



OCR Labs®

# The Light of New EU AML Regulations is Drawing Near

An Insight into the 2021 Proposed European Union Anti-Money  
Laundering and Countering the Financing of Terrorism Rulebook  
through an Identification Verification Lens

This document is strictly private, confidential and personal to its recipients and should not be copied, distributed or reproduced in whole or in part, nor passed to any third party without the express permission of OCR Labs.

## **The EU's new anti-money laundering (AML) package was released in July 2021.**

These far-reaching proposals, which include a Regulation on AML/CFT and the 6th AML Directive (AML6D), will have a geographic impact that will extend across the EU, UK and to third-party countries. The impact will also reach industries ranging from the “traditional” financial institutions to gaming, crypto, real estate, and more. And with a periodic open review process to define the offenses to be focused on by the governing authorities, this initiative will be a continuing work-in-process that constitutes the biggest ever overhaul to the EU's AML regime.

The proposals are a facelift to the existing regime with the introduction of new rules, updates and enhancements of the current requirements. The novel approach to supervision will be one of the biggest changes, with the establishment of a new AML Authority (AMLA) and an EU-wide Financial Intelligence Unit (FIU) to act as a coordination and support mechanism sitting over EU member states. This will align the current differences of approach to supervision.

Another fundamental shift is the potential for the current AML risk-based approach to move towards harmonized AML rules. To some extent, that risk approach permitted inconsistencies that promoted regulatory shopping between jurisdictions. Guidance from AMLA about the extent to which firms can and should apply the rules would be beneficial within the EU and to countries outside of the EU that are engaged in the web of global money movement.

From a timing perspective, AMLA is staffing up in 2023, with general activities expected to launch in 2024 and 2025, a heartbeat in time from our doorstep. It is in this context that we highlight below some key points that arise from the new package that firms should be engaging on to consider how these revisions could impact their current AML/CFT approach.



## Harmonization of AML Definition

AML6D harmonizes the definition of money laundering across the EU with the goal of removing loopholes in the domestic legislation of member states. The directive provides more detail than the subsumed 5th AML Directive, in response to changing criminal methodologies and legislative priorities. It includes a list of the 22 “predicate offenses” that constitute money laundering. (Predicate offenses refer to subsets of crime that constitute a larger crime of AML/CFT).

The list includes certain tax crimes, environmental crime, cyber-crime and fraud money laundering. The inclusion of cyber-crime as a predicate offense is significant since it is the first time it has been featured in this context in an EU money laundering directive. The inclusion of fraud is also of particular importance.

***This implies that a fraud, for example in the context of gambling onboarding or reverification required for cashing out a player’s account, could be swept into the EU AML umbrella, with the host of consequences to follow that are summarized in part in this paper.***

When the list of predicate offenses comes into legal effect, firms within member states will have to ensure that their AML/CFT programs can deal with the new risk environment that is created. As it relates to the writer, this means strengthening the identity verification and document fraud analysis tools in the KYC toolbox.

## Expanded Regulatory Scope

AML6D expands the number of offenses that fall under the definition of money laundering. For example, “aiding and abetting” will also constitute money laundering and be subject to the same criminal penalties. Previously, EU money laundering regulations punished only those who profited directly from the act of money laundering. Under the new directive, “enablers” will also be legally culpable.

## Extension of Criminal Liability

Under the current EU AML rules, only individuals can be punished for the act of money laundering. AML6D will extend criminal liability to allow for the punishment of legal persons, such as companies or partnerships. The new rules mean that a legal person will be considered culpable for the crime of money laundering if it is deemed by AMLA that they failed to prevent a “directing mind” from within the company from carrying out the illegal activity. Practically, the new rules will place AML/CFT responsibility on management employees along with employees acting separately.

This extension of criminal liability is intended to hold larger companies to account in the global effort to combat money laundering. The move will allow authorities to better target organizations that do not implement AML/CFT effectively. Punishments for legal persons may range from a temporary ban on operations or judicial supervision to permanent closure.

## A Bigger Stick

As with most regulations that seek to alter behavior, AML6D will bring with it tougher enforcement measures. It introduces a minimum prison sentence of four years for money laundering offenses (previously one year). Also, judges will have the power to fine individuals and exclude entities from accessing public funding.

The increased prison terms for money laundering and potential financial repercussions are part of the EU's effort to bring consistency to AML/CFT regulation across all member states and stricter enforcement of money laundering rules.

AMLA will also have the authority to issue guidance to and conduct investigations of selected "obliged entities" (defined below) and to impose fines for breaches of money laundering or countering the financing of terrorism (CFT) rules. Fines can be up to €10m or 10% of annual turnover, depending on the nature of the breach, and further fines can be imposed for each day a breach is not remedied.



