Submitted electronically via Federal eRulemaking Portal

October 17, 2025

Julie Lascar
Director, Office of Strategic Policy, Terrorist Financing, and Financial Crimes
U.S. Department of the Treasury
1500 Pennsylvania Avenue, NW
Washington, D.C. 20220

RE: Request for Comment on Innovative Methods to Detect Illicit Activity Involving Digital Assets

Dear Ms. Lascar:

The Independent Community Bankers of America ("ICBA")[1] welcome this opportunity to respond to the U.S. Department of the Treasury's ("Treasury") request for comment ("RFC") on innovative methods to detect and deter illicit activity involving digital assets. Although most community banks currently have limited direct exposure to digital assets, whether through custodial services or various stablecoin-related activities, they remain on the frontlines in the ongoing fight against fraud and scams.

Background

Stablecoins are a rapidly growing category of digital assets that, in contrast with volatile cryptoassets like bitcoin, seek to maintain a stable value. As such, they have become part of the burgeoning world of decentralized finance ("DeFi") applications that attempt to replicate traditional banking services and products. As of October 2025, there is more than $300 billion worth of stablecoins in circulation.[2]

These stablecoins use a variety of mechanisms and assets to maintain a stable value, with many using cash deposits and US Treasurys as the basis for their reserves. Stablecoins serve

[1] The Independent Community Bankers of America® has one mission: to create and promote an environment where community banks flourish. We power the potential of the nation's community banks through effective advocacy, education, and innovation. As local and trusted sources of credit, America's community banks leverage their relationship-based business model and innovative offerings to channel deposits into the neighborhoods they serve, creating jobs, fostering economic prosperity, and fueling their customers' financial goals and dreams. For more information, visit ICBA's website at https://www.icba.org/.
[2] DeFiLlama, *Stablecoins*, (last accessed Oct. 13, 2025), https://defillama.com/stablecoins.

as a nexus between the banking system and the crypto ecosystem. This nexus has attracted significant attention from policymakers due to concerns about stablecoin failures leading to runs that could harm the US financial system. There is also increasing evidence that criminals are turning to stablecoins to serve as a "shadow banking" system that enables quick payments and circumvents the anti-money laundering processes and procedures of traditional banks and payments providers.

In July 2025, Congress passed the Guiding and Establishing National Innovation for U.S. Stablecoins ("GENIUS") Act to establish a legal and regulatory framework for payment stablecoins, a digital asset that is designed to be used as a means of payment or settlement. The rulemaking process to implement the Genius Act begins with this RFC which "supports the Administration's policy of supporting the responsible growth and use of digital assets."[3]

ICBA General Comments

Financial institutions ("FIs") can have trouble identifying illicit activities in digital assets because the ecosystem was designed for secrecy and to bypass the traditional financial system. Indeed, the concealment of one's identity is a foundational goal, and as such is a foundational challenge. It is unreasonable to expect FIs to bear the brunt for detecting illicit activity in digital assets, especially when so much of it comes from those acting at the behest—or with the tacit approval—of adversarial nations.

In fact, the world's global anti-money laundering watchdog, the Financial Action Task Force ("FATF") recently reported that "most on-chain illicit activity now involves stablecoins."[4] FATF held that fraud is now a "major predicate for money laundering"[5] and "one of the fastest growing threats on a global scale."[6] ICBA and our member banks emphatically agree with these assessments. Increasingly, community bankers report that their customers fall victim to sophisticated crypto fraud and scams perpetrated by cybercriminals and large criminal syndicates operating overseas. In response, they are developing additional resources to educate consumers and are dedicating more time and resources to ensure their staff are trained on the latest criminal techniques. But there is only so much a single institution can do to challenge a seemingly endless cascade of bad actors and illicit activity.

---

3 Exec. Order No. 14178, *Strengthening American Leadership in Digital Financial Technology*, 90 Fed. Reg. 8647, (Jan. 31, 2025).
4 FATF, *Targeted Update on Implementation of the FATF Standards on Virtual Assets and Virtual Asset Service Providers,* (June 26, 2025), https://www.fatf-gafi.org/en/publications/Fatfrecommendations/targeted-update-virtual-assets-vasps-2025.html.
5 Financial Action Task Force, *Explanatory Note for Revised R.16*,(June 18, 2025), https://www.fatf-gafi.org/content/dam/fatf-gafi/recommendations/Explanatory%20note%20for%20revised%20R.16.pdf.coredownload.pdf.
6 Financial Action Task Force, *FATF Updates Standards on Recommendation 16 on Payment Transparency*, (June 18, 2025), https://www.fatf-gafi.org/en/publications/Fatfrecommendations/update-Recommendation-16-payment-transparency-june-2025.html.

