



A HooYu compliance guide to the CDD elements of the:

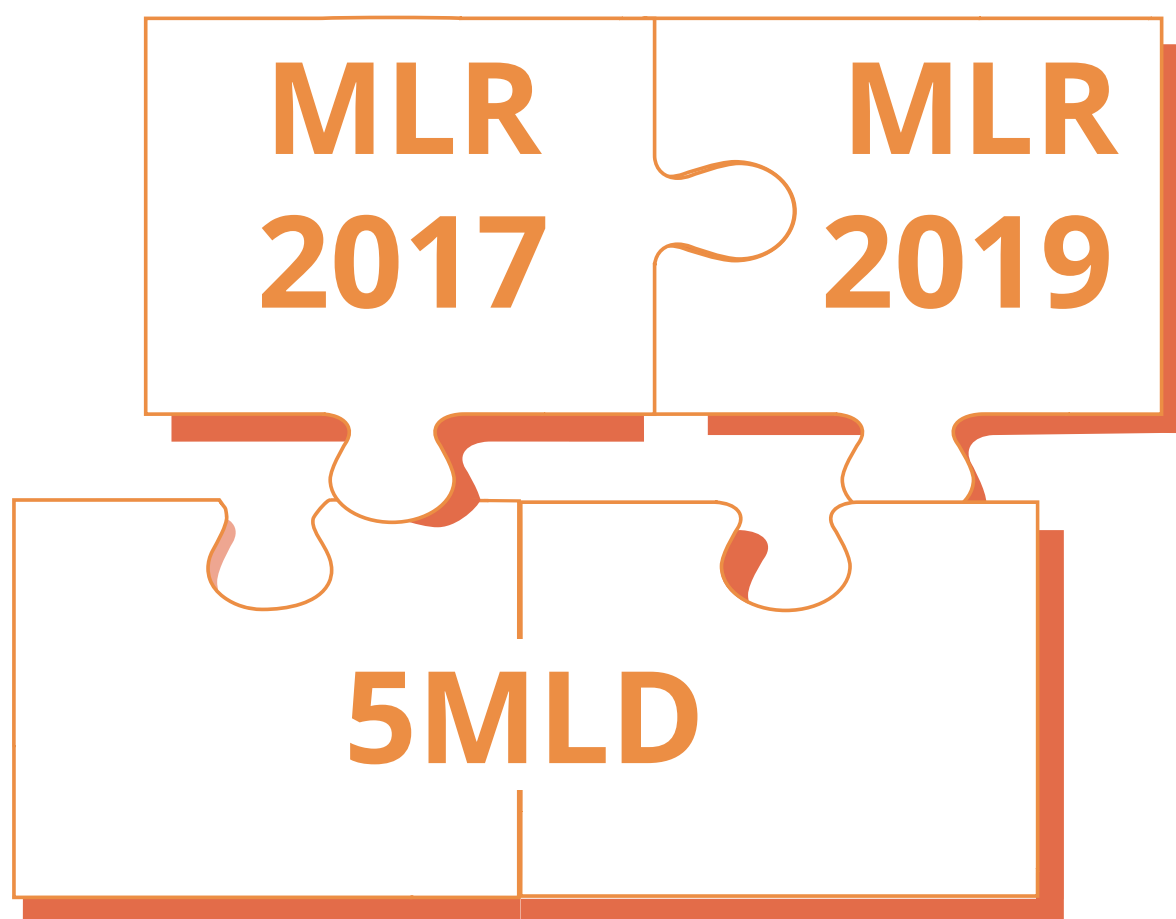
THE MONEY LAUNDERING AND TERRORIST FINANCING (AMENDMENT) REGULATIONS 2019



New Anti-money Laundering regulation - what's happened?

The UK government published new legislation on 20th December 2019, the Money Laundering and Terrorist Financing (Amendment) Regulations 2019 (MLR19).

These regulations transpose the 5th Money Laundering Directive (5MLD) into national law and update the earlier 2017 UK regulation, The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017. (MLR17)



As such, MLR19 updates and inserts new sections into MLR17. As experts in Customer Due Diligence (CDD) and customer onboarding, HooYu has produced this compliance guide to explain the new CDD requirements as laid down in the combined MLR17 & MLR19 regulations.

The main concepts of CDD regulation

The MLR19 updates MLR17 so as such, MLR19 can't be read as a complete Regulation in isolation, the two need to be read together. Here's a quick reminder of the main principles of CDD regulation as laid down in MLR17:

1. Identification & verification

A common misconception when it comes to CDD is that obtaining name, address and date of birth information constitutes CDD. Coming to know the identity of a customer is only deemed to be identification of the customer. A regulated entity then has to verify the identity of the customer by checking identity data against a database or by authenticating government issued ID documentation.