## A Single Rulebook

Arguably the largest and most impactful of the proposals is the proposal for a single rulebook on AML/CFT. Key areas of change here include:

### Increased scope of obliged entities:

The Regulation proposes to include new types of firms in the scope of the AML/CFT rules including creditors for mortgage and consumer credits, and associated intermediaries; unregulated crowdfunding service providers; and investment migration operators.

In addition, there has been an amendment to the scope for persons storing, trading or acting as intermediaries in the trade of works of art, and an expansion of the scope for crypto asset firms (more on crypto below).

### Roles and responsibilities:

There are new requirements around the appointment by a firm of a compliance manager, with specific tasks and duties, including responsibility for implementing policies, controls and procedures. This officer will also be responsible for reporting significant weaknesses to the board of directors.

While many firms currently have these responsibilities split across teams and individuals, the new rules will bring a change in roles and responsibilities and may require adjustment of staffing and resources. Firms could be challenged to demonstrate that these areas of activity are adequately resourced, in particular if faced with any adverse control effectiveness findings.

### Customer due diligence (CDD) measures:

The Regulation explicitly sets out the specific information and documentation to be obtained as part of identification and verification for natural persons, legal entities and trusts, providing much greater detail than at present. It also highlights when CDD is required. As examples:

*“Obligated entities” must apply CDD steps when establishing a business relationship; when involved in or carrying out an occasional transaction that amounts to €10,000 or more (in a single or linked transactions); when there is a suspicion of money laundering or terrorist financing (no exemptions or thresholds apply here); or when there are doubts about the veracity or adequacy of previously obtained customer data.*

***Gambling operators must apply CDD on the collection of winnings, the wagering of a stake, or both, when carrying out transactions of at least €2,000 (in a single or linked transactions).***

Of note is that the threshold for applying CDD measures for occasional transactions is reduced from €15,000 to €10,000, which will place added CDD requirements on firms.

Firms may already be collecting information and verification documents during onboarding. But they should perform a gap assessment against procedures relating to the management of both identity verification and supporting documentation collection and storage to ensure they are doing so to the extent laid out in the Regulation.

There is also a new requirement for firms to obtain information on the source and destination of funds, as well as the estimated amount and economic rationale of contemplated trades or actions. Under the 4th AML Directive, source of funds (SOF) is a specific requirement only for politically exposed persons (PEP) relationships. AML6D will to some extent standardize the different approaches around asking for destination of funds, estimated amounts or economic rationale.

Of interest is the new ongoing monitoring requirement. This mandates firms to update customer information at least every five years. This will create uniformity of approach, because currently some firms have higher review frequencies; others follow event-driven reviews as an option; and low-risk customers review only on a new account / initial transaction basis and are not subject to periodic review requirements.

### **Enhanced due diligence (EDD).**

The EU's high-risk third country (HRTC) list, prepared with the assistance of the Financial Action Task Force (FATF), is limited presently to countries with "strategic deficiencies." Under the new AMLA requirements, this HRTC list is to be expanded by identifying (i) countries with AML/CFT "compliance weaknesses" and (ii) countries "posing a threat to the Union's financial system." EDD measures are required in both cases. This means that certain firms may have to prepare for more of their client base to require automatic EDD.

### **Outsourcing.**

The Regulation clarifies that firms may outsource tasks deriving from CDD only. There are some tasks however that are precluded from outsourcing, including the development, and drawing up of internal policies, controls and procedures and the approval of the risk assessment of customers' risk profiles.

### **Reporting obligations.**

The new Regulations include significant detail that will standardize obligations for submitting suspicious activity reports (SARs) or suspicious transaction reports (STRs) - currently defined by member states in national legislation. Firms are required to respond to FIU requests for information (relating to SARs or STRs) within five days, or even on shorter 24 hours' notice. This condensed time frame could cause bottlenecks in the reporting process, especially for large firms that file large volumes of reports.



***Notable is that firms cannot execute a transaction for a customer which is deemed to be suspicious until a SAR or STR is filed with the FIU, and any further FIU instructions have been followed.***

So firms would have to hold off on processing transactions deemed suspicious until they receive consent from the FIU.

This deal flow management will be a new challenge for certain firms. They will have to build this new requirement into their systems, with the added balance of how to pause transactions while waiting for consent from the FIU, including without letting on to the customer that an investigation may be in motion.

## **The New Officer on the Block**

AMLA is newly placed at the heart of supervision of the new AML/CTF regulations and central to the FIU support mechanism, with AML6D providing the teeth of enforcement.

The transition of power from the European Central Bank (ECB) and the European Banking Authority (EBA) to AMLA will bring with it more formal enforcement powers, experience outside of the banking sector, and improved governance structures. It will also result in a larger enforcement team, from the current size of approximately 10 EBA people to the planned 250 for AMLA.

Following implementation of the new EU AML rulebook, AMLA will directly supervise the highest-risk financial institutions (“obliged entities”) with a presence in multiple EU jurisdictions with teams led by AMLA and including employees of national supervisory authorities. Financial institutions that are not obliged entities and all non-financial institutions which are subject to the new AML rulebook will be indirectly supervised by AMLA through AMLA’s coordination of national supervisors, with the power to set supervisory standards. AMLA also has intervention rights over national supervisors where it holds a position that the local supervisory regime is not effectively enforcing AML rules.