Most community banks are not currently offering digital asset products and services. Therefore, our comments primarily focus on illicit finance trends observed by community banks in their role as the key providers of financial services on Main Street. As more community banks start to explore digital assets and the regulatory framework develops in step, we look forward to more opportunities to provide specific feedback on the deployment of innovative technologies to support monitoring and reporting requirements.

Regulatory Landscape

Unresolved Domestic Regulatory Framework

Treasury seeks input from banks on innovative ways to detect and mitigate illicit financing involving digital assets. Before imposing detection requirements on banks, Treasury should first work with the appropriate federal agencies and international counterparts to evaluate and define how digital assets will be regulated. The GENIUS Act is a start within the United States, but a comprehensive framework coupled with robust enforcement powers needs to be developed before FIs are expected to mitigate illicit uses or execute their U.S. anti-money laundering/countering the financing of terrorism ("AML/CFT") responsibilities.

Treasury is charged with promulgating regulations to implement the Act. Recently, the agency released an advance notice of proposed rulemaking on developing regulations to carry out Section 4(a)(5) of the Act.[7] ICBA believes the GENIUS Act final rule should be issued before asking stakeholders for innovative ideas on mitigating illicit uses and therefore contend the underlying request for which this letter is based is premature.

Treasury asserts that "[i]nnovative tools are critical to advancing AML/CFT and sanctions compliance. FIs can leverage these tools to protect the digital asset ecosystem from misuse by illicit actors like drug traffickers, fraudsters, ransomware attackers, terrorist financiers, Iranian regime-linked sanctions evaders, and Democratic People's Republic of Korea cybercriminals."[8] ICBA agrees that innovative tools are critical, but we depart in our agreement as it pertains to the agency's view in how community banks can leverage such tools. The view overlooks the challenges small community banks face in accessing the necessary tools. Next, the assertion fails to acknowledge the decentralized, borderless, instantaneous, and secretive nature of digital assets which could render efforts void. Finally, the view fails to recognize that critical questions about the application of AML/CFT (and OFAC) have not yet been settled. Indeed, we hope that the final rule implementing the GENIUS Act will resolve these concerns. But for now, suggestions on innovative tools to advance AML/CFT and sanctions compliance are

[7] GENIUS Act Implementation, 90 Fed. Reg. 45159, (proposed Sept. 19, 2025).
[8] Request for Comment on Innovative Methods to Detect Illicit Activity Involving Digital Assets, 90 Fed. Reg. 40148 (Aug. 18, 2025).

speculative and premature at best.

Furthermore, anonymity tools like convertible virtual currency ("CVC") mixing are designed to dilute or eliminate transactional trails. CVC mixers can use different methods to obscure transactional trails, such as pooling multiple people's crypto assets together into a single wallet, thus concealing the identities of the parties or creating single-use accounts in a series of transactions that distort the destination of the transferred funds. Unsurprisingly, these capabilities have turned crypto mixers into one of the most important elements in money laundering operations throughout the world. The proliferation of these capabilities has confounded the government's mitigation efforts, complicated law enforcement investigations, and has directly harmed the US economy and countless consumers.

FIs are the most regulated industry in the US. In the ordinary course of business, they are expected to conduct surveillance on customer accounts, file suspicious activity reports when warranted, and mitigate harm from financial crimes. Expecting FIs, especially community banks, to perform these same duties on digital assets that are designed for anonymity and near instantaneous transfers, should not be the focus during the build-out of a comprehensive and robust regulatory framework.

International Regulatory Arbitrage Remains a Concern

As payment instruments that circulate on public distributed ledgers, stablecoins hold the promise of delivering faster and more efficient payments. Proponents believe that stablecoins are particularly well-suited to address pain points in cross-border payments, and they claim that cryptographically secured ledgers enhance tracing capabilities to support financial crime investigations.

