**Ledger SAS**
1, rue du Mail
75002 Paris

Paris, 26 February 2024

## Introduction

Ledger appreciates the opportunity to respond to the European Banking Authority's (EBA) consultation paper on its Guidelines on preventing the abuse of funds and certain crypto-assets transfers for money laundering and terrorist financing (ML/TF) purposes under Regulation 2023/1113 (the "Guidelines").

### *About Ledger*

Ledger, a leading blockchain security company headquartered in Paris, empowers individuals and enterprises to securely manage their digital assets. With over 500 employees worldwide and its principal production facility in Vierzon (France), Ledger has earned trust globally, selling over 6 million units of our hardware devices. As the first and only digital asset wallets to receive a First Level Security Certification from the French Cybersecurity Agency (ANSSI), we take pride in setting the global standard for blockchain and digital asset security.

We have focused our consultation response on a few selected issues of interest described below. We also support the comprehensive response put forward by the Digital Currencies Governance Group (DCGG) to which we have contributed as a member, but we wanted to comment specifically on issues of particular concern relating to self-hosted wallets.

We look forward to a continuing and open dialogue with you on these issues and would welcome an opportunity to discuss this further. For any question or comment, please do not hesitate to contact Seth Hertlein, Global Head of Policy (seth.hertlein@ledger.fr) or Julien David, Head of Regulatory Affairs, EMEA (julien.david@ledger.fr).

## General comments

1. Digital assets are demonstrably less used for ML/TF purposes than traditional finance

We would like to start by stressing our deep concern about the prevalent misconception and disproportionate focus placed by Regulation 2023/1113 and the EBA's proposed draft Guidelines on the use of digital assets for ML/TF purposes. While all stakeholders in the Web3 environment are unequivocally committed to combating ML/TF practices, **Ledger strongly opposes the misguided belief that cryptocurrencies are primarily (or even significantly) used for criminal activities**. This erroneous assumption stems from a fundamental misunderstanding of crypto transactions and their purported prevalence in illicit activities. This fallacy has been repeatedly debunked by empirical data and numerous reports.

The latest Chainanalysis Crypto Crime Report from January 2024 provides compelling evidence that the extent of crypto-related crime is significantly overstated and subject to unrealistic projections. This report conducts a thorough analysis of cryptocurrency transaction data, shedding light on the actual prevalence of illicit activities within the crypto ecosystem. According to the findings, **criminal activity constituted just 0.34% of all cryptocurrency transaction volume in 2023**, down from 0.42% in 2022, amounting to an estimated total of $24.2 billion. However, it is crucial to note that this estimate likely exaggerates the actual level of ML/TF activities. For instance, the inclusion of creditor claims against FTX significantly inflates the reported figures. Moreover, the majority of illicit transactions identified in 2023 (61.5%) are linked to sanctioned entities and jurisdictions under US law. Importantly, a good proportion of these transactions involve average crypto users residing in these jurisdictions, rather than nefarious actors engaging in illicit activities. Another significant portion of the total number of illicit transactions relate to garden-variety scams and frauds, which phenomena are not unique to digital assets and do not relate to ML/TF activity. Once you adjust for the FTX claims, US sanctions, and run-of-the-mill scams, the amount of digital asset transactions attributable to ML/TF activities is a tiny fraction of an already tiny fraction (0.34%).

**In contrast, fiat currencies remain the predominant medium for ML/TF, with the United Nations Office on Drugs and Crime estimating that up to *$2 trillion (5% of global GDP)* is laundered annually through traditional financial systems**.

2. Self-hosted wallets do not carry higher ML/TF risks

In line with this, Ledger also strongly opposes the assertion introduced by Regulation 2023/1113 that self-hosted wallets would pose "potential high risks" or represent a greater "technological and regulatory complexity" in mitigating ML/TF risks compared to other digital asset solutions on the market.

Firstly, **the effectiveness of combating ML/TF crimes is actually enhanced when cryptocurrencies are involved**. Unlike traditional fiat money, cryptocurrency transactions are inherently traceable due to the public nature of blockchain technology. Every transaction processed on a blockchain is permanently recorded, immutable, and cannot be altered or deleted. This stands in stark contrast to fiat currency, where records are private, siloed within thousands of financial institutions spread across scores of legal jurisdictions, and can be easily manipulated, making it difficult, expensive and time consuming for authorities to trace illicit cash flows. Despite its vastly superior transparency, there remains a misconception that cryptocurrencies provide complete anonymity for criminal activities. However, Bitcoin transactions, for instance, offer pseudonymity rather than absolute anonymity, as each transaction is linked to a unique address on the public blockchain. This pseudonymity is the only privacy protection afforded to blockchain users, and even this meager degree of privacy is lost the moment one links their blockchain address with an account at a regulated intermediary. This attribution of a blockchain address with a human identity is permanent and irreversible.