2. The Risk-Based Approach

Based on risk rating factors such as product, geography, velocity, value, change in customer details and any other factor deemed relevant, regulated firms must take a risk-based approach to CDD.



3. When does CDD have to take place?

Before the establishment of a customer relationship - the customer, any person purporting to act on behalf of the customer and any beneficial owner of the customer must undergo CDD before the start of a business relationship or the carrying out of the transaction. During the relationship - customers and beneficial owners must be re-verified on an ongoing basis on a Risk-Based Approach.



STATUTORY INSTRUMENTS
2017 No. 692
FINANCIAL SERVICES
The Money Laundering, Terrorist Financing and
(Information on the Payer) Regulations 2017

So what's new in MLR19?



Brings cryptocurrency into scope for CDD



Clarification of CDD requirements for sectors that have not embraced CDD under MLR17



Reduction of threshold to conduct CDD on electronic money products



Acceptable methods to conduct CDD



Extends focus on high-risk third countries



Brings cryptocurrency into scope for CDD

MLR19 provides a definition of cryptoasset exchange providers and custodian wallet providers, and mandates these entities as regulated businesses for CDD.

Cryptoasset exchange providers

- a) exchanging, or arranging or making arrangements with a view to the exchange of, cryptoassets for money or money for cryptoassets,*
- b) exchanging, or arranging or making arrangements with a view to the exchange of, one cryptoasset for another, or*
- c) operating a machine which utilises automated processes to exchange cryptoassets for money or money for cryptoassets.*

Custodian wallet providers

Provides services to safeguard, or to safeguard and administer—

- (a) cryptoassets on behalf of its customers, or*
- (b) private cryptographic keys on behalf of its customers in order to hold, store and transfer cryptoassets,*

14A



Clarification of CDD requirements for sectors that have not embraced CDD under MLR17

Following HMRC fines on businesses that have been slow to comply with CDD requirements¹, MLR19 provides further scope and detail for several sectors.

Estate agents & letting agents

Estate & letting agents are now tasked to conduct CDD on both the renter and the landlord for high-value rentals where the rent is greater than £10k per month.

The letting agent must apply customer due diligence measures...in relation to both the person by whom the land is being let, and the person who is renting the land.

7A

Art market participants

High value dealers (art and motor) were called into scope under MLR17 but MLR19 brings greater detail to when CDD is in scope.

An art market participant must also apply customer due diligence measures (a) in relation to any trade in a work of art...when the firm or sole practitioner carries out, or acts in respect of, any such transaction, or series of linked transactions, whose value amounts to 10,000 euros or more; (b) in relation to the storage of a work of art (within the meaning given in regulation 14), when it is the operator of a freeport and the value of the works of art so stored for a person, or series of linked persons, amounts to 10,000 euros or more.

Tax advisers

The detail of which tax advisory services are in scope is clarified to help ensure that tax advisors realise which of their business activities fall into CDD scope.

“material aid, or assistance or advice, in connection with the tax affairs of other persons, whether provided directly or through a third party”.

4-2

¹<https://www.gov.uk/government/publications/businesses-not-complying-with-money-laundering-regulations-in-2018-to-2019/current-list-of-businesses-that-have-not-complied-with-the-2017-money-laundering-regulations>



Reduction of threshold to conduct CDD on electronic money products

There is a reduction in the value threshold at which CDD must be implemented. Under MLR17, the threshold was €250 and under MLR19 is now €150, irrespective of whether the e-money instrument can only be used in the UK or globally.

The maximum amount which can be stored electronically is 150 euros, or (if the amount stored can only be used in the United Kingdom), 150 euros;

The implementation for this element of MLR19 is delayed until 10th July 2020.

(3) Regulation 5(5)(c) (amendment of Part 3: customer due diligence: anonymous prepaid cards) comes into force on 10th July 2020.

MLR19 recruits acquiring PSPs to the CDD cause

PSP's now need to be sure that they are not processing payments via e-money instruments that do not conduct CDD on customer accounts.

Credit institutions and financial institutions, acting as acquirers for payment using an anonymous prepaid card issued in a third country, shall only accept payment where —

- (a) the anonymous prepaid card is subject to requirements in national legislation having an equivalent effect to those laid down in this regulation; and*
- (b) the anonymous prepaid card satisfies those requirements.*



Acceptable methods to conduct CDD

MLR19 states that existing CDD methods such as “using documents or information in either case obtained from a reliable source” are still permitted.

1. “verify” means verify on the basis of documents or information in either case obtained from a reliable source which is independent of the person whose identity is being verified;

2. (b) documents issued or made available by an official body are to be regarded as being independent of a person even if they are provided or made available to the relevant person by or on behalf of that person.

