

EU Commission AML/CFT legislative package

Adan's position

October 2021

Introduction

Adan (Association for the Development of Crypto-Assets) is a non-profit bringing together and representing crypto-assets and blockchain professionals in France and Europe. Adan's members cover a wide range of activities: crypto-asset markets, custody, payments, investment management, blockchain analysis tools, support for crypto/blockchain projects, IT security, etc. Adan's mission is to promote the development of the crypto-assets industry in favour of a new digital economy.

Adan is thankful to the European Commission for allowing the expression of industry players thanks to this consultation. The Association's objectives are to help create the most favourable environment in the EU for the development of a crypto-asset industry competitive with other regions of the world.

Contacts:

- Faustine Fleuret, President and CEO: faustine.fleuret@adan.eu
- Hugo Bordet, Regulatory Affairs Officer: hugo.bordet@adan.eu

Website: www.adan.eu

Twitter : [@adan_asso](https://twitter.com/adan_asso)

Mail: contact@adan.eu

Summary

Recent money laundering cases in the European Union have highlighted the need for a harmonised and cooperative regulatory framework for national supervisors and financial intelligence units to deal more effectively with money laundering and terrorist financing activities.

The Anti-Money Laundering and Combating the Financing of Terrorism (AML/CFT) legislative package published by the European Commission on 21 July is intended to address these regulatory gaps and bring more consistency to the implementation of the risk-based approach in Member States.

Adan thus encourages the European Commission's desire to harmonise the requirements and supervision of Member States in the area of AML/CFT at the European level, in particular through the establishment of a European AML/CFT authority.

However, some less positive findings also emerge from this legislative package. On the one hand, some of the provisions of this legislative package will **need to be clarified** in order to avoid any deviation by Member States. On the other hand, some points seem **too restrictive** to the crypto-asset industry.

Adan, therefore, considers that it is necessary to bring the provisions of this European Commission package into line with the specificities of the activities of the crypto-asset industry.

I - Context and challenges of the European Commission's AML/CFT package

On 20 July, the European Commission published a [package of legislative and regulatory proposals](#) to strengthen the anti-money laundering and combating the financing of terrorism (AML/CFT) rules in the European Union.

This package consists of four new texts with a regulation establishing a European AML/CFT authority called "AMLA" (Anti-Money Laundering Authority), a regulation on AML/CFT (known as "AMLR"), containing rules directly applicable for the Member States, in particular with regard to customer due diligence and beneficial owners, a sixth anti-money laundering directive (known as "AMLD 6") incorporating the former provisions of the fifth directive and strengthening cooperation between financial intelligence units and a revision of Regulation 2015/847/EU on fund transfers in order to ensure the traceability of transactions on crypto-assets.

The publication of this package by the European Commission takes place in a particular context concerning European AML/CFT regulation.

Adan welcomes the harmonisation and strengthening of the European framework applicable to the crypto-asset industry . First, the current European AML/CFT legislation is characterised by a lack of harmonisation. The AML/CFT obligations of reporting entities, in particular with regard to crypto-asset service providers, may vary considerably between Member States' national laws and facilitate "*law shopping*" by some actors. Secondly, some Member States' AML/CFT control systems are deficient. This is due, in particular, to the lack of resources to carry out an effective risk-based approach.

However, Adan promotes some necessary adjustments to strike the balance between guaranteeing financial security and promoting innovation effectively.

In this paper, Adan takes a position on the publication of the European Commission's legislative package aimed at strengthening the EU's anti-money laundering and counter-terrorist financing (AML/CFT) rules, and its effects, both positive and negative, on the crypto-asset industry.

