October 17, 2025

VIA REGULATIONS.GOV

Julie Lascar, Director,
Office of Strategic Policy,
Terrorist Financing and Financial Crimes, Department of Treasury

Re: Response to Department of the Treasury's Request for Comment on Innovative Methods to Detect Illicit Activity Involving Digital Assets

The DeFi Education Fund, Paradigm Operations LP, and Solana Policy Institute appreciate the opportunity to submit this response (the Response) to the Department of the Treasury's (Treasury's) Request for Comment on Innovative Methods to Detect Illicit Activity Involving Digital Assets (RFC).

DeFi Education Fund (DEF) is a U.S.-based nonpartisan research and advocacy nonprofit that advocates for sound policy for decentralized finance (DeFi).

Paradigm Operations LP (Paradigm) is a U.S.-based investment firm that backs entrepreneurs building innovative crypto companies and protocols, including those developing non-custodial, peer-to-peer software enabling DeFi.

Solana Policy Institute (SPI) is a U.S.-based nonpartisan nonprofit focused on educating policymakers on how decentralized networks like Solana are the future of the digital economy and why those building on and using them need legal certainty to flourish.

I. Introduction

The purpose of a financial integrity regime—consisting of anti-money laundering (AML), countering the financing of terrorism (CFT), and sanctions—is to protect people from harm by safeguarding the financial system from illicit use. This regime plays a critical role in maintaining the stability and trustworthiness of global financial markets and is accomplished through a framework of controls, policies, and procedures, which is established by (i) the Bank Secrecy Act (BSA) and its progeny for AML/CFT as well as (ii) the International Emergency Economic Powers Act (IEEPA) for sanctions and related transactional and asset-based restrictions. These foundational laws and regulations ensure that financial institutions implement robust measures to document, detect, and report suspicious activities, thereby contributing to broader national and international security efforts.

Without belaboring the specifics of the relevant statutes and regulations, the foundation of this framework focuses on requiring financial institutions to document, detect, report, and ultimately deter, illicit financial

activity. Importantly, the standard for covered financial institutions is not total elimination of risk (i.e., zero tolerance) but rather *reasonable* mitigation of risks that focuses on priorities while allowing individuals and businesses to access the financial system.[1] This balanced approach recognizes that overly stringent measures could inadvertently exclude legitimate users, stifling economic growth and innovation, while prioritizing high-risk areas such as high-value cross-border transactions or activities involving high-risk jurisdictions.[2]

Over the years—and in the absence of formal rules from policymakers and regulators—the digital asset industry has come together and taken proactive steps to identify and address the risks in the ecosystem by implementing increasingly effective risk mitigation measures. Notably, according to TRM Labs' 2025 Crypto Crime Report, in 2024, digital asset transaction volume grew to over $10.6 trillion, with illicit volume[3] dropping to $45 billion, representing 0.4% of overall crypto volume and a 51% decrease year over year.[4] Chainalysis, in its 2025 Crypto Crime Trends Report, reported an even lower estimate for illicit volume[5] at $40.9 billion, representing 0.14% of overall crypto volume.[6]

In contrast, the estimated annual amount of money laundered—without accounting for other illicit financial crimes—globally is 2-5% of global Gross Domestic Product (GDP), or $800 billion-$2 trillion USD.[7] For example, recently, the Wall Street Journal reported, "Chinese money launderers appear to have moved some $312 billion in illicit transactions through U.S. banks and other financial institutions in recent years to aid Mexican drug cartels and other criminals, the Treasury Department said."[8] On the one hand, these statistics underscore the persistent challenges in traditional finance, where opaque systems and centralized intermediaries

---

[1] U.S. Dep't of the Treas., AMLA: The Department of the Treasury's De-Risking Strategy, 22-23 (2023), https://home.treasury.gov/system/files/136/Treasury_AMLA_23_508.pdf ("Nonetheless, surveyed bank compliance officials indicated they vary in their level of comfort with applying the risk-based approach, and some believe that they face a risk of large fines from regulators for any failure in banking controls. Federal regulators, however, note that such fines are rare and that they are uniformly the result of total failure of AML/CFT compliance programs, not a result of more limited shortcomings that might result from a **reasonable application of the risk-based approach**.") (emphasis added).

[2] *Id*. at 1 ("De-risking undermines several key U.S. government policy objectives by driving financial activity out of the regulated financial system, hampering remittances, preventing low- and middle-income segments of the population, as well as other underserved communities, from efficiently accessing the financial system, delaying the unencumbered transfer of international development funds and humanitarian and disaster relief, and undermining the centrality of the U.S. financial system. As such, the strategy aims to provide potential solutions to promote financial inclusion by reducing barriers to the legitimate use of financial services as much as possible, while supporting efficient, safe, and affordable domestic and cross-border transactions.").