MLR19 also refers to eIDAS and trust providers as a suitable means of CDD
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—

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—

(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

(b) that process is secure from fraud and misuse and capable of providing an appropriate level of assurance that the person claiming a particular identity is in fact the person with that identity.

The inclusion of eIDAS schemes as a suitable means of CDD follows on from a 2016 EU Regulation “Electronic Identification and Trust Services” that considers how harmonised identity verification processes can contribute towards the building of a single digital market. The end goal is that governments issue an eID that is backed by a government ID database that can be queried to confirm identity information and that national EIDs will be recognised equally in all Member States.



Extends EDD focus on high-risk third countries

Under MLR17 EDD (Enhanced Due Diligence) was called for:

“in any business relationship or transaction with a person established in a high-risk third country;”

Under MLR19, EDD has to be applied to both parties to the transaction in a high-risk country.

“any relevant transaction where either of the parties to the transaction is established in a high-risk third country”;

For a list of high-risk third countries, please see [definition from European Commission](#)

MLR19 also prescribes a list of EDD measures to be taken when transacting with high-risk third countries.

The enhanced due diligence measures taken by a relevant person for the purpose of paragraph (1)(b) must include—

- (a) obtaining additional information on the customer and on the customer’s beneficial owner;*
- (b) obtaining additional information on the intended nature of the business relationship;*
- (c) obtaining information on the source of funds and source of wealth of the customer and of the customer’s beneficial owner;*
- (d) obtaining information on the reasons for the transactions;*
- (e) obtaining the approval of senior management for establishing or continuing the business relationship;*
- (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.”;*

How HooYu helps achieve compliance with the AML Regulations

HooYu offers a multi-stage verification process that can be configured according to your customer, product, geography and other customer risk parameters.

Step One: Plan your Customer Due Diligence steps with HooYu.

For example:

- UK domiciled - confirm identity with the HooYu UK Data Service
- Non-UK domiciled – confirm identity with the HooYu digital KYC journey
- On a Risk-Based Approach - check data-bases and verify an ID document

Risk Based Analysis to inform CDD

Transaction Size

Product Risk

Geography

Step Two: Check customer identity against the HooYu UK Data service.

Positive data

Includes positive data sources such as Credit Reference Agency identity databases, Electoral Roll and Directors and Shareholders Data.



Negative data

Includes negative data sources such as Deceased and PEP's & Sanctions.



Fraud data sources

Includes fraud alert data sources such as Forwarding Address Warnings.



UK Data Service






HooYu delivers a comprehensive report to indicate the number of name/address/date of birth matches with a granular audit of which databases have been matched to customer data.



- Name
- Address
- Date of Birth

Step Three: Where database check results yield a thin match, trigger the HooYu digital KYC journey.

The customer takes a selfie with their mobile or web cam, shares their social media or online account details and takes a picture of their ID document and proof of address document.

-  ID document authentication against document security features.
-  Proof of Address checks customer name & address match against utility bill or bank statement.
-  Facial biometric comparison from selfie to ID document photo.
-  Digital footprint analysis and profile verification.
-  PEPs & Sanctions checks and adverse media checks.



Step Four: HooYu returns results back to the regulated firm's CRM system.



- ✓✓✓ **NAME** 98%
- ✓✓ **ADDRESS** 100%
- ✓✓✓ **DATE OF BIRTH** 100%
- ✓✓ **BIOMETRIC** 87%
- ✓✓✓ **PASSPORT** 100%
- ✓✓✓ **DRIVING LICENCE** 100%
- ✓✓ **NATIONAL ID** 87%

The HooYu digital KYC journey maximises customer onboarding success rates:

- 🛡 Examines the sources used to provide a Pass or a Fail decision to indicate if the customer has provided the relevant pieces of identity information.
- 🛡 Generates an identity confirmation report showing how many sources have been used to confirm customer identity attributes so you can confidently transact with your customer.
- 🛡 Cross-references, matches and scores identity attributes against each other to drive an overall identity confirmation score to help manage fraud risk.



“HooYu helps us not just to comply with money laundering regulations but also helps us to curate a great digital journey that makes for easy and convenient account opening.”



“easyMoney aims to make financial services products accessible as possible by making sure we can onboard customers as easily as possible with minimal friction, HooYu Identify enables us to do this.”



“By adding HooYu to our KYC tools, we can improve some of our higher risk customer processes and can now facilitate customer requests without asking the customer to post in copies of documentation”

If you want to know more about your CDD compliance requirements under MLR19 and how HooYu can help you comply please email:

david.pope@hooyu.com

