

# **The Money Laundering and Terrorist Financing (Amendment) Regulations 2019 (“MLRs”):**

## **What You Need to Know for KYC and CDD**

---

## Contents

---

### Introduction

- 1) Welcome to the Family – New Entities and Expanded Scope of Covered Activities**
- 2) Risk Assessing the New- Expanded Requirements**
- 3) Widening the Net on Training**
- 4) Regulation 27(8) KYC and Existing Customers- It's a Taxing Matter**
- 5) Regulation 28- Customer Due Diligence Measures**
- 6) Regulation 28(19) - eKYC Has Finally Arrived!**
- 7) Regulation 33 – High Risk Third Countries.**
- 8) Next Steps**

### Appendix

## Introduction

---

The 10<sup>th</sup> of January 2020 was the official transposition date for the requirements of the 5<sup>th</sup> Anti-Money Laundering Directive (“**5AMLD**”) by EU Member States. Putting to one side the UK’s impending departure from the EU, a series of amendments to the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (“**MLRs**”) have now come into effect. These amendments not only transpose the majority of changes proposed in the 5AMLD, but also introduce some additional items that affect how relevant persons (those required to comply with the MLRs) approach the use of new AML technology.

The following is a high-level summary of the key changes we identified in relation to the obligations that must be met by relevant persons.

## 1) Welcome to the Family – New Entities and Expanded Scope of Covered Activities

---

Art market participants, letting agents and crypto exchange and wallet providers (VASPs) are the latest new members of the family of entities now required to comply with the MLRs here in the UK. Some participants will be finding their feet over the next few months as they navigate the AML regulatory terrain. On the positive side, this will hopefully provide other financial institutions with additional information, as needed, to satisfy themselves that these businesses have controls in place to detect and prevent financial crime risks.

The activities undertaken by a **tax advisor** covered by the MLRs has also expanded, from advice about tax affairs to now cover:

- **Material aid, or**
- **Assistance or**
- **Advice**

in connection with the tax affairs of other persons, whether provided directly or through a third party.

### Key Changes

- Art market participants and VASPs now covered by the MLRs
- Real Estate sector cover by MLRs includes letting agents
- Expansion of tax-related services covered by the MLRs

### What to do?

- New relevant persons need to develop and operationalise KYC and CDD processes both comply with the MLRs and are appropriate for their business.
- Tax advisors to review existing processes and procedures to identify where KYC and CDD activities must be extended to cover services identified in MLRs; additional training may be required to ensure that advisory understand changes to procedures.

## 2) Risk Assessing the New – Expanded Requirements

---

A small but significant change was made to Regulation 19 – Policies, Procedures and Controls. Regulation 19(4) requires that appropriate measures are taken before and during the adoption of new technology to assess and mitigate any associated AML or TF risks.

This obligation has been expanded so that, essentially, this assessment exercise, and corresponding control implementation, also be applied to **new products and new business practices (including new delivery mechanisms)**.

These new requirements could conceivably cover centralizing certain AML functions, introducing mobile phone access via new apps, which are just a few activities I can think of. Hopefully, the amendments to the JMLSG Guidance, anticipated sometime this February, will provide some more insight on the types of activities this amendment is intended to capture.

### Key Changes

- Policies and procedures concerning AML or TF risks required to mitigate risks associated with new products and new practices (including delivery mechanisms)

### What to do?

- Identify KYC and CDD projects and change initiatives and incorporate procedures and processes to ensure compliance with new requirements.
- Assess AML and TF risks, record results and ensure that demonstrable roll-out of additional control measures are operationalised.

### 3) Widening the Net on Training

---

There have been cases where a third party acting as agent for a financial institution, has ended up exposing a financial institution to financial crime risks. The amendments made to Regulation 24 appear to not only try address one of the causes of this risk – a lack of awareness about ML and TF risks by the agent –but to also ensure that other parties involved in the delivery of AML and CTF compliance activities are covered. The amendment requires that both relevant employees **AND any agents whose work involves;**

- Contributing to the identification or mitigation of the risk of money laundering and terrorist financing for the relevant business, or
- Prevention or detection of money laundering and terrorist financing in relation to the relevant person’s business.

Are:

- (i) Made aware of the law relating to money laundering and terrorist financing, and to the requirements of data protection, which are relevant to the implementation of these Regulations; and
- (ii) Regularly given training in how to recognise and deal with transactions and other activities or situations which may be related to money laundering or terrorist financing.

