Written Testimony of Jacqueline Burns Koven
Head of Cyber Threat Intelligence
Chainalysis Inc.

Before the
House Financial Services Committee,
Subcommittee on National Security, Illicit Finance, and International Financial Institutions

Hearing on
Following the Money: Tools and Techniques to Combat Fraud

April 1, 2025

Chairman Davidson, Ranking Member Beatty, and distinguished members of the Subcommittee: Thank you for inviting me to testify before you today on the pressing issue of fraud targeting Americans.

My name is Jacqueline Burns Koven, and I am the Head of Cyber Threat Intelligence for the blockchain data platform Chainalysis, where we help make blockchains safer and more secure so that banks, businesses, and governments have the confidence and knowledge they need to help this new digital economy thrive. Leveraging the blockchain's inherent transparency, we track cryptocurrency activity by illicit actors, such as those perpetrating investment and confidence scams and provide data on their financial activity to private and public sector customers, including the federal government.

The intersection of scams and cryptocurrencies

This hearing could not be more timely. Americans are facing a growing threat by scammers and fraudsters as a result of numerous factors, including the convergence of technological developments such as social media, cryptocurrencies, and artificial intelligence. Of particular focus, cryptocurrency adoption and the application of blockchain technologies has expanded into a vibrant, innovative ecosystem, but fraudsters can always be counted on to abuse novel technologies and are leveraging cryptocurrency as a tool in a broader, more diverse set of criminal activity. Cryptocurrencies are increasingly a part of virtually every type of illicit activity, from scams targeting vulnerable US citizens to complex national security challenges driven by the most persistent foreign adversaries and nation states.[1]

Today’s hearing shines an important spotlight on the pervasive issue of fraud and scams, including their connection to cryptocurrencies. Over the years, the prevalence and sophistication of scams involving cryptocurrencies has increased, and now there are classes of scams that are almost exclusively associated with cryptocurrencies – most notably, so-called “pig butchering” – which refers to

[1] “2025 Crypto Crime Trends: Illicit Volumes Portend Record Year as On-Chain Crime Becomes Increasingly Diverse and Professionalized,” *Chainalysis*, Jan. 15, 2025, https://www.chainalysis.com/blog/2025-crypto-crime-report-introduction/.

investment or confidence scams that target and build relationships with individuals, convincing them to invest in fraudulent opportunities.

The utilization of cryptocurrency should fundamentally place scammers at a disadvantage due to the traceable nature of these assets. Cryptocurrency transactions are inherently public and the data from those transactions is preserved on a transparent, immutable ledger. At Chainalysis, we analyze the transaction data from blockchain networks in conjunction with open source intelligence information and proprietary data to map the ecosystem of benign as well as illicit participants in these networks. Blockchain investigations and transaction monitoring leveraging Chainalysis software and data provides a clear and visual representation of potential scam networks and laundering activities, a level of transparency that is unparalleled in traditional financial institutions. Indeed, identifying a single cryptocurrency payment to a scam enterprise can often lead to identifying hundreds of other victim payments, even revealing in some cases the scam compound from which the scammers are operating from, allowing for more effective disruption and restitution efforts rather than just one-off criminal investigations.

However, the current reality is that scammers are exploiting the disjointed and siloed nature of how the public and private sector respond to their schemes. Today, scam victims have multiple state, local, and federal agencies they can report to, yet there is no easy mechanism or obligation for these agencies to share reported information with each other or those in the private sector. Cryptocurrency businesses and financial institutions reporting scam information through Suspicious Activity Reports (SARs) and Currency Transaction Reports (CTRs) have no visibility into the scam indicators and cryptocurrency wallet addresses submitted by their peers and are unable to protect their customers from scams known to the government or the financial institution next door. At the same time, private sector actors outside of financial institutions, like blockchain forensics companies, lack the structures to comprehensively share and receive information from the public sector about scam activity that would allow them to take more proactive measures. More broadly, the cryptocurrency industry as a whole lacks a unified regulatory framework that clearly delineates which regulator has frontline responsibility for oversight of businesses offering stablecoins and trading services. This fragmentation allows scammers to operate with impunity, often due to the lack of communication and information flow between different entities and regulatory bodies.

