EUROPEAN FINTECH ASSOCIATION POSITION PAPER ON CRYPTO ASSETS UNDER THE ANTI-MONEY LAUNDERING REGULATION

Executive Summary

The European Fintech Association (EFA) welcomes the progress made on the Anti-Money Laundering Package by the European Commission, European Parliament, and the European Council. The EFA fully supports a harmonized regime containing clear rules intended to improve the detection of suspicious transactions and activities. The EFA has already presented comments to the AMLR Regulation in relation to outsourcing and AISPs. In line with our previous position papers, we believe that the comments presented in this document addressing specific crypto-related matters in the AMLR text will help harmonize and enhance the effectiveness of anti-money laundering and countering financial terrorism (ML/FT) rules across Europe.

The following details EFA's views as regards AMLR

- **Self-hosted wallets**
  We encourage co-legislators to:
  - Clearly differentiate between wallets specifically designed to obfuscate transactions and self-hosted wallets.
  - Remove thresholds for transactions with self-hosted wallets.
  - Apply a fit-for-purpose approach to customer due diligence (CDD) measures for transactions involving self-hosted wallets.
- **CDD requirements**
  - We encourage co-legislators to introduce CCD requirements for crypto asset service providers (CASPs) that are equal to those in the wider financial services ecosystem.

Self-hosted wallets

Self-hosted wallets empower users to directly hold their crypto assets without using intermediaries' custody services. In doing so, users gain greater control over their crypto assets and minimize dependency risks (e.g. stemming from insolvency of the third party). However, self-hosted wallets, based on their design, may also require different approaches to protect users and help prevent ML/FT.

We are supportive of the European Parliament's (EP) changes to Recital 93 that clarifies that CASPs should not be restricted from offering self-hosted wallet service to customers. However, we believe that AMLR needs to appropriately distinguish between different types of privacy-enhancing solutions.

We wish to flag the importance of enabling the industry to develop privacy-enhancing solutions in the crypto asset market as well as financial services, provided that those solutions continue to enable law enforcement agencies to take appropriate action to trace and lead enforcement action where required, and do not prevent CASPs' ability to comply with legal obligations under financial crime legislation.

EFA is against the provision of services that are inherently designed to prevent law enforcement from tracing transactions. We believe that AMLR needs to appropriately distinguish between the respective characteristics of these different types of privacy-enhancing solutions. Privacy is important for the consumer - but only to the extent that a solution feasible for law enforcement can be found. EFA is aware of a number of industry solutions in the market that help trace crypto asset transactions and support law enforcement initiatives without eroding individuals' privacy rights.

EFA does not support the EP's Article 59a, which prevents the acceptance or transfer of values equivalent to or over EUR 1 000 using self-hosted wallets. In our view any limit imposed should be removed or at least match that applied to cash transactions (i.e. EUR 7 000 or EUR 10 000).

Article 31a of the European Parliament's AMLR version requires CASPs to identify and verify the identity of the person who owns or controls a self-hosted wallet outside of a customer relationship. This raises broader issues of privacy. Requiring crypto asset service providers to collect potentially sensitive personal information about people who are not their customers creates risks for businesses and consumers, and risks harming the competitiveness of the EU in the digital finance space.

- Businesses would be required to seek and store personal data of individuals they have no relationship with, unnecessarily increasing risk to a greater number of individuals and heightening potential impact in the event of a data breach.

- Consumers, simply seeking to understand who holds personal data about them, might submit personal data access requests to a broad range of crypto asset businesses, just to understand who holds their personal data. This will generate a disproportionate amount of access requests and therefore make data management by market players less efficient.

- Consumers would be placed at risk from a privacy and security perspective because third parties, potentially unknown to them, would hold their personal information, and have no contractual obligations to maintain privacy of such information. This increases the vector for possible cyber-attacks that could affect a broad range of consumers.

- Local privacy laws may prevent the customer of a custodial wallet provider from providing personal information to third parties.

Additionally, there are no technically proven means of identifying the person that manages or owns a self-hosted wallet outside of customer relationships. Verifying the identity of the person who owns or benefits from a self-hosted address is something that will not be required by other jurisdictions, and risks harming the competitiveness of the EU in this area.

A more appropriate approach would be to minimize the impact on CASPs by relying on customer data collected through existing know-your-customer and customer due diligence processes at on- and off-boarding and using crypto asset tracing technology to match customer data collected by CASPs with

custodial wallet IDs. In doing so, regulators would place less burden on CASPs and increase law enforcement agencies' ability to trace transactions of concern.

Customer Due Diligence Requirements

Article 15(2) of the AMLR in the Council's version introduces a change requiring CASPs to perform CDD measures of at least identifying and verifying the customer's identity for occasional transactions in crypto assets below EUR 1 000. We believe such a measure does not align with the introduced sector-wide rules, which require CDD measures only above the EUR 1 000 threshold. We encourage co-legislators to take the technology-neutral approach and align CCD rules for CASPs with the wider financial ecosystem rules.

AML and CTF requirements should target the point at which customers enter or exit the crypto asset market (i.e. where they are onboarded to platforms that facilitate conversion between fiat currencies (e.g. EUR, USD, GBP) and crypto assets (so-called on/off ramps)) and more broadly align with existing CDD approaches in financial services. This would ensure customer data is collected through existing know-your-customer and customer due diligence processes, and in any event before a crypto asset can be purchased or sold. This should be supplemented by the use of crypto asset tracing technology to match customer data collected by CASPs with custodial wallet IDs. In doing so, regulators would place less burden on CASPs and increase law enforcement agencies' ability to trace transactions of concern.

ANNEX

Background on crypto assets: *What are crypto assets? How do they work?*

Crypto assets are the digital representation of a value or of a right that is able to be transferred and stored electronically using distributed ledger technology (DLT) or similar technology. They can be stored, transferred and traded electronically. As noted by the Bank for International Settlements, DLT is a type of technology, encompassing protocols and the supporting infrastructure that enables computers in different locations to propose, validate and store records in a synchronised way across a network. DLT is not new, it has been used in many industries by organisations that have distributed offices or branches as a method to store and share information. Traditionally, however, such distributed ledgers have been operated by a system administrator that performs key functions to maintain consistency across multiple copies of the ledger.

Novel decentralized crypto asset models (e.g. Bitcoin and Ethereum) have enabled open and trustless DLT by developing mechanisms to verify and agree on new information to be added to the DLT. They do this through so-called consensus mechanisms (e.g, Proof of Work, Proof of Stake), in which network participants validate transactions. By confirming and reconfirming a crypto asset's ownership history, it is possible to attest to the crypto asset holder's right to transfer ownership in it to a recipient. The information stored on distributed ledgers is public, allowing all transactions to be linearly tracked.

We believe that crypto assets and DLT have the potential to improve how today's financial services operate, by restoring consumers' control and autonomy when they transact with each other and businesses, by increasing competition in financial services and driving innovation by new market entrants and incumbents alike.

CSDDD: Establishes requirements for very large companies to integrate sustainability due diligence in corporate policies, identify and mitigate impacts on the environment and human rights in their value chains. Requirement to adopt a plan to make business compatible with climate targets.

"