The reality, however, is that criminals have excelled in finding creative ways to exploit the abilities of digital asset technologies and the wide regulatory gaps across the globe. Indeed, the latest FATF survey revealed an unsettling fact: "Three-quarters of FATF Global Network countries were evaluated to be non-compliant or partially compliant with international standards on virtual assets and virtual asset service providers ("VASPs")."[9] These gaps allow cybercriminals to operate from many jurisdictions with complete impunity. ICBA strongly agrees with FATF's grim assessment that "virtual assets are inherently international and borderless, meaning a failure to regulate VASPs in one jurisdiction can have serious global consequences."[10]

[9] Financial Action Task Force, *FATF Report: Complex Proliferation and Sanctions Evasion Schemes,* (June 9, 2025), https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Complex-PF-Sanctions-Evasions-Schemes.pdf.coredownload.inline.pdf. .
[10] FATF, *supra* note 3.

Stablecoins, and the wider decentralized ecosystem in which they circulate, afford cybercriminals with unique capabilities. In mere seconds, bad actors can exchange stablecoins with a decentralized exchange into other cryptoassets, quickly negating any potential for an issuer to seize and freeze in compliance with a legal order. Bad actors can also make an infinite number of wallets and execute thousands of complex transactions to obfuscate their criminal trails. These capabilities, combined with gaping holes in global regulation, permit criminals to swiftly move illicit funds across borders, with the safe knowledge that their home jurisdiction either lacks the will or manpower to bring them to justice.

While we encourage the administration to continue its efforts to implement a robust regulatory framework to address illicit uses of payment stablecoins, we caution that any effort will be limited so long as other countries fail to act. The US should leverage its position as a leader in digital assets to work with important international bodies, such as the Financial Stability Board and FATF, to encourage wider adoption and implementation of effective regulatory models and support emerging economies with training and other resources to aid in the investigation and prosecution of crypto criminals.

Emerging Threats and Enforcement Challenges

North Korea's Threat Demands Effective Government Actions

As the Treasury Department works to develop and implement regulations to support payment stablecoins, we urge policymakers to focus on the considerable threat posed by North Korea. North Korean cybercriminals have repeatedly executed skillful and daring thefts to acquire resources to bolster the regime's weapons of mass destruction program.

In February, North Korean hackers stole approximately $1.5 billion worth of ether from the crypto exchange ByBit.[11] This attack, which the FBI soon attributed to TraderTraitor operatives of the North Korean regime, ranks as the single largest heist of all-time.[12] In less than a month, nearly all the stolen ether was converted into bitcoin with the help of privacy wallets and mixers, most notably Wasabi, CryptoMixer, Railgun, and Tornado Cash.[13] As of June, FATF reported that only 3.8% of the stolen assets were recovered, underscoring not only the complexity of untangling obfuscated crypto transactions but also the speed with which investigators must act before trails run cold. The ByBit hack also illustrates the difficulties that even the largest and most sophisticated crypto firms experience when dealing with major hacks. The frozen assets largely resulted from bounty hunters who combed through intricate

---

[11] Joe Tidy, *North Korean Hackers Cash Out Hundreds of Millions from $1.5bn BuBit Hack,* BBC News (Mar. 9, 2025), https://www.bbc.com/news/articles/c2kgndwwd7lo.
[12] Federal Bureau of Investigation, *Alert Number: I-022625-PSA, North Korea Responsible for $1.5 Billion Bybit Hack,* (Feb. 26, 2025), https://www.ic3.gov/psa/2025/psa250226.
[13] Ben Zhou (@benbybit), X (Mar. 20, 2025, 4:19 AM),https://x.com/benbybit/status/1902635986259247207.

webs of mixed transactions. The fact that the largest and most sophisticated crypto entities must turn to volunteers to help track illicit transactions—and even then, still come up short—should stand out to policymakers as a glaring example of the inherent challenges of fighting criminal activity in the crypto ecosystem.

Although North Korea did not steal stablecoins with this attack, they routinely use stablecoins to help evade sanctions. For example, one independent researcher has detailed frequent stablecoin payments to North Koreans posing as IT workers for western companies. In fact, from January through July, his research uncovered $16.58 million worth of payments, much of it occurring with stablecoins.[14] This example highlights how easily North Korean agents can ignore sanctions that block them from cross-border payments provided by traditional financial entities, thus underscoring our broader concerns about the lack of an effective crypto regulatory regime.

