Submitted via Federal E-Rulemaking Portal

June 4, 2025

Financial Crimes Enforcement Network
P.O. Box 39
Vienna, Virginia 22183

RE: Special Measure Regarding Huione Group, as a Foreign Financial Institution of Primary Money Laundering Concern, Docket Number: FINCEN-2025-0004

Dear Sir or Madam:

The Independent Community Bankers of America ("ICBA")[1] strongly supports the Financial Crime Enforcement Network's ("FinCEN") decision to designate Huione Group ("Huione") as a primary money laundering concern, pursuant to its authority established by section 311 of the USA PATRIOT Act. The nation's community banks have long opposed the rise of crypto scams, and we have called for federal authorities to take stronger actions against the organizations and individuals responsible for these criminal actions. We recognize FinCEN's decision as a critical first step in a much larger campaign that is necessary to confront the growing use of cryptocurrency to defraud Americans.

Background

Americans are losing billions to crypto scams every year. The 2024 Internet Crime Complaint Center 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.[2] Unfortunately, the true toll is much higher since many victims do not report their losses to authorities. Research by the University of Texas at Austin conservatively estimates that victims lost a total of $75 billion between January 2020 and February 2024.[3]

---

[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 www.icba.org.*
[2] Federal Bureau of Investigation, 2024 Internet Crime Report, https://www.ic3.gov/AnnualReport/Reports/2024_IC3Report.pdf.
[3] Zeke Faux, "Pig-Butchering Scams Net More Than $75 Billion, Study Finds," Bloomberg, February 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.

As documented throughout this Notice of Proposed Rulemaking and detailed in numerous other government and media reports, transnational criminal syndicates have taken advantage of weak or non-existent governance in large swathes of Southeast Asia to establish compounds from which they conduct wide-scale fraud operations. More disturbingly, these compounds are populated with people who are kidnapped and forced to cultivate false relationships to trick victims into sending their life savings to scammers. The United Nations believes at least 220,000 individuals are currently held captive at these scam compounds.[4]

One of the most important entities that sustains these scam operations is the Cambodia-based financial conglomerate, Huione. As described throughout the NPRM, Huione supports illicit financial activities across its varied business arms. For example, Haowang Guarantee—formerly Huione Guarantee—operates as 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."[5] 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 to be unfreezable, thereby making it a highly attractive asset to bad actors.[6] 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.[7]

In recognition of the harm inflicted by these scams and Huione's central role in aiding scammers, FinCEN now seeks to use its authority granted by section 311 of the USA PATRIOT Act to classify Huione as a primary money laundering concern. FinCEN argues that it has reviewed sufficient public and non-public information to determine that "Huione Group is used to facilitate and promote money laundering, particularly in support of illicit financial activities connected to the Democratic People's Republic of Korea (DPRK) and Southeast Asia-based TCOs [transnational criminal organizations]."[8] Moreover, FinCEN notes that while Huione does seem to engage in some legal business activity, particularly in Cambodia, it "assesses that the benefits of any legitimate business activities Huione Group conducts are outweighed by the substantial money laundering risks it poses."[9] FinCEN concludes that a complete prohibition on opening or maintaining correspondent banking relationships for Huione is the only remedy that will safeguard the US financial system.

---

[4] United Nations Office on Drugs and Crime, "Casinos, Money Laundering, Underground Banking, and Transnational Organized Crime in East and Southeast Asia: A Hidden and Accelerating Threat," January 2024, https://www.unodc.org/roseap/uploads/documents/Publications/2024/Casino_Underground_Banking_Report_2024.pdf, 54.
[5] Financial Crimes Enforcement Network, "Special Measure Regarding Huione Group, as a Foreign Financial Institution of Primary Money Laundering Concern," Federal Register 90, no. 85 (May 5, 2024): 18937.
[6] Ibid, 18942.
[7] Ibid, 18940.
[8] Ibid, 18939.
[9] Ibid, 18942.

ICBA Comments

The designation of Huione as a primary money laundering concern is a commendable action; however, ICBA and its members urge FinCEN to consider additional actions to curtail the rapid rise of crypto scams. Although Huione is one of the largest payment providers for scammers and hackers associated with the DPRK, it is not the only one. Recent research by the blockchain analytics firm Elliptic revealed that another Telegram-based marketplace for scammers, Xinbi Guarantee, has facilitated $8.4 billion in transactions since 2022, primarily using the Tether stablecoin, which makes it "the second largest illicit online market to have ever operated".[10] This unsettling report shows that dark web markets and payment processors for scammers are like the fabled Hydra—FinCEN can cut off access to one by declaring it a primary money laundering concern, but bad actors will quickly move to other channels or create new outlets to continue their misdeeds. ICBA and community banks highlight this fact to underscore the need for a broader and comprehensive strategy to address the prominent roles of social media and telecom companies in the propagation of scams and other financial crimes.

To that end, ICBA encourages FinCEN to work with other relevant parties across the federal government to produce more comprehensive data about the scale of cryptocurrency fraud. Reports by victims remain scattered across multiple agencies, leaving both the federal government and the banking industry with an incomplete assessment that impairs their ability to take more proactive measures to detect and deter potentially fraudulent activity. Improved data collection efforts, coupled with better information-sharing between the government and private industry, are absolutely essential to maintain the safety of the US financial system and protect consumers from increasingly sophisticated and well-resourced bad actors.

Lastly, ICBA also calls on the federal government to consider additional punitive steps to curtail North Korea's rampant thefts of cryptocurrency to support its growing weapons of mass destruction program. As we have noted in previous comment letters, North Korea's cyberattacks pose a tremendous threat to US national security. Earlier this year, North Korean hackers stole more than $1 billion from Bybit, an audacious act that likely ranks as the single largest theft of all time.[11] While we expect that Huione's designation as a primary money laundering concern will close one of their main money laundering conduits, the North Korean regime has proven itself adept at circumventing US sanctions and they will likely find new avenues to launder their ill-gotten assets. Therefore, we urge FinCEN to finish the work it

[10] Elliptic Research, "Xinbi: The $8 Billion Colorado-Incorporated Marketplace for Pig-Butchering Scammers and North Korean Hacks," May 13, 2025, https://www.elliptic.co/blog/xinbi-guarantee.
[11] Federal Bureau of Investigation, "Public Service Announcement, Alert Number: I-022625-PSA," February 26, 2025, https://www.ic3.gov/psa/2025/psa250226.

started in 2023 to classify Convertible Virtual Currency Mixing as a primary money laundering concern.[12]

Conclusion

ICBA welcomes FinCEN's strong efforts to address the growing plague of crypto scams; however, we do not think this action alone will be enough. We urge FinCEN to consider additional steps, such as punitive measures for other large facilitators of money laundering, and improved data collection to advance this critical mission. Please contact me at brian.laverdure@icba.org if you have any questions about our comments.

Sincerely,

/s/

Brian Laverdure
Senior Vice President, Digital Assets and Innovation Policy

[12] Financial Crimes Enforcement Network, "Proposal of Special Measure Regarding Convertible Virtual Currency Mixing, as a Class of Transactions of Primary Money Laundering Concern," Federal Register 80, no. 203 (October 23, 2023): 72701-72723.
.