Depending on how broadly the term “agent” is applied, this may require that financial institutions verify how their agents ensure that their staff who work in the areas above are appropriately trained and also how they determine whether that training was effective.

#### Key Changes

- Relevant persons to ensure that agents undertaking KYC and CDD for them are trained in compliance with the MLRs.

#### What to do?

- Identify existing agents who may undertake or provide KYC and CDD support.
- Seek information on training provided or undertaken by agents and assess degree of compliance with new training requirements
- Adopt processes to ensure ongoing engagement with agents to verify appropriateness and effectiveness of training provided to or undertaken by agents and their staff.

## 4) Regulation 27(8) KYC and Existing Customers - It's a Taxing Matter

---

When the US FATCA regime was first introduced several years ago, the question of whether its KYC requirements could also be incorporated into existing AML KYC processes was explored by several institutions, although many maintained separate KYC processes for each of these requirements.

Fast forward to 2020, and the MLRs now expressly require that one of the triggers for reviewing existing customer KYC and CDD includes when a financial institution is required to “reach out” to a customer as part of the collection, validation/reason to doubt and reporting of tax residency information, including ongoing monitoring of changes in circumstances that impact on the tax residency information.

Additions to this same regulation also expand KYC and CDD requirements for existing customers requiring a review where any additional information is received as a part of ongoing monitoring, adverse media checks or other information that suggests a change in ownership or control. Expect regulatory onsite visits to involve greater scrutiny of the review of existing customer files and the application of these new triggering requirements.

### Key Changes

- “Reach out” provisions on existing customers extended to ensure that new information on beneficial ownership is obtained on a more frequent basis
- Obtaining KYC information to comply with CRS/FATCA related regulations will also trigger a review of existing customer KYC information.

### What to do?

- Revisit existing KYC procedures to ensure that amended review requirements are included are part of existing processes and practices.
- Assess extent to which current operations allow for AML and Tax KYC processes to coincide and read across required KYC data to trigger required reviews.

## 5) Regulation 28 – Customer Due Diligence Measures

---

There's been a small update to this regulation that is not likely to pose a huge change for most institutions. The addition of a paragraph that expressly states that relevant persons “must take reasonable measures to understand the ownership and control structure of that legal person, trust, company, foundation or similar legal arrangement” is unlikely to catch-out many institutions who have been required to comply with the MLRs for some time now. This also applies to the amendment made in 28(8) about what to do when a beneficial owner of a legal entity can't be identified.

Nonetheless, institutions should ensure that a “health check” is performed internally to verify that their policies and procedures reflect in their wording an acknowledgement of this requirement. This will be particularly relevant where reliance has been placed on powers of attorney, authorised signatory lists etc.

### Key Changes

- Relevant persons expressly required to take reasonable measures to understand the ownership and control structure of legal entities and legal arrangements.

### What to do?

- Undertake “health check” review of existing KYC related procedures and processes to verify that this requirement is expressly incorporated into customer onboarding and ongoing review activities.

## 6) Regulation 28(19) - eKYC Has Finally Arrived!

---

For those of you who know me, I've been talking about eKYC for the last three years or so and am thrilled to see it finally transposed into the MLRs. Here in the UK, this is the Gov ID programme – if you file your own tax returns online, you'll have had your identification set up with one of approved providers of this programme.

In addition to extending the use of eKYC established under this programme. eKYC made available by private vendors can also be used. One interesting variation between the 5AMLD wording and the MLRs, is that the latter has not included the 5AMLD wording that any such providers as are “regulated, recognised, approved or accepted by the relevant national authorities”.

Watch this space to see whether this is elaborated upon in the revised JMLSG Guidance expected in February.

### Key Changes

- eKYC may be used as part of KYC processes, provided it is independent of the person whose identity is being verified; secure from fraud and misuse; and capable of providing assurance that the person being identified is in fact that individual.
- UK government does not anticipate regulating eKYC providers.

### What to do?

- In combination with Regulation 19(4), verify whether eKYC projects or activities (whether fully implemented or being considered) satisfy control requirements and the process used to assure these remain effective throughout the use of eKYC.

## 7) Regulation 33 – High Risk Third Countries

---

The 5AMLD Article 18a was the subject of debate and as most are aware, much disagreement, especially in terms of the “list” of third countries (what I called ‘bad AML list’) and the process for adding jurisdictions to it.