We are encouraged that this subcommittee is interested in learning more about the impact of scams and fraud involving cryptocurrency on victims in the United States and globally. We strongly believe that blockchain intelligence solutions like Chainalysis are key to helping fight back against this growing form of criminal activity. To that end, we invite Congress' continued engagement on this topic, as addressing this issue requires an all-of-government approach in collaboration with the private sector, and we recommend that Congress ensure that state and local as well as federal law enforcement and other federal agencies have the resources necessary to comprehensively combat this issue.

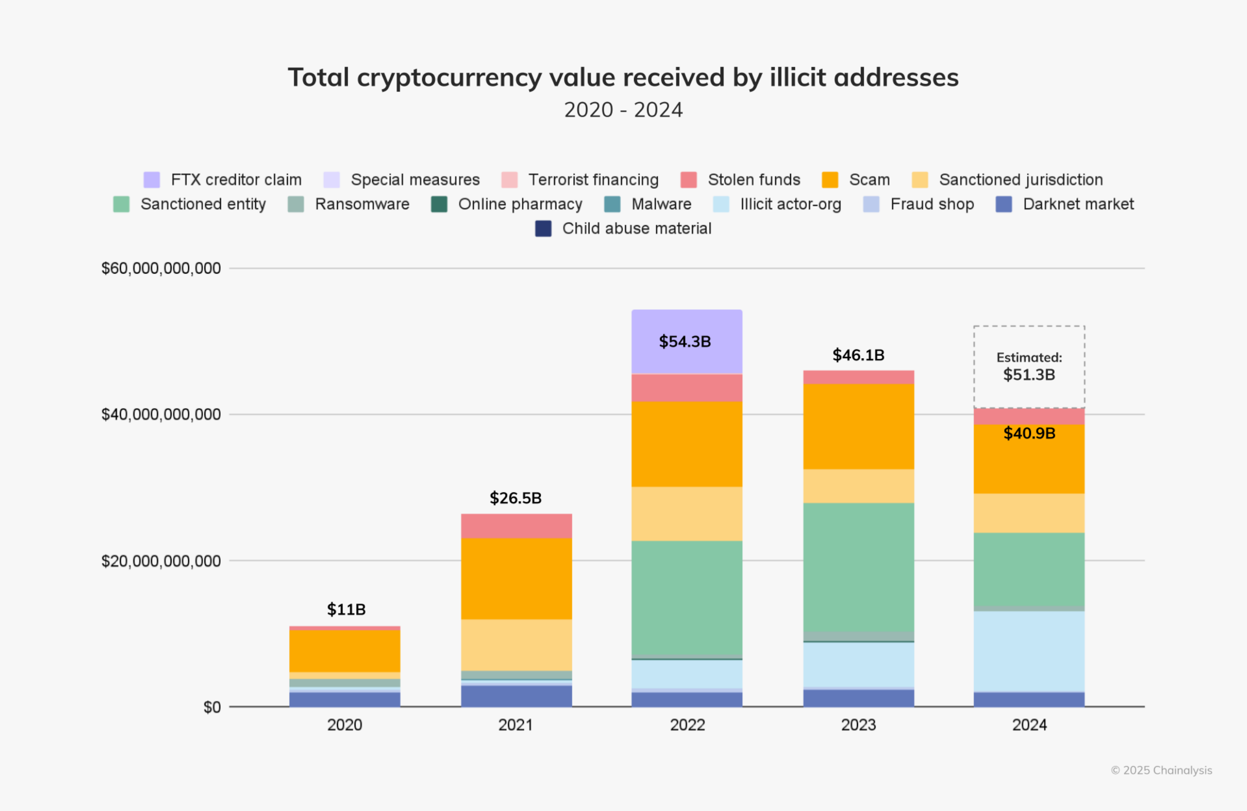
Chainalysis data and insights on scam activity

Chainalysis publishes an annual Crypto Crime Report that provides a detailed survey of the various types of illicit activity involving cryptocurrencies.[2] As cryptocurrency adoption accelerates and the broader crypto economy grows in size, cryptocurrency transactions are now frequently observed as part of activities as disparate as the manufacturing of fentanyl precursors supplied to Mexican drug cartels, the financing of entities affiliated with designated terrorist organizations, and the laundering of proceeds from cyberattacks conducted by hacking groups connected with the Democratic People's Republic of Korea (DPRK).