***The realization of a single, independent, superior, and well-resourced EU supervisor will bring with it consistency and an improvement of standards across the region.***

It is expected to most affect:

**Firms with a substantial presence across the EU and higher money laundering risk.**

These entities should expect direct supervision by AMLA.

**Firms in member states with weaker AML/CFT enforcement systems.**

These entities should experience material changes to their local AML/CFT regimes as regulatory and supervisory standards are elevated. Direct supervision by AMLA is a possibility.

**Non-financial sector firms who traditionally have been subject to limited AML/CFT supervision.**

For example, in gambling, crypto and real estate. They will be subject to enforcement by national regulators overseen by AMLA.

## FIU Coordination

As mentioned above, AMLA will provide a support and cooperation mechanism for FIUs. Amongst their responsibilities as a coordination hub, AMLA will establish standardized reporting and provide specialized training and assistance to FIUs as well as to obliged entities. These changes should provide much-needed clarity for firms on FIU expectations and will help them streamline their own operations when reporting to multiple law enforcement authorities.

On an international level, there will be increased cooperation and communication between EU FIUs around best practices, including sharing expertise and coordinating threat and risk assessments. This could extend to third party country FIUs too.

***It is conceivable that this will reinforce a tale of two worlds, where the EU maintains a power block of EU regulation with an open exchange of information and cooperation with like-minded third-party countries and separated from countries taking a less strong approach.***

Continuing from current practice, AML6D requires the establishment of centralized automated mechanisms to allow FIUs immediate access to raw identity information of payment and bank account holders. These mechanisms will be interconnected through a single access point bank account register, which will be open to all member states.

FIU related changes will improve the challenges of information exchanges across national borders. There will be a greater data burden on firms, however, to ensure that data submitted through the centralized mechanisms and delivered to FIUs is accurate and of high quality.



## Crypto Transfers

***There is a sharp increase in identification verification requirements for transfers of crypto-assets for the purpose of ensuring effective and full traceability of crypto transfers.***

Identifiable information must be held on the originator (for example name, address and place and date of birth) and the beneficiary (name and account number) of the transfer. Also, the crypto asset service providers (CASP) of the originator must verify the accuracy of the information on the originator using an independent reliable source before executing the transfer. The CASP will not be able to execute any transfer of crypto assets until this information is obtained.

For transfers exceeding €1,000 (either single or linked), the CASP of the beneficiary must verify the accuracy of the beneficiary's information using an independent reliable source, before the crypto-assets can be made available to the beneficiary. For transfer values below €1,000, the CASP must verify beneficiary information when payment is made in cash, via anonymous electronic money, or where the CASP has reasonable grounds to suspect an act of money laundering or terrorist financing.

Also, payment service providers (PSPs) established in the EU and involved in sending or receiving crypto-assets will have to collect information on the originator and beneficiary of a transaction and verify this information using independent sources.

These above changes should be relatively easy for firms to implement given that this has been covered in previous EU Directives. That said, there will be heightened attention by AMLA on cyber firms given the increased regulatory attention that the sector has recently attracted.





## In Closing

The brighter EU AML light carried through the implementation of the new regulations will shine on many businesses that stood in the shadows of regulation. This will include industry verticals such as cyber, payment processors, gambling, and real estate (beyond just financial institutions). So too will broader AML crime definitions, notably fraud, widen the net of capture.

AMLA will be incentivized to display its worth, part of this through a heavy enforcement hand that will demand high financial penalties. For those firms that are happy to verify a new client using a photocopy of an identification document that is cut in half, consider that your name may be the focus of this AMLA flashlight.

### **Terry Brenner,**

*OCR Labs Global*

*Head of Legal, Risk & Compliance, North America*

## About OCR Labs

OCR Labs Global helps you quickly scale your business globally. Our fully-automated solution verifies new users in seconds with just their face and smartphone - in over 220 countries and territories with any ID document - without the burden of human intervention.

We empower true identity for people around the world. Through our Zero Bias AI™ technology, we are pioneering the use of generative AI to train deep neural network systems to protect against discrimination on the basis of race, age and gender. We are the first company to achieve 99.99% accuracy in independent lab testing.

Our advancements in Natural Vision Processing (NVP) are enabling machines to autonomously see and perceive as humans and excel in ways that humans cannot.

OCR Labs Global is trusted by startups, governments, and global enterprises, including HSBC, Vodafone, BMW, Virgin Money, and ANZ, for borderless and inclusive identity verification. Founded in Australia in 2018, OCR Labs Global is a Series B venture-backed company with headquarters in London and offices in North America, Asia and Europe.

**For more information, visit [ocrlabs.com](https://ocrlabs.com)**