II - Comments on the establishment of an AML/CFT authority

At the heart of the legislative package published by the European Commission is a proposal for a regulation to establish a new European anti-money laundering authority, the AMLA. The role of the AMLA would be to fill the current gaps in the supervision of regulated entities and to harmonise the transposition and enforcement of AML/CFT regulations within the European Union.

a) Consistent supervision of players at EU level

The creation of an EU-wide AML/CFT authority - which would replace national supervisors - would provide a wide range of new opportunities for supervising reporting entities:

- **A central body for the coordination of AML/CFT regulation at the EU level.** AMLA will ensure greater convergence of supervisory standards within the European Union, thus integrating a single EU-wide supervisory system.
- **Direct supervision of certain entities.** AMLA will be responsible for directly supervising certain risky financial actors whose cross-border activity requires immediate action to address BC-FT risks. To date, crypto-asset service providers or CASPs are not subject to AMLA supervision.
- **Enhanced cooperation between financial intelligence units (FIUs).** AMLA will ensure cooperation between national FIUs and assist in the coordination and joint analysis between them to better detect illicit cross-border financial flows.

Adan's position

Adan welcomes the creation of a European anti-money laundering authority. The AMLA will ensure equal treatment in the supervision of reporting entities within the European Economic Area and will enable the establishment of an exchange network between financial intelligence units, thus facilitating the coordination of FIUs in the prosecution of money laundering and terrorist financing breaches.

b) Precautions to be taken in the supervision of reporting entities

The draft regulation establishing the AMLA will give this authority the task of direct supervision over the reporting entities presenting the most BC-FT risks and indirect supervision over the other entities (i.e. by bypassing the national supervisory authorities, if a non-selected entity presents BC-FT risks deemed particularly significant).

→ Precautions for direct AMLA supervision;

As regards direct supervision by the AMLA, Article 12 of the Regulation specifies the selected entities that will be subject to periodic assessment by the authority:

- Credit institutions which are established in at least seven Member States; and
- Other financial institutions operating in at least ten Member States, including the Member State of establishment, another Member State where they operate through a subsidiary or branch, and all other Member States where they operate through the direct provision of services or through a network of representative agents.

Article 12 also details the methodology for the selection of the selected entities to be directly supervised by the AMLA.

The risk profile (low, medium, substantial or high) inherent in the activity of obligated entities is assessed according to three main criteria, systematically taking into consideration the volume of the entity's activity:

- Type of clientele;
- Types of products and services; and
- Geographic areas.

Adan's position

While crypto-asset service providers will not initially be subject to AMLA oversight, it appears that, due to the exponential growth of these players, the AMLA may gradually extend its jurisdiction to these providers. Thus, in time, these crypto-asset industry players could be selected by the AMLA.

However, given the criteria established to assess the BC-FT risks related to an entity's activity, it would seem that these players could more easily be subject to direct supervision by the AMLA. Indeed, it appears from the AMLA's risk assessment method that the most established crypto players could be subject to direct supervision, particularly in light of the risks associated with their type of activity (often cross-border) and their volume of

transactions.

A too broad selection - based on irrelevant and/or missing criteria - could be counterproductive: this would not help distinguish actors between them (in terms of the risks that they bear) then identify and manage risks correctly given resources and expertise allocated to the AMLA.

As a result, Adan calls for a more granular selection of the selected entities, being more vigilant about entities whose AML/CFT system is deficient, in particular those entities that have already been convicted for failure to meet their AML/CFT obligations.

Adan's proposal

Adan proposes to add an additional criterion to the AMLA selection methodology: a criterion related to the age and the level of updating of the entity's AML/CFT system. Indeed, entities recently created and approved by the competent State authorities are supposed to have put in place an AML/CFT system in compliance with recent standards. As such, it would be less relevant to audit them during the first years. On the other hand, for older companies, the opportunity of a direct control is more interesting because the question of updating their systems arises.

c) Establish trained crypto-asset teams within AMLA.

In recent years, the growth of the crypto-asset sector has led to the need to regulate this sector, particularly to limit money laundering and terrorist financing breaches. Faced with the growth of these new technologies, regulators have sometimes found themselves unable to understand certain projects or to regulate them due to the decentralised and distributed nature of these networks.