In 2024, we estimate that the total amount of cryptocurrency received by illicit actors will be over $51 billion. Our current data reflects over $40 billion received by illicit actors which, based on historical trends, will invariably increase as we identify more illicit transactions associated with activity in 2024. Scams as a class of illicit activity is one of the largest we track, accounting for approximately 25% of all illicit cryptocurrency proceeds that we trace. For each of the past four years, scam operators received

[2] "The Chainalysis 2025 Crypto Crime Report," *Chainalysis*, https://go.chainalysis.com/2025-Crypto-Crime-Report.html.

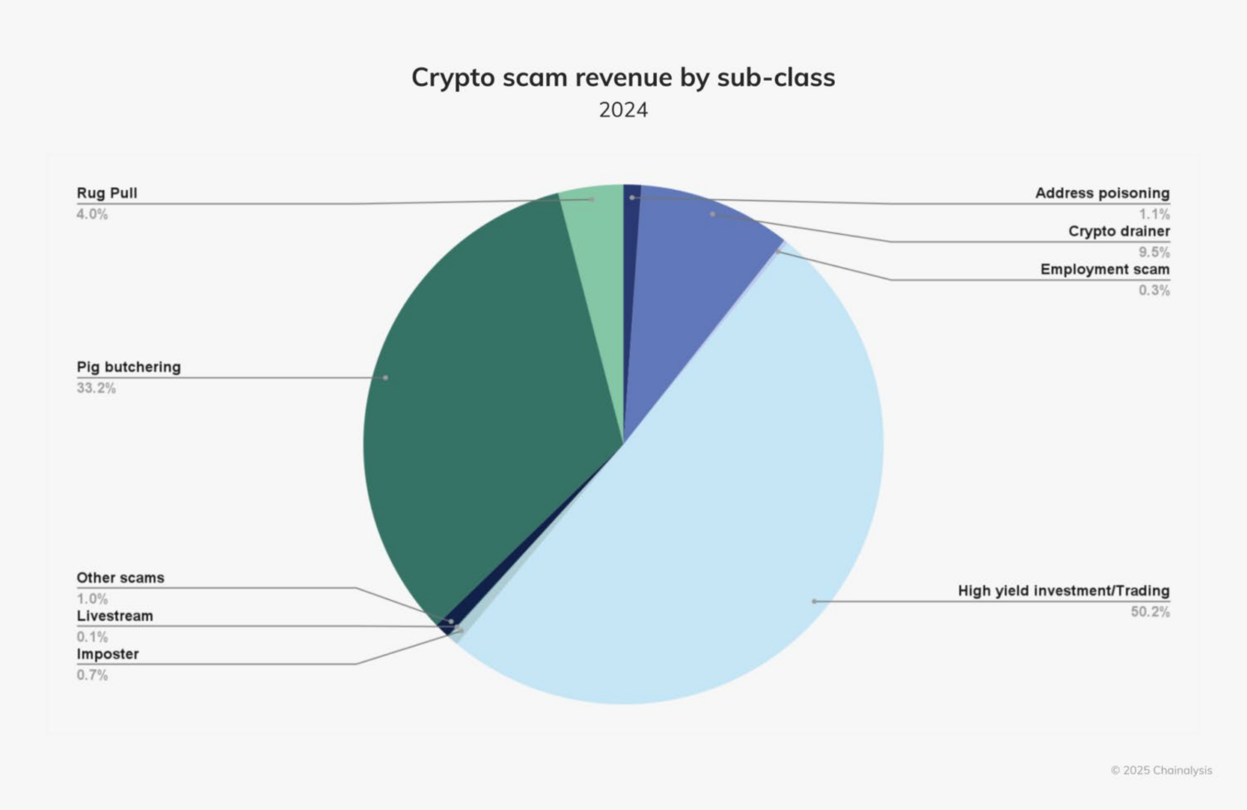
over $10 billion in cryptocurrency payments, and 2024 is estimated to be a record year in terms of cryptocurrency scam revenue.[3]