The MLRs has added an interesting amendment. It provides that when dealing with a transaction involving a high risk third country, **where EITHER OF THE PARTIES to the transaction is established in a high-risk third country**, enhanced due diligence measures should be applied New 33(3A)).

A small revision, but potentially a significant one for those institutions who have not already incorporated the monitoring of both senders and recipients into existing transaction monitoring programmes.

Helpfully, the MLRs amendments also clarify that an individual should not be treated as de facto high risk simply because they were born in a high-risk country. There must be evidence to show that they are an actual resident in that jurisdiction. The amendment also makes it clear that the term “established” in terms of legal entities, refers to a customer have its principal place of business or its principal regulatory authority (for a financial institution).

### Key Changes

- Expands EDD measures in relation to transactions to parties at each end of the process (sender and recipient)
- Clarifies that place of birth alone should not be used as grounds to classify an individual as high risk
- Clarifies that requirement covers jurisdiction where the principal place of business of a legal entity is located.

### What to do?

- Assess existing transaction monitoring process and customer payment instruction activities and consider how to incorporate new EDD requirements.
- Revisit existing KYC procedures to ensure that clarifications provided concerning establishment and place of birth for customers are reflected in their requirements.

## 8) Next Steps

---

We're anticipating the revised JMLSG Guidance that will support and clarify the application of these amendments will be released in February but until then, there's no time like the present to start reviewing existing KYC policies, procedures and processes.

### What to do?

- Develop a plan of attack! Consider how to best review and evaluate existing processes and operations to verify (a) what needs updating and (b) what might be missing, in order to comply with the MLR amendments.
- Identify and assess changes that will be needed to KYC and CDD processes, and in particular, how to address the changes to the review triggers in relation to existing customer KYC.
- Evaluate how to "bake-in" AML and TF risk assessments in relation to the broader scope of business activities, including the selection and retention of agents providing specialised anti-financial crime related services.

## Appendix – Extract Table of Amendments

Regulation	Subject	Nature of Change
8	<b>Entities Required to Comply with MLRs</b>	<p>Addition of letting agents, art market participants, crypto exchange and wallet providers; description of letting activities covered by or excluded from the MLRs are described in Regulation 13(3)-(7)</p> <p>Description of art market activities covered by Regulation 14(1); includes those involved in the operation of freeports.</p> <p>Description of crypto asset exchange and wallet providers covered by new Regulation 14A (collectively, <b>VASPs</b>). Added throughout rest of MLRs re: regulatory requirements.</p>
9	<b>Carrying on Business in the UK</b>	<p>Revises definition to reflect incoming changes post departure from the EU – which entities must comply with the MLRs due to carrying on business in the UK by removing reference to single market directive and EEA passport rights</p>
11d	<b>Regulated Activities - Tax</b>	<p>Expanded from advice about tax affairs to material aid, or assistance or advice in connection with the tax affairs of other persons, whether provided directly or through a third party.</p>
19	<b>Policies, Procedures and Controls</b>	<p>19(4) clarification that transactions that require identification and scrutiny those that that are complex <b>or</b> unusually large – corrects description that transactions subject to this requirement must be complex <b>AND</b> unusually large.</p> <p>19(4)(c ) clarification that requirement for policies, controls and procedures in relation to assessing the ML and TF risks associated with the introduction and use of new technology is clarified as encompassing “<b>new products, new business practices (including new delivery mechanisms) or new technology</b>”.</p>

24	<b>Training - Agents</b>	<p>24(1) Extends obligation to any agents the relevant person uses for the purposes of its business whose work is:</p> <p>(a) Relevant to the relevant person’s compliance with any requirement in the MLRs, or</p> <p>(b) Otherwise capable of contributing to the—</p> <p>(i) Identification or mitigation of the risk of money laundering and terrorist financing to which the relevant person’s business is subject; or</p> <p>(ii) Prevention or detection of money laundering and terrorist financing in relation to the relevant person’s business.</p>
27	<b>Customer Due Diligence Measures</b>	<p>Expands circumstances when CDD measures must be applied to existing customers</p> <p><b>27(8) – NEW</b></p> <p>(za) When relevant person has a legal duty in the course of the calendar year to contact an existing customer for the purpose of reviewing any information which:</p> <p>i. Is relevant to the risk assessment for that customer and</p> <p>ii. Relates to the beneficial ownership information necessary to understand the ownership or control structure of a customer who is a legal entity or legal arrangement.</p> <p>(zb) When the relevant person must contact an existing customer in order to fulfil any duty under the International Tax Compliance Regulations 2015</p>