In this context, if the European authorities are now familiar with this new asset class (especially since the digital finance package), the implementation of the AMLA would be a real opportunity for the European Union to understand more effectively the specificities related to the crypto-asset sector in order to adapt the regulations accordingly (i.e., especially concerning the understanding of AML/CFT in the decentralised finance sector).

Adan's proposal

For these reasons, Adan invites the European Commission to set up a team dedicated to the specificities of the crypto-asset sector - a sector that is still destined to grow and become more complex. This dedicated team will allow the European Union to have a first direction related to the fight against BC-FT in the context of crypto-asset transactions.

III - Comments on the introduction of an AML/CFT regulation

The legislative package published by the Commission also consists of a new AML/CFT regulation. With the AMLR, the European Commission intends to harmonise the customer due diligence and beneficial owner requirements for reporting entities.

a) Harmonisation of the rules applicable to CASPs at the European level

Regarding the AML/CFT Regulation on customer and beneficial owner due diligence, the proposed regulation (AMLR) includes crypto-asset service providers (i.e. CASPs as defined in the draft MiCA Regulation) in its scope.

Article 15 of the AMLR requires a CASP that initiates or executes an occasional transaction that constitutes a transfer of funds in crypto-assets exceeding €1,000 or the equivalent in national currency to implement customer due diligence measures. The draft regulation will harmonize the rules related to customer due diligence within the European Union. Under the regulation, all European crypto-asset service providers offering their services in the EU will be obliged to collect details of customers sending and receiving crypto-assets and to implement customer due diligence measures.

Adan's position

Adan is in favour of the introduction of these rules on due diligence and identification of beneficial owners and welcomes the harmonisation efforts orchestrated by the European Commission. The introduction of a client identification requirement for CASPs will facilitate the creation of a framework of confidence for users and will oblige certain unregulated players to carry out due diligence measures on their clients.

Nevertheless, although this provision is a good approach, Adan encourages the European Commission not to leave any room for interpretation to the Member States in the

implementation of these thresholds relating to customer due diligence measures. Indeed, the French legislation in force which currently obliges (French and non-French) CASPs addressing the French public to put in place vigilance measures for all transactions carried out by their clients from the first euro¹. In order to avoid regulatory gap facilitating law shopping for players in the crypto-asset industry within the European Union, an alignment on the most ambitious frameworks should be envisaged.

Adan's proposal

The current wording of the article is as follows:

"2. In addition to the circumstances referred to in paragraph 1, credit and financial institutions and crypto-asset service providers shall apply customer due diligence when either initiating or executing an occasional transaction that constitutes a transfer of funds as defined in Article 3, point (9) of Regulation [please insert reference – proposal for a recast of Regulation (EU) 2015/847 - COM/2021/422 final], or a transfer of crypto-assets as defined in Article 3, point (10) of that Regulation , exceeding EUR 1 000 or the equivalent in national currency."

According to Adan, the European Commission has two alternatives regarding customer due diligence:

1/ Adan suggests adapting the French regulation currently in force to the European Union level. In this context, we propose to amend Article 15 of the AMLR in order to adapt the threshold set by the European Commission to that of the French customer identification system in order to avoid any distortion of competition.

Thus, Article 15 of the AMLR would read as follows:

"2. In addition to the circumstances referred to in paragraph 1, credit and financial institutions ~~and crypto-asset service providers~~ shall apply customer due diligence when either initiating or executing an occasional transaction that constitutes a transfer of funds as defined in Article 3, point (9) of Regulation [please insert reference – proposal for a recast of Regulation (EU) 2015/847 - COM/2021/422 final], or a transfer of crypto-assets as defined in Article 3, point (10) of that Regulation , exceeding EUR 1 000 or the equivalent in national currency."

¹ Decree n°2021-387 of April 2, 2021

3. ***Crypto-asset service providers shall apply customer due diligence when involved in or carrying out any occasional transaction.***

2/ If this proposal is not retained, another alternative remains possible : **Adan invites the European Commission to engage all Member states to apply similar rules and regulatory thresholds (by adjusting national laws when necessary)** for any transaction above EUR 1 000 in crypto-assets in order to promote the harmonisation of the AML/CFT framework at the EU level.

b) The debatable ban on anonymous crypto-assets wallets.