In 2024, over 80% of total crypto scam profits can be attributed to pig butchering and high-yield investment scams. Pig butchering - also referred to as investment, confidence, or romance scams - target and build relationships with individuals, convincing them to invest in fraudulent opportunities. This subclass of scam activity grew over 40% in 2024 based on total crypto funds received by wallets identified as belonging to entities operating pig butchering schemes. The other major subcategory of

[3] "Crypto Scam Revenue 2024: Pig Butchering Grows Nearly 40% YoY as Fraud Industry Leverages AI and Increases in Sophistication," *Chainalysis*, Feb. 13, 2025, https://www.chainalysis.com/blog/2024-pig-butchering-scam-revenue-grows-yoy/.

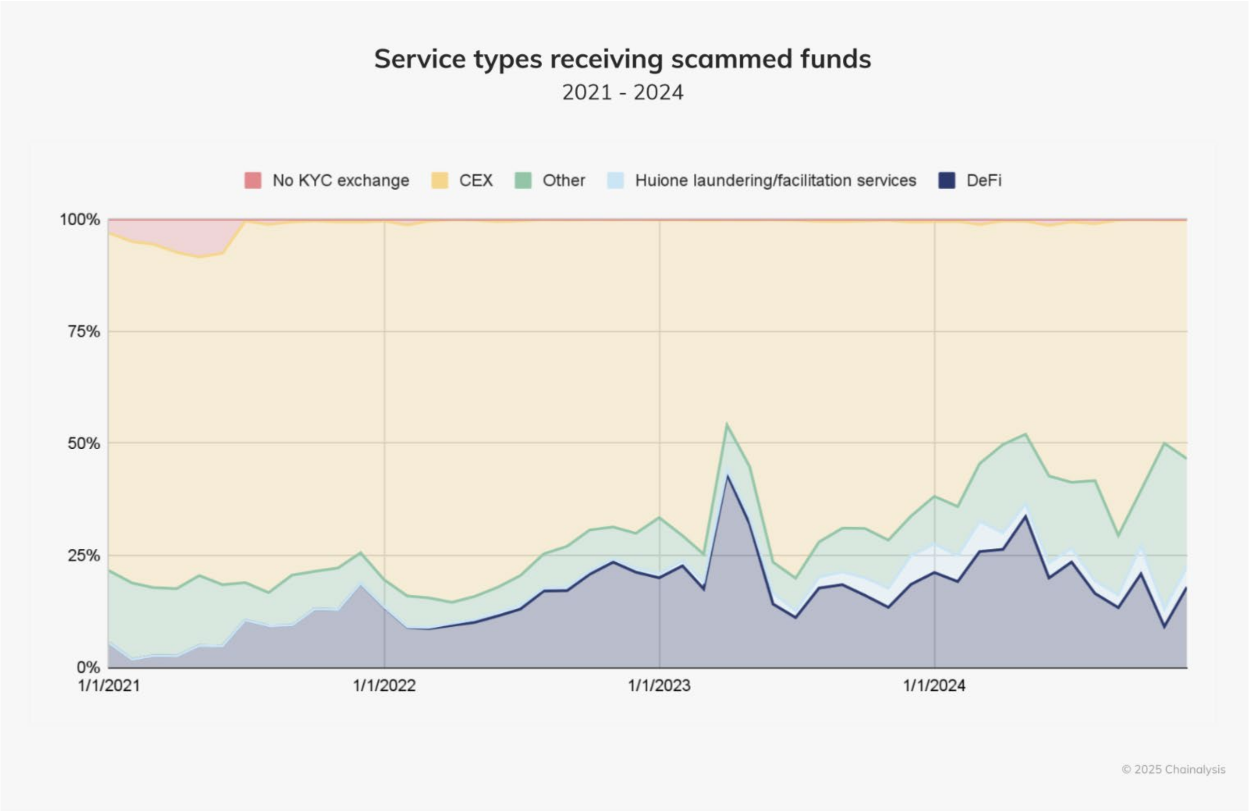
scams, high-yield investment scams, generally include Ponzi schemes and other get-rich-quick schemes. A more detailed breakdown of different scam types can be observed in the chart below.