28	<b>Customer Due Diligence Measures</b>	<p>Addition of new paragraph to make it UBO identification and understanding the ownership/control structure of legal entities and arrangements.</p> <p><b>28(3A) - NEW</b></p> <p>“Where the customer is a legal person, trust, company, foundation or similar legal arrangement the relevant person must take reasonable measures to understand the ownership and control structure of that legal person, trust, company, foundation or similar legal arrangement”.</p>
28	<b>Customer Due Diligence Measures</b>	<p>Transposition of 5AMLD requirement that if UBO cannot be satisfactorily identified for a legal entity or arrangement.</p> <p>8. ...the relevant person must—</p> <p>(a) Keep records in writing of all the actions it has taken to identify the beneficial owner of the body corporate;</p> <p>(b) <b>Take reasonable measures to verify the identity of the senior person in the body corporate responsible for managing it</b>, and keep records in writing of—</p> <p>(i) All the actions the relevant person has taken in doing so, and</p> <p>(ii) Any difficulties the relevant person has encountered in doing so.”</p>
28	<b>Customer Due Diligence Measures</b>	<p>Transposition of 5AMLD requirement permitting reliance on eKYC, including Gov.ID or similarly recognised government identification authorised under the eIDAS Regulation of Europe.</p> <p><b>28(19) - NEW</b></p> <p>For the purposes of this regulation, information may be regarded as obtained from a reliable source which is independent of the person whose identity is being verified where—</p>

		<p>(a) It is obtained by means of an electronic identification process, including by using electronic identification means or by using a trust service (within the meanings of those terms in Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23rd July 2014 on electronic identification and trust services for electronic transactions in the internal market(11)); and</p> <p>(b) That process is secure from fraud and misuse and capable of providing an appropriate level of assurance that the person claiming a identity is in fact the person with that identity.</p>
30	<b>Registers</b>	<p>New requirement to report discrepancies in registers – see separate note posted on EFI website.  <a href="https://efilimited.com/news-and-insights/">https://efilimited.com/news-and-insights/</a></p>

<p>33</p>	<p><b>Duty to Apply Enhanced Due Diligence</b></p>	<p>Amendment to expand the application of EDD in relation to transactions involving high risk third countries.</p> <p>..."in any business relationship with a person established in a high-risk third country <b>or in relation to any relevant transaction where EITHER OF THE PARTIES to the transaction is established in a high-risk third country</b>".</p> <p>Revisions include terms which are defined as:</p> <p>(a) A <b>"high-risk third country"</b> means a country which has been identified by the European Commission on its High Risk Third Country List adopted under Article 9.2 of the 4AMLD;</p> <p>(b) A <b>"relevant transaction"</b> means a transaction where CDD must be applied under Regulation 27;</p> <p>(c) Being <b>"established in"</b> a country means—</p> <p>(i) In the case of a <b>legal person</b>, being <b>incorporated in or having its principal place of business in that country</b>, or, in the case of a <b>financial or credit institution</b>, having its <b>principal regulatory authority in that country</b>; and</p> <p>(ii) In the case of an <b>individual</b>, being <b>resident in that country</b>, but <b>not merely having been born</b> in that country</p>
<p>33</p>	<p><b>Duty to Apply Enhanced Due Diligence</b></p>	<p><b>33(3A) – Revised</b></p> <p>EDD in relation to <b>connections to high risk third countries</b> must include:</p> <p>(a) Obtaining <b>additional information</b> on the <b>customer</b> and on the customer's <b>beneficial owner</b>;</p> <p>(b) Obtaining additional information on the <b>intended nature of the business relationship</b>;</p> <p>(c) Obtaining information on the <b>source of funds</b> and <b>source of wealth</b> of the customer and of the customer's beneficial owner;</p>

		<p>(d) Obtaining information on the <b>reasons for the transactions</b>;</p> <p>(e) Obtaining the approval of senior management for establishing or continuing the business relationship;</p> <p>(f) Conducting enhanced monitoring of the business relationship by increasing the number and timing of controls applied and selecting patterns of transactions that need further examination.</p>
--	--	--