In order to mitigate the risks associated with anonymous financial instruments, Article 58 of the AMLR aims to prohibit crypto-asset service providers from maintaining any anonymous wallet on behalf of their clients.

Adan's position

To date there is no model for anonymous crypto asset wallets kept by CASPs for their clients. Anonymous crypto-assets wallets such as Wasabi Wallet or Samurai Wallet are non-custodial (i.e. they are not maintained by regulated entities such as CASPs).

As a result, it would appear that article 58 is inapplicable due to the lack of cases where CASPs would keep anonymous crypto-asset wallets for its clients.

It is possible that the European Commission's intention would be to prohibit the use of anonymous non-depository wallets in order to enforce the Travel Rule more effectively, but the prohibition of these wallets is questionable :

- **First of all, Adan understands the European Commission's desire to regulate this type of product, which presents significant AML/CFT risks.** However, in practice, anonymous wallets are a tool that is not very popular with criminals². Moreover, the protection of the right to privacy of users of crypto-assets must be ensured on blockchain networks. This prohibition thus seems severe in view of the small number of crypto-assets laundered via anonymous wallets.

² [Over 13% of all Proceeds of Crime in Bitcoin are Now Laundered Through Privacy Wallets](#), Elliptic, 09 December, 2020.

- **These tools are not traceable, but identifiable.** According to the European Commission, it appears necessary to prohibit the provision of these anonymous wallets because they do not allow the traceability of crypto-asset transfers. However, the transactional analysis tools of blockchain networks (such as Chainalysis, Elliptic or Scorechain) can inform compliance services that a customer has used an anonymous wallet, without being able to trace the origin of the funds. This decisive information will allow compliance departments to implement additional vigilance measures to determine the origin of funds in crypto-assets. Thus, while the traceability of transactions made on anonymous wallets is particularly complex, it is not impossible.
- **There are several alternatives to using anonymous wallets.** Criminals have other transaction anonymisation tools to launder their ill-gotten gains³ such as anonymous crypto-assets (such as Zcash and Monero), mixers (such as Tornado Cash), and non-depository anonymous wallets.

Adan's proposal

For these many reasons, Adan proposes to review Article 58 of the AMLR.

The current wording of the article is as follows:

"Credit institutions, financial institutions and crypto-asset service providers shall be prohibited from keeping anonymous accounts, anonymous passbooks, anonymous safe-deposit boxes or anonymous crypto-asset wallets as well as any account otherwise allowing for the anonymisation of the customer account holder [...]."

According to Adan, the European Commission has two alternatives regarding the use of anonymous wallets:

1/ Delete the provision to prohibit the detention of anonymous crypto-asset wallets of CASPs for their clients and require CASPs to strengthen their controls on anonymous wallets in order to better identify AML/CFT risks among their customers who use them.

Thus, Article 58 of the AMLR would read as follows:

"Credit institutions, financial institutions and crypto-asset service providers

³ [The fight against money laundering in front of crypto-assets activities: which risks for which regulation?](#), Adan, 12 July, 2021

*shall be prohibited from keeping anonymous accounts, anonymous passbooks **or** anonymous safe-deposit boxes ~~or anonymous crypto-asset wallets~~ as well as any account otherwise allowing for the anonymisation of the customer account holder. [...]*

If the CASP identifies that its client has used an anonymous wallet for any casual transfer of funds, it will have to carry out enhanced due diligence measures on its client and identify the origin of the funds in crypto-assets.”