[3] Illicit volume is "based on the USD value of funds stolen in crypto hacks, combined with the USD value of transfers to blockchain addresses on Bitcoin, Ethereum, TRON, Binance Smart Chain, and Polygon that we have linked to entities in illicit categories such as fraud schemes, sanctions, and darknet marketplaces." TRM Labs, 2025 Crypto Crime Report (2025), https://www.trmlabs.com/reports-and-whitepapers/2025-crypto-crime-report.

[4] *Id*.

[5] Illicit volume includes (1) funds sent to addresses Chainalysis has identified as illicit and (2) funds stolen from crypto hacks. Chainalysis, 2025 Crypto Crime Trends: Illicit Volumes Portend Record Year as On-Chain Crime Becomes Increasingly Diverse and Professionalized (2025), https://www.chainalysis.com/blog/2025-crypto-crime-report-introduction/.

[6] *Id*.

[7] United Nations Office on Drugs and Crime, Money Laundering, https://www.unodc.org/unodc/en/money-laundering/overview.html (last visited Sept. 30, 2025).

[8] Dylan Tokar, *Chinese Money Launderers Are Moving Billions Through U.S. Banks*, The Wall Street Journal (Aug. 28, 2025), https://www.wsj.com/finance/regulation/chinese-money-launders-are-moving-billions-through-u-s-banks-cf617283.

dominate and, therefore, are able to facilitate large-scale illicit finance operations. On the other hand, they also evidence the relative effectiveness of financial integrity efforts in the digital asset ecosystem.

The digital asset ecosystem has seen such success in combating its illicit finance risks due to the suite of risk management solutions that has developed over the years to detect and deter high-risk activity. The focus of the Response will be on this suite of solutions, demonstrating how innovation in the sector has contributed to a safer environment for users. The structure of the Response is as follows:

- Section II provides a response to Question 1 in the RFC: specific illicit finance risks and vulnerabilities in the digital asset ecosystem.
- Section III provides a response to Question 5 in the RFC: tools currently being used for detecting illicit activity and mitigating the illicit finance risks discussed in Section II.
- Section IV concludes the Response by summarizing the progress made and the importance of innovative activity-based risk management tools in the digital asset industry.

II. Response to Question 1: Risks and Vulnerabilities in the Digital Asset Ecosystem

Cyber vulnerabilities—although not unique to the industry—pose the greatest risk for illicit financial activity in the digital asset ecosystem.

In contrast, one significant risk in traditional financial systems is the concentration of data and information (i.e., honeypots), which creates a vulnerability for targets and attacks and creates victims out of some of the very people that the financial integrity system is meant to protect from threats. Honeypots refer to centralized repositories of sensitive user data, such as personal identification, financial histories, and transaction records, which become attractive targets for cybercriminals due to their high value and potential for mass exploitation. Honeypots pose a serious risk to consumer privacy and financial security, since massive troves of highly personal information—that is nearly impossible to remediate—can get leaked to scammers.

The targeting of honeypots has become increasingly more common, affecting financial institutions that have some of the most robust security practices. For example, an external individual gained unauthorized access to 100 million of Capital One's potential and existing customers in the U.S., exposing the applicants' personal information (name, address, self-reported income, etc.) as well as the existing customers' Social Security numbers, linked bank accounts, payment history, among other sensitive information.[9]

In particular, honeypots are inherent in any risk mitigation solutions that necessitate Know Your Customer (KYC) measures, since they require the collection of personally identifiable information (PII) like government IDs, addresses, and biometric information, which, when stored centrally, amplifies the potential impact of a breach. Moreover, once a breach occurs, companies end up spending large sums of money to provide tracking

[9] Information on the Capital One Cyber Incident, https://www.capitalone.com/digital/facts2019/ (last visited Oct. 6, 2025).

and other remedial measures to try to minimize the damage to victims, even though the data is already gone, with the impact persisting for years thereafter.

Generally, decentralizing systems and hardening personal data are ways to mitigate the risk posed by concentration of data. Decentralization distributes data across networks, reducing single points of failure, while data hardening techniques, such as encryption, ensure that even if data is accessed, it remains unusable to unauthorized parties. There has also been a proliferation of privacy-enhancing verification methods such as zero-knowledge proofs, which provide a verifiable claim without exposing the underlying—and potentially sensitive—data. For these reasons, the primary risk in the digital asset ecosystem does not come from honeypots.