Crypto scam revenue by sub-class

2024

We not only track the amount of cryptocurrency funds received by scam operators but also where those funds are directed for purposes of laundering or cashing-out to fiat currency. In the last few years, laundering destinations for scammed funds have remained relatively constant, with most funds going to centralized exchanges (CEXs). It is important to note that scam proceeds are largely laundered through overseas entities, reinforcing the effectiveness of the US anti-money laundering regime domestically.


Service types receiving scammed funds
2021 - 2024

One example of an offshore institution playing a large role in facilitating scams is the Cambodian service Huoine Guarantee. Huoine Guarantee has become a one-stop shop for illicit actors needing the technology, infrastructure, and resources to conduct scams. As we have highlighted in our annual Crypto Crime report, Huione and all vendors operating on their platform have processed more than $70 billion in crypto transactions since 2021.[4] This platform has provided infrastructure that facilitates the sale of scam technology and processed on-chain transactions for pig butchering and other fraud and scams, addresses reported as stolen funds, sanctioned entities such as the Russian exchange Garantex, fraud shops, child sexual abuse material, and Chinese-language gambling sites and casinos, among others. Many merchants on Huione Guarantee put little effort into masking their illicit activities, advertising the types of services they look for using thinly-veiled code words.

Other vendors on Huione catering to the scam ecosystem offer technology for facial recognition or facial alteration, targeted data lists for outreach to potential victims, web hosting services, social media accounts and content creation, orchestration of pig butchering and Ponzi schemes, and global passports, visas, and purportedly assisting with applications, and AI software. While generative AI can accelerate

[4] "Crypto Scam Revenue 2024: Pig Butchering Grows Nearly 40% YoY as Fraud Industry Leverages AI and Increases in Sophistication," *Chainalysis*, Feb. 13, 2025, https://www.chainalysis.com/blog/2024-pig-butchering-scam-revenue-grows-yoy/.

legitimate innovation, it can also make scams more scalable and affordable for bad actors to conduct. Generative AI is amplifying scams, the leading threat to financial institutions, by enabling high-fidelity, low-cost, and highly scalable fraud that exploits human vulnerabilities. It facilitates the creation of synthetic and fake identities, allowing fraudsters to impersonate real users and bypass identity verification controls.

In fact, Chainalysis recently acquired a company, Alterya, that found that 85% of scams involve fully verified accounts that are not detected by traditional identity-based fraud prevention solutions. Additionally, GenAI enables the generation of realistic fake content, including websites and listings, to power investment scams, purchase scams, and more, making these attacks easier and cheaper to deploy at scale, and more convincing and harder to detect. With this technology, scammers can deceive targets into authorizing payments under false pretenses, often known as authorized push payment (APP) fraud. The Huione Guarantee platform hosts dozens of software vendors that provide generative AI technology to facilitate scams.

Chainalysis solutions and the power of blockchain intelligence

The data and insights above barely scratch the surface of the type of intelligence that Chainalysis has developed on scammers, as well as numerous other types of illicit actors exploiting cryptocurrency networks. This is because the uniquely transparent manner in which cryptocurrency networks operate opens up powerful opportunities to gain invaluable insights into illicit activity occurring on these networks. Since all crypto transactions occur on a public and immutable ledger, detailed data is accessible for all transaction activity occurring on permissionless crypto networks.