In this regard, the immutable and transparent nature of public blockchains equips law enforcement agencies with significantly enhanced tracking capabilities compared to traditional fiat currency transactions. The use of self-hosted wallets does not alter that situation, thereby not introducing any additional ML/TF risk compared to other digital asset management tools available on the market. At its core, a digital asset wallet consists of a public blockchain address and a private key. A private key is a unique string of random characters. It is all one needs to custody and control one's digital assets. Thus, an self-hosted wallet can be as simple as a so-called "brain wallet" (committing the private key to memory), a "paper wallet" (writing it down on a piece of scrap paper), or a physical wallet (for example, inscribing it into some physical medium like a piece of metal). Of course, we at Ledger believe the safest way to protect one's private key is with our Ledger hardware devices.

In addition, there is a significant risk to the EU of creating regulatory and supervisory discrepancies with the internationally-accepted approach to self-custody by applying additional requirements that would go beyond the Financial Action Task Force (FATF) standards and the practices observed in like-minded jurisdictions such as the United Kingdom (UK). His Majesty's Treasury states unequivocally in its Amendments to the Money Laundering, Terrorist Financing and Transfer of Funds Regulations that, "The government does not agree that unhosted wallet transactions should automatically be viewed as higher

risk; many persons who hold cryptoassets for legitimate purposes use unhosted wallets due to their customisability and potential security advantages (e.g. cold wallet storage), and there is not good evidence that unhosted wallets present a disproportionate risk of being used in illicit finance."

Furthermore, HM Treasury's stance on self-hosted wallets reflects a balanced perspective that acknowledges the innovation offered by cryptoassets and the unique advantages enabled by self-custody. In keeping with this understanding, UK crypto firms are directed to apply a risk-based approach in determining when additional customer due diligence is appropriate. EU CASPs should also be trusted to make these determinations free of the biased assumptions built into the Guidelines.

3. Law-abiding citizens are likely to be disproportionately harmed by the proposed Guidelines

Ledger questions some of the requirements outlined in Regulation 2023/1113 and the proposed EBA's Guidelines, particularly in relation to the fundamental EU principles of necessity and proportionality. Such requirements appear to unduly target crypto assets and transactions when compared to traditional financial instruments, despite the inherent higher ML/TF risks associated with the latter, as highlighted above. **This is likely to pose significant harm to law-abiding citizens in the EU**.

While Ledger is fully committed to fighting against ML/TF risks, we are concerned that some of the transparency/reporting requirements imposed on crypto transactions would put EU citizens at risk by facilitating the collection of personal information of crypto users. The use of financial transaction data coupled with personal data could be used by criminals for nefarious purposes. With a blockchain address and a home address, criminals could see exactly how much crypto a specific individual holds and choose whether to attack that person virtually (through hacking, phishing or any other online fraud) or physically (by means of robbery, kidnapping, or extortion). Not only do such measures overlook the fundamental right to privacy enshrined in the General Data Protection Regulation (GDPR) and Universal Declaration of Human Rights, but they would also undermine the safety and security of EU citizens in the digital realm whilst exposing them to greater risk of crime.

In addition to reducing the financial freedom of EU citizens, such measures would also weaken consumer protection and compromise financial inclusion. Underprivileged communities are far more likely to be unbanked or underbanked compared to higher-income individuals. Even the FATF has acknowledged that its AML standards contribute to limiting access to basic financial services for these individuals. While self-hosted wallets on public blockchains offer a cost-effective solution for these marginalised populations to access financial services, the Guidelines' efforts to discourage the use of self-hosted wallets will further deprive the underprivileged of a valuable tool well-suited to their specific needs.

