consensys

Consensys response to the EBA Consultation on revised Guidelines on money laundering and terrorist financing (ML/TF) risk factors (EBA/CP/2023/11)

Consensys welcomes the EBA's proposal on amendments to its Guidelines on money laundering and terrorist financing (ML/TF) risk factors in order to adequately reflect the realities of the financial crime in the crypto ecosystem. Consensys believes that money laundering and other forms of criminal activity in the cryptocurrency space is a serious problem whose solution can be addressed through public policy and regulation as well as technology. Hence, we recognize the importance of engaging with European Union policymakers in developing harmonized and sensible Anti-Money Laundering and Terrorism Financing rules for the crypto-assets markets. This will strengthen the effective fight against financial crime and provide legal clarity while protecting consumers.

In particular, we encourage the implementation of blockchain analytics to facilitate risk management and supervision. We also think it is essential to apply a risk-based approach that acknowledges the specificities of the sector and which allows for proportionate treatment to ensure the underlying technology and CASPs are not put at a disadvantage to other obliged entities and financial products and services.

Consensys would like to provide comments on question 9: ¨Do you have any comments on the proposed changes to Guideline 21?¨

Guideline 21.3. d) i. states that using a self-hosted wallet is a factor that may contribute to increasing ML/TF risks and merits enhanced due diligence.
EBA should clarify that Using a self-hosted wallet alone is not grounds for enhanced due diligence.

Self-hosted wallets (SHWs) are software programs that allow a user to read blockchain data and compose transactions that can be executed by the user pseudonymously without the assistance, permission, or interference of a third-party intermediary. It does not appear to be the EBA's position that the use of SHW software itself is a factor that, on its own, merits the application of enhanced due diligence. We agree, and believe the EBA should expressly state that in its final guidance.

Using a SHW is akin to using a web browser. In the same way that web browsers allow consumers broad access to the Internet, SHW are essential for users to access and operate in the Web 3.0 space which

encompasses not just financial services but also social, commercial, and recreational applications. Moreover, SHWs allow users to retain custody of their own crypto-assets and minimize third-party dependency risks. It would be a new and unwarranted step to require that intermediaries conduct enhanced due diligence on persons merely because they use an individualized technological interface to read information from and send cryptographically secured messages to a computer network. We agree with the EBA that this approach is unwarranted.

When assessing how SHWs impact illicit finance risks, it is important to recognize that, the pseudonymity offered by an SHW is of only very limited 'help' to bad actors due to the effectiveness of blockchain analytics. Generally, everything that happens within a blockchain can be monitored and traced back to transactions where the parties can be identified. That is where the technology brings added value to AML investigations, as has been recognized by the EBA in these proposed Guidelines.

Moreover, as the EBA undoubtedly understands, there is a distinction between SHWs and software protocols and other tools specifically designed to obfuscate transactions. The former does not provide anonymity or transparency obfuscation and therefore does not merit any sort of EDD that the EBA feels is necessary in relation to privacy-enhancing technology[1]. For guidance to specify that EDD should be applied in the instance where either were used would be to ignore the important distinction between them.

The conclusion that EDD is not required in situations involving a SHW is further buttressed by the Transfer of Funds Regulation (TFR) regime, which already established identification and verification requirements along with a risk-based assessment that CASPs need to apply in relation to transfers done to, from or among SHWs. This regime allows the implementation of AML due diligence based on the financial activity and not on the technology used to perform the transaction. Deviating from this approach would not only create tension with the TFR that would be needlessly burdensome on market participants, but also would not be consistent with the overarching goals of being pro-innovation and technology-neutral. We are appreciative of the EBA's position that the TFR regime should be adhered to in this respect.

The qualification by default for the application of EDD based solely on the mere use of self-hosted wallets would not be technology agnostic. We believe that an EDD regime shall be proportionate and preserve a level playing field, preventing the adoption of unnecessary barriers to legitimate businesses operating in the crypto space. We strongly discourage the placement of excessively burdensome EDD requirements on CASPs for transactions involving self-hosted wallets.

Guideline 21.5. b) xv. acknowledges that repeatedly receiving crypto assets from or sending crypto assets to multiple self-hosted addresses or multiple addresses located in other CASPs is a factor that may contribute to increasing ML/TF risks and merits enhanced due diligence.

[1] Please note that Consensys strongly supports policies that protect user privacy and opposes any guidance that serves to disfavor technologies and processes that undermine the ability of everyday people to conduct lawful transactions privately. Such discussion, however, is beyond the scope of our consultation response.

Consensys disagrees that using multiple wallets or CASP accounts is an indication of higher risk, necessitating EDD.

