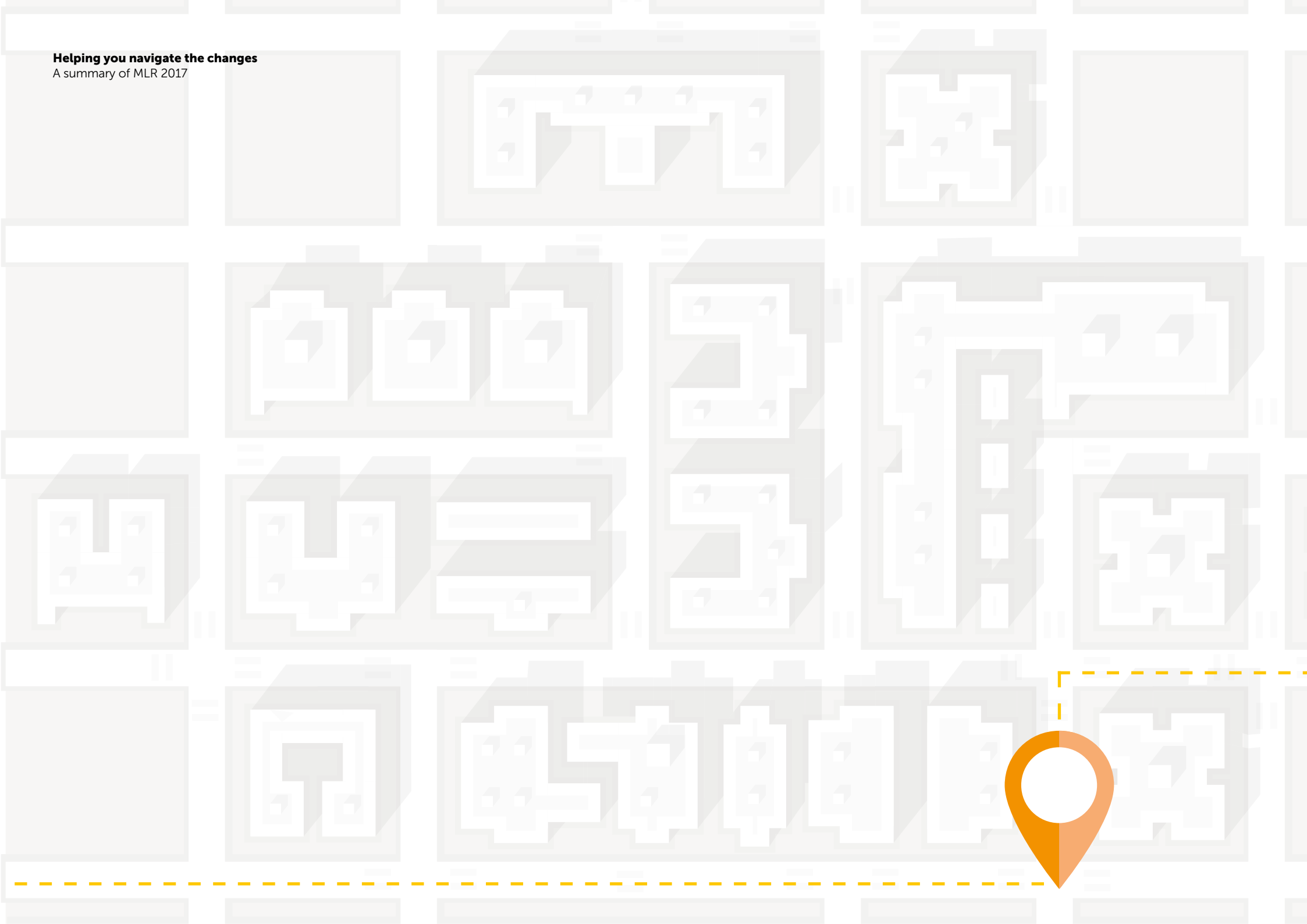
Victoria Turner
Senior Associate

T: +44 16 1831 8718
victoriaturner@eversheds-sutherland.com

Helen Harvey
Senior Associate

T: +44 20 7919 4847
helenharvey@eversheds-sutherland.com

Helping you navigate the changes
A summary of MLR 2017



eversheds-sutherland.com