2/ Harmonise the EUR 1 000 threshold initially set by the FATF in its 2019 Guidelines on VASP, below which operations involving anonymous wallets are authorised without further investigation on the origin of funds. This provision would be economically acceptable given the small number of assets laundered via anonymous crypto-asset wallets, the EUR 10 000 threshold set for cash transactions in the same Regulation and the need to guarantee the privacy rights of users of blockchain technologies. This provision would thus be consistent with the level of privacy that crypto-asset wallets offer compared to cash.

c) The need to introduce a Grandfather clause for providers already regulated in Europe

Within the European Union, many crypto-asset service providers are already obliged to implement an AML/CFT procedure when they wish to deploy their services to the public (e.g. in France, the PACTE law of 22 May 2019 requires crypto-asset service providers to implement an AML/CFT scheme when they offer all or part of their digital asset service to the French public).

Thus, although the European Commission's AML/CFT legislative package establishes a harmonised AML/CFT framework within the EU, many actors already comply with the provisions set out in the AML Regulation.

Adan's proposal

In this context, Adan considers that it would be necessary to insert a grandfather clause to ensure that those actors who already carry out their AML/CFT due diligence do not have to engage into the authorisation procedure again (for all or relevant part of their AML/CFT system) with the entry into force of the European Commission's AML/CFT legislative

package. On the one hand, actors would avoid to engage necessary time and costs twice ; on the other hand, regulators would better focus on actors who need to get compliant with the EU framework.

To this end, such clause should be added into AMLR and/or AMLD6 and/or Regulation for an AMLA.

IV - Comments on the revision of the Regulation on Transfers of Funds

Due to the lack of regulation applicable to crypto-asset transactions in several EU member states, the European Commission wants to revise the 2015 Regulation on Transfers of Funds to adapt the regulation to crypto-asset service providers.

Indeed, according to the Commission, the lack of regulation of the crypto-asset market exposes crypto-asset holders to money laundering and terrorist financing risks, as illicit money flows can occur through crypto-asset transfers.

a) The application of the travel rule to crypto asset activities

Articles 12 et seq. set out the requirements related to the obligation to identify the customer when transferring funds in crypto-assets equivalent to or exceeding EUR 1 000.

At the time of the transfer, the provider shall collect the name, residential address, date of birth, account number of the client. For the beneficial owner, the provider shall collect the name and account number of the beneficiary of the funds.

Adan supports the European Commission's intention to introduce these obligations relating to the identification of customers and beneficial owners for crypto-asset service providers.

The amendment of this regulation will serve as a means of introducing the *travel rule* within the European Union. However, the European Commission has identified obstacles to the implementation of the travel rule - obstacles that will need to be addressed in order for the rule to apply to all regulated entities: "*Stakeholder input on the Action Plan was broadly positive. However, some European Union VASP representatives claimed that the absence of a standardised global, open source and free, technical solution for the travel rule could lead to the exclusion of small actors from the crypto-assets market, with only important players being able to afford compliance with the rules.*"

Adan's position and proposal

- **Technically the solutions are not yet ready.** The transmission of information between CASPs requires a secure, accessible and open communication channel and an information standard.

In order to be effective and secure, this transmission of information between CASPs needs to be deployed after audits have been carried out and certain standards have been met concerning the data format, the security of the information channel, the constraints linked to the transmission of personal data, etc.

In practice, the existing solutions do not meet these requirements and are therefore not satisfactory as they stand to meet the European Commission's criteria, which take up those previously set out in Article 15 of the latest FATF Recommendations.

- **In terms of data protection.** Adan considers that it would be dangerous to mandate actors to automatically transmit very sensitive information such as the surnames, first names, date of birth of customers to a CASP that potentially would not be supervised or in a much less strict manner than in France, or established in jurisdictions that could have an economic or strategic interest in exploiting this data.

At the very least, this automatic transmission of information should only be implemented for the benefit of establishments that meet certain strict criteria - yet to be defined.

- **In terms of the competitiveness of France and Europe.** It must be stressed again that an immediate transposition of this obligation would have significant consequences on the competitiveness of the companies that would be subject to it. Giving a monopoly to the first solution provider would be detrimental to the industry.

b) Uncertainties related to unhosted wallets

Unhosted wallets are non-depository wallets in which the holders retain full custody of the private keys and dispose of their funds without necessarily involving an intermediary. Adan wonders about the implications of the regulation of fund transfers on unhosted wallets

The risk is that users of unhosted wallets may be unable to transact with a regulated CASP when transferring crypto-assets to a hosted wallet, particularly if they are unable or unwilling to provide beneficiary information when transferring funds.