One of the central vulnerabilities in the digital asset ecosystem is standard cyber risk, which stems from: (i) bugs and vulnerabilities in smart contracts or application code, which may be exploited by attackers or may result in accidental loss of funds; (ii) lack of standardization and fragmented technology stacks, which may lead to integration and compatibility issues; and (iii) dependency on third-party oracles or bridges, which may become critical points of failure or attack if not sufficiently secured or integrated. This vulnerability can arise from rushed development, lack of thorough auditing, or evolving attack vectors that exploit unforeseen weaknesses in smart contracts or protocols.

Illicit actors can exploit these vulnerabilities in the underlying software to hack the technology and steal user funds. For example, in 2022, an attacker exploited a bug in the Wormhole bridge smart contracts, which allowed the attacker to generate and steal $611 million USD worth of cryptocurrency from the bridge, resulting in one of the largest crypto exploits to date.[10] However, risks stemming from the software itself are not unique to the digital asset ecosystem. In fact, any technological system will create a cyber risk vector. For example, First American Financial exposed over 885 million sensitive documents—including bank details, mortgage records, tax documents, Social Security numbers, and driver's licenses dating back to 2003—on its website due to a design flaw, allowing unauthorized access without passwords by simply modifying document links/addresses (URLs).[11] The critical difference between the Wormhole and the First American Financial exploits is that the First American Financial incident exposed hundreds of millions of incredibly sensitive personal and financial data. The Wormhole incident—involving a cyber attack to infrastructure, rather than accounts—fortunately, did not.

In addition to cyber risk, the digital asset ecosystem also experiences use risk, operational risk, and centralization risk. For users, mistakes such as poor password practices; phished, exploited, or lost private keys; or funds sent to the wrong address can have substantial consequences. For companies, operational security risks include compromised private keys (through phishing or social engineering), poor infrastructure protections,

[10] Rekt Leaderboard, https://rekt.news/leaderboard (last visited Sept. 30, 2025).

[11] AJ Dellinger, *Understanding The First American Financial Data Leak: How Did It Happen And What Does It Mean?*, Forbes (May 26, 2019), https://www.forbes.com/sites/ajdellinger/2019/05/26/understanding-the-first-american-financial-data-leak-how-did-it-happen-and-what-does-it-mean/.

vulnerabilities in Web2 dependencies (such as cloud service hacks), and inadequate access controls for staff or contractors. Insufficient decentralization (like too few validators controlling a bridge or protocol) and vulnerabilities in software supply chains (e.g., using vulnerable third-party code) can also be causes of major loss events.

Effectively addressing illicit finance risks requires risk mitigation solutions that focus on the needs and realities of the technology underpinning the digital asset ecosystem. Unlike traditional finance, where opacity can hide illicit flows, blockchains offer inherent traceability, allowing for proactive monitoring and rapid response to threats when combined with advanced analytics and collaborative networks.

III. Response to Question 5: Suite of Solutions Leading to the Success of Industry in Addressing Illicit Finance Risks

Best practice in the digital asset ecosystem is to not rely on a single tool for risk mitigation but instead use a suite of solutions—i.e., a collection of software that performs different functions—to address illicit finance risks. This multi-layered approach ensures comprehensive coverage, combining preventive, detective, and responsive measures to adapt to the dynamic nature of threats in a decentralized environment. It also removes single points of failure, making the overall system more resilient against illicit finance risk.

As noted in the RFC, these solutions, at their core, "leverage[ ] public blockchain data and blockchain analytics to trace and attribute illicit activity in digital assets" and use data to "evaluate high-risk counterparties and activities, analyze transactions across multiple blockchains, trace or monitor transaction activities, and identify patterns that indicate potential illicit transactions."[12] This data-driven methodology leverages the transparency of blockchains to provide insights that are often real-time and verifiable, enabling stakeholders to act swiftly.

The suite of solutions can, broadly, be organized into three buckets: (i) risk assessment and defensive blocking, (ii) proactive user-protection tools, and (iii) threat information coordination, which are all discussed below.

a. Risk Assessment and Defensive Blocking

Risk assessment solutions focus on evaluating and identifying potential threats in the digital assets ecosystem through reputational due diligence—i.e., analyzing wallet histories, token legitimacy, smart contract vulnerabilities, and transaction patterns—and attributing a "risk score" to the wallets, tokens, and smart contracts. These tools employ advanced algorithms, including machine learning, to scan historical data and flag anomalies, such as unusual transfer volumes or connections to known illicit addresses. Based on these risk scores, users can make informed decisions prior to engaging in transactions, reducing the likelihood of falling victim to scams or interacting with sanctioned entities.