ICBA urges policymakers to keep the threat posed by North Korea at the forefront of their rulemaking efforts to develop regulations to implement the GENIUS Act. The outsized threat posed by North Korea—not only in terms of its success in hacking but also the danger of its growing nuclear arsenal funded by stolen crypto—cannot be exaggerated. Community bankers cannot wage a fight against such a dedicated and well-equipped rogue nation by themselves. A threat of this nature demands a forceful response led by the US government focused on deterrence as opposed to detection.

Rising Crypto Fraud Losses

Americans are losing billions to crypto scams every year, and cryptocurrency now serves as the primary way that Americans lose money to fraud.[15] The 2024 IC3 report tallied 149,686 complaints totaling $9.3 billion in losses, with investment scams (commonly known as “pig butchering”) accounting for almost $6 billion of those losses.[16] Research by the University of Texas at Austin conservatively estimates that victims lost a total of $75 billion between January 2020 and February 2024.[17] Unfortunately, the true toll is much higher since many victims do not report their losses to authorities. In fact, the real losses stemming from crypto fraud equal, or potentially exceed, all other payment methods combined.

Against this backdrop, ICBA has repeatedly called for the US government to strengthen its legal and regulatory framework to confront significant fraud, money laundering, and evasion of

---

[14] ZachXBT (@zachxbt), X (July 2, 2025, 8:35 AM), https://x.com/zachxbt/status/1940388827392344261.
[15] Internet Crime Complaint Center, *Federal Bureau of Investigation: Internet Crime Report 2024*, (Apr. 23, 2025), https://www.ic3.gov/AnnualReport/Reports/2024_IC3Report.pdf..
[16] Id. at 35.
[17] Zeke Faux, *Pig-Butchering Scams Net More Than $75 Billion, Study Finds,* Bloomberg, (Feb. 29, 2024), https://www.bloomberg.com/news/articles/2024-02-29/pig-butchering-crypto-scams-netted-more-than-75-billion-new-study-finds?srnd=cryptocurrencies-v2.

sanctions enabled by cryptocurrency. Most recently, we were the only trade association to support FinCEN's proposal to designate the Cambodia-based financial conglomerate Huione as a primary money laundering concern and sever its connections to the US financial system.[18]

Huione created the world's largest illicit marketplace, and through its various arms, offered financial services to sustain extensive money laundering and fraud. For example, Haowang Guarantee—formerly Huione Guarantee—operates as a peer-to-peer e-commerce platform that "provides money laundering services to criminal organizations, helping them transfer the proceeds of investment frauds and other cyber scams to the legitimate banking sector undetected."[19] This subsidiary alone has reportedly processed at least $49 billion worth of cryptocurrencies since 2021. Huoine also launched a stablecoin in September 2024 that was deliberately designed without freezing capabilities, thereby making it a highly attractive asset to bad actors.[20] Additionally, FinCEN has found evidence that the Lazarus Group, North Korea's most notorious hacking group, has used Huione to move millions of dollars' worth of stolen crypto, including $35 million taken from a Japanese crypto exchange last year.[21]

Although FinCEN recently finalized its proposal, they acknowledge that Huione has continued its operations with little interruption. In the final rule, FinCEN shared that one blockchain analytics company identified $10 billion worth of stablecoin transactions between Huione wallets in the weeks immediately after the proposal was released.[22] This news comes on top of a recent report by Chainalysis indicates that Huione's cryptocurrency exchange only briefly paused operations before coming back to life with a new domain.[23] Its social media channels, especially those hosted on Telegram, still offer a variety of money laundering services.[24]

This apparent ability to shrug off some of the most severe regulatory actions speaks both to the growing capabilities provided by the crypto ecosystem and the lack of sufficient regulatory and supervisory powers in many parts of the world. This problem cannot be solved through stronger regulation, supervision, and oversight alone. As transnational criminal organizations expand their ability to execute devastating global scams and deepen their connections with rogue nations, action by the highest levels of national security organizations, bank regulators, foreign affairs departments, and law enforcement agencies is urgent.

