Crypto-wallets and the new EU AML package: where are the battle lines drawn?

BY NADIA POCHER - 07 SEPTEMBER 2021

In an effort to overcome the fragmentation stemming from the national transpositions of the existing EU framework to combat money laundering and the financing of terrorism (AML/CFT), the European Commission has recently put forward a comprehensive set of legislative proposals. While accounting for the most significant aspects of this "AML package", this blogpost explores the endeavor to implement the so-called "crypto travel rule" and the relevant impact on different types of cryptocurrency wallets.

Last March we explored the controversial interplay between the AML/CFT regulatory framework and the subtype of cryptocurrency wallets dubbed *self-hosted* or *unhosted* wallets. Given the absence of regulatable intermediaries in the peer-to-peer (P2P) transactions enabled by the latter, the FATF was providing restrictive recommendations, and the US FinCEN was considering stark measures. You may have been left wondering: where has the EU been standing on this? A recent legislative proposal may provide a first answer.

AML/CFT harmonization in the EU: a brief overview

Following in the footsteps of the FATF, from 1991 onwards the EU has been increasingly involved in drafting AML/CFT legislation. Indeed, the accelerating socio-economic interconnection at a global level demanded supranational measures to avoid exploitation for criminal purposes. To the present day, the effort has primarily pursued an EU-wide harmonization of the relevant rules by the means of Directives. Hence, application and enforcement have been largely left to the Member States.

The modern EU AML framework was introduced by the Fourth AML Directive (EU) 2015/849, along the lines of the 2021 recast of the FATF's Recommendations. Later, the amendments introduced by the Fifth AML Directive (EU) 2018/843 specifically addressed cryptocurrencies and providers of related services. Subsequent directives were adopted in 2018 and 2019 in the areas of criminal law and information exchange.

2021 AML Package: key take-aways

The Package of four legislative proposals published on July 20, 2021, implements a six-pillar-based Action Plan on AML adopted in 2020. The goal of the initiative is not to transform the AML framework, but to ensure its effective implementation vis-à-vis the discrepancies among the Member States' transposition (or lack thereof) of the Directives. Meanwhile, the EC intends to narrow the gap between the AML effort and the Digital Finance Package adopted in September 2020, with chief reference to the proposal for a Regulation on Markets in Crypto-Assets and its definition of crypto-assets.

Besides extending the application of AML rules to the entire crypto sector, the goal of the Package is primarily twofold. On the one hand, it aims to create a single EU-wide rulebook on AML/CFT, largely grounded on Regulations – *i.e.*, on legislative instruments that are inherently applicable at domestic level in a direct and immediate way. The scheme would deal with, *inter alia*, customer due diligence, beneficial ownership, enhanced coordination among Financial Intelligence Units (FIUs) and an EU-wide limit to cash payments of 10,000 EUR. On the other hand, the EC plans to have the framework overseen and enforced by an *ad hoc* supervisor: a new Anti-Money Laundering Authority (AMLA).

The "crypto travel rule": recast of Regulation (EU) 2015/847

The EU AML effort, however, has never been a stranger to the use of Regulations. On the contrary, the Fourth AML Directive was complemented by Regulation (EU) 2015/847 on the information accompanying transfer of funds. The goal was to ensure the traceability of fund transfers by imposing on payment service providers

(PSPs) information transmission obligations concerning the payer/sender and the payee/beneficiary. Thus, EU law aligned with the FATF's so-called "travel rule".

Before the Interpretative Note to Recommendation 15 was revised in 2018, the "travel rule" did not mention crypto funds but only wire transfers as per Recommendation 16. Consequently, Regulation (EU) 2015/847 bears no reference to the crypto sphere. When the international debate evolved towards the latter, the relevant industry started denouncing the absence of global standards and technical solutions able to underpin affordable compliance.

The 2021 Package proposes a recast to narrow the "crypto travel rule" gap. To this end, in case of crypto transfers of more than 1,000 EUR (*i.e.*, individual transfers exceeding the threshold or more transfers seemingly linked), originating Crypto-Assets Service Providers (CASPs) would be required to (i) obtain and hold accurate information on the payer, and (ii) certain information on the beneficiary, and (iii) immediately and securely submit it to the beneficiary entity. In turn, beneficiary CASPs would be mandated to (i) obtain and hold certain information on the payer, and (ii) accurate information on the payee. Upon request, all the information must be made available to the authorities.

What does it mean for self-hosted wallets?

The revision of Regulation 2015/847 pivots around CASPs – indeed, an intermediary-based framework could not have done any different. Nonetheless, crypto communities have highlighted possible repercussions on the use of self-hosted wallets – *i.e.*, non-custodial wallets whereby holders retain full custody of the private keys and dispose of their funds without necessarily involving a middleman. In this respect, two scenarios appear to be worthy of attention.

On the one hand, "self-hosted wallet to self-hosted wallet" transfers would raise questions of legitimacy, given they would elude both "travel rule" requirements and cash-related restrictions, but also of a possible displacement of crypto transfers towards unsupervised areas. On the other hand, users of self-hosted wallets could prospectively be unable to transact with a regulated PSPs – *e.g.*,

transfer crypto funds to a hosted wallet. This could happen if they are unable or unwilling to provide the necessary information to the custodian service provider of their counterparty, but also if the PSP adopts a de-risking approach to transactions originating from/destined to unregulated counterparties.

(Some) open issues

The debate on the travel rule is one of the most complex among those affecting the crypto sphere. Indeed, it involves implementation and technical issues that are interwoven with policy decisions and business incentives. At the same time, the recent debates surrounding Decentralized Finance (DeFi) applications show that although the development of innovative services is influenced by regulation, a set of crypto communities can leverage technology to thrive outside the border of compliance. The nature of self-hosted wallets is an emblem of this tension.

When assessing the AML Package's approach to the "crypto travel rule" issue, conflicting sentiments arise. Undeniably, it is not easy to effectively mitigate the risk of abuses for criminal purposes without displacing shady activities to the underground world of P2P transfers, thereby impeding any transaction scrutiny with possibly disastrous consequences. At the same time, however, we are left wondering whether it is feasible to place bans or restrictions on self-hosted wallets without unduly affecting the freedom of economic activity, and/or whether the degree of enforceability of such limitations should bear any weight in the relevant decisions.

ABOUT THE AUTHOR — NADIA POCHER
Nadia Pocher is a doctoral researcher in the Law, Science and Technology Joint Doctorate - Rights of Internet of Everything (LAST-JD-RIoE), funded by the EU Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie International Training Network European Joint Doctorate Grant Agreement No 814177. Her research takes place at the Institute of Law and Technology of the Autonomous University of Barcelona (UAB), in collaboration with the University of Bologna (UNIBO) and the KU Leuven Centre for IT & IP Law (CiTiP).