More sophisticated tools may implement additional functionalities, such as detecting address poisoning, which is a scam where attackers inject fake addresses into a user's transaction history in hopes the user will copy and

[12] RFC at 5.

paste the wrong address when transacting. A January 2025 study found over 270 million poisoning attempts on Ethereum and BNB Chain between July 1, 2022, and June 30, 2024. Of those, 6,000 attempts were successful, leading to losses over $83 million.[13] This highlights the prevalence of such tactics and the need for automated detection to protect users, which the digital asset ecosystem develops and integrates to meet new security challenges. Examples of risk assessment solutions include: Dapp.Webacy.com,[14] TokenSniffer.com, and ScamSniffer.io.

Defensive blocking solutions act as proactive barriers that prevent harmful actions from executing, such as screening transactions in real-time, enforcing specific pre-transaction logic (e.g., ensuring regulatory compliance in privacy bridges), or detecting and halting bots, malicious users, or exploits. By integrating directly into protocols or user interfaces, these tools can automatically reject or flag suspicious activities, providing an immediate layer of defense against rapid exploits. These tools integrate into applications, bridges, or networks to block threats like scams, inorganic behaviors, or unauthorized access before they cause damage. Examples of defensive blocking solutions include: Predicate.io, Firewall.Forta.Network, and Honeypot.run.

Moreover, many user interfaces/websites (front ends) already build-in such functionalities. For example, Uniswap Labs,[15] 1inch,[16] and MetaMask[17] use BlockAid, which alerts users to potentially malicious transactions, scams, etc. through the user interface. Traditional on-chain analytics tools like Chainalysis, TRM, and Elliptic can also provide standard wallet screening and fraud prevention and are commonly used in front ends. Furthermore, APIs can be integrated into blockchain search hubs (blockexplorers, such as Etherscan) for real-time risk intelligence about any address on the chain, which any user can access. In addition, such APIs can also be integrated into self-custody solutions such as wallets for transaction simulation and risk alerts.

Products and services that implement user-empowering risk detection tools are more competitive in the digital asset ecosystem because users prefer using them over other products that lack such protection. This market-driven incentive encourages widespread adoption, fostering a cycle of innovation and improved security standards across the industry.

---

[13] Taro Tsuchiya et. al., Blockchain Address Poisoning (Carnegie Mellon University, 2025), https://arxiv.org/abs/2501.16681.

[14] Webacy diligence and decisioning protocol and cybersecurity firm, Trugard, developed an artificial intelligence-based system for detecting crypto wallet address poisoning, leveraging a supervised machine learning model trained on live transaction data in conjunction with on-chain analytics and behavioral context that demonstrated a success score of 97%, tested across known attack cases. This system adapts to evolving threats by incorporating synthetic data simulations, ensuring high efficacy in real-world scenarios. Adrian Zmudzinski, *AI Tool Claims 97% Efficacy in Preventing 'Address Poisoning' Attacks*, Cointelegraph (May 21, 2025), https://cointelegraph.com/news/ai-system-has-97-claimed-efficacy-in-preventing-address-poisoning-attacks.

[15] *New Token Warnings and Labels on Uniswap Web and Wallet*, Uniswap Labs Blog (Dec. 19, 2024), https://blog.uniswap.org/new-token-warnings.

[16] Ezra Reguerra, *1inch Partners with Blockaid to Combat DeFi Fraud and Cyber Threats*, Cointelegraph (June 20, 2024), https://cointelegraph.com/news/1inch-blockaid-partnership-defi-security.

[17] Megan Dias, *MetaMask Security Alerts by Blockaid: The New Normal for a Safer Transaction Experience*, MetaMask News (Feb. 20, 2024), https://metamask.io/news/metamask-security-alerts-by-blockaid-the-new-normal-for-a-safer-transaction.

b. Proactive User-Protection Tools

Proactive transaction simulation solutions–through front ends and wallets—simulate blockchain transactions before they are executed on-chain, predicting potential outcomes such as asset transfers, approvals, or interactions with smart contracts. By modeling the effects of a transaction in a safe environment, these tools can uncover hidden risks, such as infinite approvals that could drain wallets or interactions with phishing contracts. They assess risks like scams, malicious approvals, unauthorized access, and policy violations, providing warnings and automated recommendations to users before any funds are committed. Examples of these solutions include Hypernative.io, WalletGuard.app, Fordefi.com, and Blowfish.xyz.

c. Threat Information Coordination

Threat information coordination solutions facilitate real-time collaboration and intelligence sharing among the digital asset ecosystem, law enforcement, security researchers, and other stakeholders to combat digital asset crimes. By creating centralized, yet secure, platforms for reporting and dissemination, these tools enable a collective defense mechanism that amplifies individual efforts. These platforms enable verified participants to flag suspicious activities (e.g., illicit wallet addresses or transactions), propagate alerts across networks, and coordinate rapid responses to prevent fraud, hacks, or money laundering before funds are cashed out or laundered, enhancing ecosystem-wide security.