Adan's position

Adan considers that the implementation of the travel rule with regard to CASPs would be complex regarding the recovery of information related to the beneficiary of the transaction. Indeed, if a CASP customer transfers funds in crypto-assets to an unhosted wallet (for example, on Metamask), the latter will not be able to retrieve the name and surname of the beneficiary of the transaction, given the fact that no KYC procedure has been carried out on him.

c) The risk related to the total traceability of crypto-asset transactions

Finally, Adan would like to draw the attention of the European Union to its willingness to trace all crypto-asset transactions in order to limit the risks of money laundering and terrorist financing.

Indeed, in its press release, the European Commission stated that *"Today's amendments will ensure full traceability of crypto-asset transfers, such as bitcoin, and will allow for prevention and detection of their possible use for money laundering or terrorism financing (...). These proposals have been designed to find the right balance between addressing these threats and complying with international standards while not creating excessive regulatory burden on the industry."*

In the crypto-asset sector, as in the art or real estate market, there are undoubtedly risks of money laundering and terrorist financing. But for several years now, these risks have been diminishing as regulations have developed and technology has become more sophisticated. According to the Crypto Crime Report from transactional analytics firm Chainalysis, in 2020, illicit activity on crypto-assets accounted for only 0.34% of all transactions on blockchain networks, or about \$10 million in transaction volume. While this amount appears large, it represents only a small portion of the \$2 trillion laundered each year worldwide⁴.

Adan's position

Adan calls on the European Commission to be cautious about its desire to ensure the traceability of all transactions on crypto-assets. A regulation that is not adapted to the level of development of the sector could be ineffective, or even restrictive for project holders, especially in the case of decentralised finance.

⁴ Source: United Nations Office on Drugs and Crime and Laundering

Finally, regarding the traceability of crypto-asset transactions, Adan would like to draw the attention of the European Commission to the key role of transactional analysis tools in AML/CFT for the crypto-asset ecosystem.

Indeed, transactional analysis tools (TATs) - such as Chainalysis, Elliptic, e-NIGMA, Scorechain, etc.) - are becoming increasingly efficient and effective. Thanks to the information gathered from public registers (so-called "on-chain" informations such as public addresses, transaction dates, transaction amounts, etc.), combined with external data (so-called "off-chain" informations), a TAT makes it possible to draw conclusions about the risks associated with a transaction or group of transactions. CASPs can thus adjust their due diligence to the level of risk identified, or even refuse to enter into a relationship or a specific transaction, or even report to their FIU or freeze assets. In 2020, they helped authorities to trace and dismantle several criminal networks like the Harrod's drug ring in 2019, ISIS-related individuals in France and in the UK in 2020, and more recently the identification of donors who helped plan the US Capital riot in January 2021. In his report Analysis of Bitcoin in Illicit Finance, Michael Morell - former CIA Deputy Director - underlines the interest of TATs and encourages their systematic use for the surveillance of flows by States. Especially as transactional analysis tools are becoming more sophisticated against certain anonymisation tools (such as anonymity-enhanced crypto-assets and mixers). Indeed, if these transactional analysis tools are not able to trace exactly the origin of crypto-assets subsequent to the use of a mixing service (e.g. whether it is centralised mixers such as chipmixer or decentralised mixers such as Tornado Cash), or of an anonymity-enhanced crypto-asset (such as Monero or Zcash), these tools will nevertheless be able to detect that a CASP client has - in the past - used an anonymizing service before putting his assets on the CASP wallet. A red flag will be raised against the client and the CASP will carry out enhanced due diligence on his suspicious client to determine the reasons for the use of such a tool and the origin of crypto-assets.

Adan is available for any question on this paper.

~