---

[18] Special Measure Regarding Huione Group, as a Foreign Financial Institution of Primary Money Laundering Concern, 90 Fed. Reg. 18934-18949 (May 5, 2024).
[19] Id at 18934,18937.
[20] Id at 18934, 18942.
[21] Id at 18934,18940.
[22] Financial Crimes Enforcement Network, *Imposition of Special Measure regarding Huione Group, as a Foreign Financial Institution of Primary Money Laundering Concern*, (Oct. 14, 2025),https://www.fincen.gov/system/files/2025-10/Huione-Group-Final-Rule_0.pdf.
[23] Chainalysis, *Huione Carries On: Chinese-Language Platform's Persistence Reveals the Complexity of On-Chain Financial Crime Disruption*, (June 12, 2025), https://www.chainalysis.com/blog/huione-guarantee-still-active-despite-shutdown/.
[24] Id.

Legal and Policy Reform is Needed to Effectively Address Illicit Crypto Use

Blanche Memo Creates Double Standards

On April 7, Deputy Attorney General Blanche issued a memo ("Memo") to outline the Department of Justice's ("DOJ") new approach towards prosecutions involving digital assets.[25] Most notably, the Memo states that the DOJ "will no longer target virtual currency exchanges, mixing and tumbling services, and offline wallets for the acts of their end users or unwitting violations of regulations."[26] According to the Memo, the DOJ will continue to "prioritize cases involving use of digital assets in furtherance of unlawful conduct by cartels, Transnational Criminal Organizations, Foreign Terrorist Organizations, and Specially Designated Global Terrorists;" however, it will not "pursue actions against the platforms that these enterprises utilize to conduct their illegal activities."[27]

Community bankers are concerned that this policy will bifurcate the stablecoin ecosystem and contribute to an already unlevel playing field. Crypto exchanges will not be held responsible for the misdeeds of their users, while community banks will be held to a much higher standard and expected to address losses that customers may incur. This disparity will factor into community banks' decision-making processes as they weigh whether and/or how to engage in stablecoin activities following the passage of the GENIUS Act. We encourage policymakers to recognize that the same activity should be subject to the same regulation and consequences for all types of entities.

Policymakers Must Take Action on Mixers

The GENIUS Act requires payment stablecoin issuers to have the ability to "seize, freeze, burn, or prevent the transfer of payment stablecoins."[28] Some stablecoin issuers currently have capabilities to act on law enforcement requests and other legal orders to block stablecoins associated with illicit activity. While this capability can be a powerful tool for criminal investigators, it is limited by the fact that bad actors are aware of these abilities and often seek to quickly dispose of stablecoins for decentralized cryptoassets.

The crypto ecosystem currently provides bad actors with myriad ways to obfuscate transactions through various mixing technologies, including but not limited to, using single-use wallets, switching between two or more different cryptoassets ("chain hopping"), and pooling

---

[25] United States Department of Justice, *Ending Regulation by Prosecution*, Deputy Attorney General Todd Blanche, (Apr. 7, 2025), https://www.justice.gov/dag/media/1395781/dl?inline.
[26] Id.
[27] Id.
[28] Guiding and Establishing National Innovation for U.S. Stablecoins Act, 12 U.S.C. §§ 5901-5916.

cryptoassets from multiple users. In response to the growth of illicit actors exploiting these capabilities, the Financial Crimes Enforcement Network ("FinCEN") issued a notice of proposed rulemaking in 2023 to exercise its Section 311 authority to classify crypto mixing as a class of transactions that are a primary money laundering concern.[29] FinCEN argued that the illicit finance risks associated with crypto mixing called for enhanced reporting requirements for covered financial institutions that determined or suspected that a transaction involved mixing.

To date, this rulemaking remains unresolved, even as bad actors continue to exploit mixers and develop other innovative technologies to cover their tracks. The American government cannot stand by as North Korean cybercriminals and ransomware operators continue to rake in millions and then disappear into the shadows. We urge the administration to finalize the crypto mixer proposal as quickly as possible.

Conclusion

Thank you again for the opportunity to submit ICBA's concerns regarding trends in illicit finance involving digital assets. ICBA and our member banks remain open to exploring the potential capabilities of payment stablecoins, but their promise rests on the government's ability and willingness to deter the skyrocketing growth of illicit finance in the digital economy.

If you have any questions or concerns about ICBA's comments on payment stablecoins and illicit finance, please reach out to me at brian.laverdure@icba.org.

Sincerely,

/s/

Brian Laverdure
Senior Vice President, Digital Assets and Innovation Policy

[29] Proposal of Special Measure Regarding Convertible Virtual Currency Mixing, as a Class of Transactions of Primary Money Laundering Concern, 88 Fed. Reg. 72701, Oct. 23, 2023).