Examples of these solutions include: the Security Alliance (SEAL)[18] and TRM Labs Beacon Network.[19] SEAL is a nonprofit coordination center for crypto threat intelligence sharing, emergency response, and industry security standards development that focuses on rapid response to exploits and threat information dissemination through SEAL 911, a free service supported by industry contributors.[20] The Beacon Network is also an industry collaboration that emphasizes sharing attributions of illicit addresses to proactively stop illicit funds before they are withdrawn: "it enables verified investigators to flag addresses linked to financial crime, immediately alerting exchanges and triggering risk-based responses."[21]

IV. Conclusion

The most significant action the Treasury can take in addressing illicit finance risks in the digital asset ecosystem is further empowering the progress already made in risk management that led to a 51% decrease in illicit volume, year over year.[22] Even a fraction of that level of successful risk mitigation would be major news in the traditional finance system. However, as bad actors evolve, so does the need to constantly improve tools and threat indicators, which Treasury is well-placed to support.

[18] Security Alliance, https://www.securityalliance.org/ (last visited Sept. 30, 2025).
[19] Beacon Network, https://www.trmlabs.com/beacon-network (last visited Sept. 30, 2025).
[20] Seal 911, https://www.securityalliance.org/seal-911 (last visited Sept. 30, 2025).
[21] Beacon Network, https://www.trmlabs.com/beacon-network (last visited Sept. 30, 2025).
[22] TRM Labs, *supra* note 3.

For example, Treasury can encourage innovative activity-based risk management tools that expand beyond blockchain analytics and into cybersecurity, rather than pushing the ecosystem to KYC systems that are easily spoofed and create significant additional risks through honeypots and breaches.

In addition, Treasury can also directly collaborate with the ecosystem by participating in information-sharing with SEAL and the Beacon Network. Such partnerships would bridge public and private sectors, enabling faster threat identification and response. In particular, integrating SEAL into private-public information sharing platforms—like the Illicit Virtual Assets Notification (IVAN) platform that MITRE is developing for the U.S. Government and private sector actors[23]—would provide a critical dissemination to SEAL's existing pathways for rapid response to address major exploits. This would mirror the way that Treasury's Office of Cybersecurity & Critical Infrastructure Protection (OCCIP) interfaces with the industry-assembled Financial Services Information Sharing and Analysis Center (FS-ISAC),[24] while matching the speed of decentralized finance.

Some law enforcement entities already work with SEAL and Beacon Network, but Treasury could help shepherd the connection between the digital asset ecosystem, IVAN, and Treasury's own threat indicators from FinCEN, the Financial Intelligence Unit, and OCCIP. This would help move from generalized trends and typologies in alerts to directly actionable information that could proactively stop illicit finance in the way that FinCEN's Rapid Response Program does in the traditional finance world, which has reactively facilitated the recovery of more than $1.1 billion for U.S. victims from 2015 to 2022.[25]

Through the above two actions—enabling innovative risk management solutions and participating in information sharing with the industry—Treasury can have the opportunity to improve outcomes along both axes: more success and less vulnerability. However, this involves recognizing that the digital asset ecosystem requires a *different* risk management approach than the one that has traditionally been used for combating illicit financial activity, one that leverages transparency and technology rather than centralized control and creation of honeypots.

On behalf of DEF,	On behalf of Paradigm,	On behalf of SPI,
Amanda Tuminelli, Executive Director & Chief Legal Officer	Justin Slaughter, VP, Regulatory Affairs	Patrick Wilson, General Counsel

[23] *Illicit Virtual Asset Notification Public-Private Partnership*, MITRE News (Oct. 2, 2024), https://www.mitre.org/news-insights/news-release/illicit-virtual-asset-notification-public-private-partnership.

[24] Safeguarding the Global Financial System by Reducing Cyber Risk, https://www.fsisac.com/ (last visited Sept. 30, 2025).

[25] Fin. Crimes Enf't Network (FinCEN), FIN-2022-FCT1, Fact Sheet on the Rapid Response Program (RRP) (2022), https://www.fincen.gov/system/files/shared/RRP%20Fact%20Sheet%20Notice%20FINAL%20508.pdf.