The use of multiple SHWs or CASPs accounts is very common given that public addresses are simply accounts which exist on a blockchain and are inexhaustible and free to access. People and entities use multiple accounts for many reasons, and that includes Consensys. Consensys, as a company, controls, using SHW software, scores of public addresses that we use for various commercial and treasury management purposes. This helps provide for seamless account management and record keeping, but it also reduces risks attendant to the technology. Because of the current technological and operational risks that custodial platforms and self-custody pose, market participants and consumers use many distinct public addresses to manage their funds to spread the risk of a hack, losing keys, or a platform having a catastrophic event. Moreover, different protocols require different public addresses which market participants may wish to manage, or indeed may need to manage, using multiple different SHW software programs.

Using multiple SHW software programs and managing numerous public addresses is thus commonplace and, to some extent, how the blockchain ecosystem is designed to function for the network user. There is nothing inherently indicative of illicit activity in such conduct. Quite to the contrary, this is completely normal market behavior given the current circumstances of a multi-chain, multi-protocol crypto ecosystem and a young, but rapidly growing blockchain software tooling market.
The EBA should not provide guidance that ignores this market reality or creates compliance burdens on intermediaries which effectively makes their due diligence obligations towards nearly all of their users as requiring EDD in nearly all situations.

Guideline 21.3.c) acknowledges that products that place no restrictions on the overall volume or value of transactions is a factor that may contribute to increasing ML/TF risks and merits enhanced due diligence.
Consensys believes that the level of restriction that would avoid enhanced due diligence should not be so low as to make EDD the default process

As an initial matter, Consensys views this guidance as not including SHWs among those products or services where this risk assessment is required. SHWs are, by design, not limited in the type of blockchain instructions that it can compose at the direction of the SHW user. SHWs, being just interface software, should not require any end user due diligence on the part of the software developer for it to be able to publish that software, let alone enhanced due diligence. Any SHW software that attempted to impose such transaction limitations on users would be rejected by the market in favor of widely available software platforms that did not automatically limit user control. Moreover, maintaining such controls for certain regions of the world would necessitate a software developer maintaining different versions of the SHW software, which is incredibly operationally, financially, and technologically burdensome.

That aside, we agree that services which facilitate the transfer of funds without limitations on volume or value do present more risk of money laundering than services that impose some level of restriction. We agree, too, that this is just one factor to consider when assessing the risks and does not, in itself, in and of itself, compel the application of enhanced due diligence.

Our concern is that it is not just the existence of a restriction that reduces the risk of money laundering, but the level of restriction. Restricting transactions to 1 billion EUR or even 1 million EUR is not much different than no restriction whatsoever as a practical matter. Market participants will surely need to decide the level of restriction that is required to eliminate the increased risk that this guidance is indicating, and we are concerned that most participants would, without guidance from the EBA, set the level so low as to have this factor nearly always weigh in favor of enhanced due diligence. If that were the case, it incentivizes service providers to place very tight restrictions on their products, which severely hampers the efficiencies that blockchain services can provide the market. The EBA should affirmatively state in its guidance that volume or value limits need not be akin to levels set in other regulations that purport to put a cap on peer to peer transaction value.

Guideline 21.11 recommends CASPs to apply advanced analytics tools as EDD measures that CASPs should apply for the identified risks.
ConsenSys supports guidance recommending the use of new blockchain analytics technology to minimise ML-TF risk.

ConsenSys recognizes that illicit activity on-chain, while not remotely comparable in volume or frequency to illicit activity in traditional finance, is a serious matter that requires both public policy and technical solutions to address. We note that the traceability of blockchain transactions has been a boon to law enforcement in their efforts to identify illicit behaviour on-chain. Blockchain analytics tools can tie DeFi activity to CeFi accounts which proves to be a powerful investigative tool, which in turn meaningfully disincentives illicit activity. But when bad actors are not sufficiently disincentivized, the blockchain is law enforcement's best friend as information is traceable and reliable. Data is recorded there in an unaltered form for posterity.

We should continue to make the best out of the inherent transparency that blockchain technology offers and collaborate across the government and the private sector to improve these new risk mitigation approaches. Whether in this guidance or in future guidance, we encourage the EBA to view blockchain analytics as not just a method to supplement current due diligence practices, but instead to gradually replace traditional mechanisms that require the burdensome, repetitive, and intrusive disclosure of highly sensitive information. To the extent that new technology can mitigate risk without incurring the costs of such risky disclosures, we hope that EBA and other regulators will take the opportunity to better safeguard the public by leveraging them instead of supporting steadily outdated methods.

About ConsenSys

Consensys is the leading blockchain and web3 software company. Since 2014, Consensys has been at the forefront of innovation, pioneering technological developments within the web3 ecosystem. Through our product suite, including the MetaMask platform, Infura, Linea, Truffle, Diligence, and our NFT platform, we have become the trusted collaborator for users, creators, and developers on their path to build and belong in the world they want to see. Whether building a dapp, an NFT collection, a portfolio, or a better future, the instinct to build is universal. Consensys inspires and champions the builder instinct in everyone by making web3 universally easy to use and develop on. To explore our products and solutions, visit https://consensys.io/