Finally, we are concerned that the Guidelines' stigmatisation of self-hosted wallets will lead EU CASPs to make faulty or erroneous assumptions about the risk level of routine transactions, and that this will cause direct financial harm to EU citizens. As demonstrated above, the volume of illicit blockchain transactions is already vanishingly small and, as correctly recognised by the UK Treasury, there is no evidence that self-hosted wallets present an increased risk. Many law-abiding citizens use self-hosted wallets everyday for a variety of lawful purposes. However, the Guidelines will force all EU financial institutions to automatically view such lawful transactions by law-abiding citizens as "high risk." We fear that this will cause ordinary transactions to be blocked, denied, or delayed by EU financial institutions, and that some transactions may become "stuck." Without good communication from these financial institutions about what has happened to their transactions and why, many EU citizens will be left to try to solve these problems on their own. This could cause them to miss making payments they owe on time, or defaulting on obligations, causing real and lasting harm to their financial record and even impairing their access to everyday necessities such as food or housing. Such harms are hardly necessary or proportionate to the goal of further reducing the already miniscule fraction of a fraction of blockchain transactions that may be illicit.

4. <u>The Guidelines will place the EU at a competitive disadvantage vis-à-vis other markets</u>

Ledger fears that the stringent rules proposed under Regulation 2023/1113 and the EBA's draft Guidelines will negatively hinder the key principles of proportionality, privacy and financial freedom. **We also believe that it will stifle innovation and economic growth of the blockchain and digital asset industry in the EU**.

By imposing burdensome compliance requirements on Crypto Asset Service Providers (CASPs) and restricting interactions with decentralised finance (DeFi) protocols and self-hosted wallets, the new rules will create barriers to entry for startups and small businesses operating in the crypto space. This could lead to a flight of talent and capital to jurisdictions that have taken more reasonable positions on these issues, thereby undermining the EU's competitiveness in the global digital economy. This would undoubtedly place Europe at a competitive disadvantage versus the United States, Asia, emerging markets, and even the UK. Entrepreneurs, innovators and the existing blockchain industry in Europe will have even more incentive to leave or grow their businesses elsewhere.

As a French-based company with a long-standing record of and commitment to helping the European digital economy to develop and grow, we see this as a major setback for EU competitiveness.

Our specific comments on several elements of the proposed draft Guidelines are set out further below.

## Guidelines 8. on Transfers of crypto-assets made from or to self-hosted addresses (Article 14 (5) and Article 16 (2) of Regulation (EU) 2023/1113)

As outlined above, Ledger strongly rejects the assumption that transfers involving self-hosted wallets would be of higher risk in relation to ML/TF, and thus be subject to a discriminatory treatment compared to other digital asset management solutions. We would like to stress once again that self-hosted wallets are simply a way to secure individuals' access to their private key. This does not affect in any way the transparency of transactions processed on the public blockchain which cannot be altered or deleted, and as such do not offer an opaque way for criminals to hide ML/TF practices as they do today with illicit cash flows.

In this regard, **we advocate for transfers involving self-hosted wallets to be assessed no differently from any other type of transaction. Self-hosted wallet transactions should be assessed based on the CASP's or financial institution's overall risk framework, which may include objective quantitative criteria such as transfer size, linked transfers, or frequency,** but which would allow the CASP or financial institution to consider the totality of information available to it without automatically leading to predetermined conclusions. **This would ensure that self-hosted wallets are not discriminated against, and would also alleviate the undue and disproportionate burden on CASPs when considering such transactions**.

Moreover, Ledger calls on the EBA to replace its prescriptive, rules-based approach with a more proportionate risk-based approach when considering the additional requirements proposed under Guideline 8. Some of the proposed measures appear to be too burdensome, complicated to put into practice, and costly for CASPs and would benefit from a more pragmatic consideration. We believe that the industry would be in a better position to effectively fight against ML/TF risks in an efficient and sustainable manner with the development of effective Travel Rule solutions based on standardised data fields and messaging. Such a crypto-asset industry-led standard setting initiative could mirror existing messaging and reporting data standards in the traditional banking sector.

## Conclusion

In conclusion, Ledger would like to stress that the EU crypto-asset industry can play a pivotal role in ensuring that it is not used for ML/TF considerations, as long as it does not suffer from a biased, discriminative approach compared to the traditional financial system. The transparent and sound nature of blockchain and cryptocurrencies can make the fight against ML/TF crimes more effective, and we would encourage the proposed EBA Guidelines to reflect that.

Overall, **Ledger is of the view that the EBA Guidelines should adopt a flexible, risk-based approach when analysing the risks associated with self-hosted wallets** by entrusting CASPs and financial institutions to develop their own compliance and due diligence measures for conducting risk assessments. This would help build a pragmatic and effective regulatory framework in the EU that balances innovation with the need for financial integrity.


Seth Hertlein

Global Head of Policy

Ledger

Julien David

Head of Regulatory Affairs, EMEA

Ledger