Over ten years ago, Chainalysis pioneered the field of blockchain analytics by combining this publicly available data with proprietary data and intelligence to ascertain the underlying identities of the entities conducting on-chain transactions. Building on top of this foundation, we have developed custom-made products to map the blockchain in order to identify potential suspicious activity, trace fund movements, and disrupt illicit activity across crypto networks. Over the past ten years, our tools and data have become indispensable to the workflows of law enforcement and intelligence agencies in the US and globally, as well as to corporate compliance and risk departments.

The most demonstrable result from from this work is Chainalysis' support of hundreds of cryptocurrency cases involving seizures and freezing of assets in partnership with government agencies worldwide, helping secure an estimated $12.6 billion dollars worth of illicit crypto with a median seizure size of $5.9 million per action.[5] Recent reports point to approximately 198,000 bitcoin currently under U.S. government custody. Chainalysis has supported much of the recovery of these seized funds, providing

[5] “Asset Seizure and Cryptocurrency: How Chainalysis Creates Opportunities for Self-Sustaining Law Enforcement,” *Chainalysis*, Mar. 26, 2025, https://www.chainalysis.com/blog/cryptocurrency-asset-seizure/.

the most comprehensive blockchain tooling and training to enforcement agencies and regulatory bodies across the world.

The following notable scam-related crypto seizures were only possible due to the transparency of the blockchain and the availability of state-of-the-art Chainalysis tools and data. They are also a reflection of the significant ability to disrupt illicit activity possible when the US government is willing to responsibly integrate private sector software and services into novel workflows.

- Stablecoin issuer Tether and the cryptocurrency exchange OKX announced that they collaborated with the United States Department of Justice in an investigation that led to Tether freezing approximately $225 million in USDT tokens linked to an international human trafficking syndicate in Southeast Asia responsible for romance scams, helped in part by Chainalysis solutions.[6]

- In 2023, a South Korea-led Interpol operation saw authorities arrest 3,500 cybercriminals associated with online scamming and seize $300 million in funds, $100 million of which was made up of digital assets.[7]

Beyond these specific law enforcement examples, last year, Chainalysis launched Operation Spincaster designed to disrupt and prevent scams through public-private collaboration.[8] Leveraging the transparency of the blockchain, Chainalysis proactively identified thousands of compromised wallets. This actionable intelligence formed the basis of a series of operational sprints across six countries (US, UK, Canada, Spain, Netherlands, and Australia) with over 100 attendees, including 12 public sector agencies and 17 crypto exchanges. The operational sprints featured training in identifying compromised wallets and tracing the stolen funds using Chainalysis Crypto Investigations solutions. Over 7,000 leads were disseminated during these sprints relating to approximately USD $162 million of losses. These leads were used to close accounts, seize funds and build intelligence to prevent future scams. In fact, in one of the sprints, participants were able to contact a victim directly to warn them of an ongoing scam,

[6] "Following Investigations by Tether, OKX, and the U.S. Department of Justice, Tether Voluntarily Freezes 225M in Stolen USDT Linked to International Crime Syndicate," *Tether* and *OKX*, Nov. 20, 2023, https://www.okx.com/en-eu/learn/tether-okx-investigation and https://tether.io/news/following-investigations-by-tether-okx-and-the-us-department-of-justice-tether-voluntarily-freezes-225m-in-stolen-usdt-linked-to-international-crime-syndicate/.

[7] Toulas, Bill, "Interpol operation arrests 3,500 cybercriminals, seizes $300 million," BleepingComputer, Dec. 19, 2023, https://www.bleepingcomputer.com/news/security/interpol-operation-arrests-3-500-cybercriminals-seizes-300-million/.

[8] "Introducing Chainalysis Operation Spincaster: An Ecosystem-Wide Initiative To Disrupt and Prevent Billions in Losses to Crypto Scams," *Chainalysis*, Jul. 18, 2024, https://www.chainalysis.com/blog/operation-spincaster/.

prompting the victim to take preventative action on-chain by revoking the approval before the scammer was able to steal a six-figure sum.

AML compliance and the need for prevention

Chainalysis data and tools are not only integral to public sector operations and seizures but also play an important role in the AML programs of financial institutions, crypto businesses, and the broad swath of private sector businesses motivated to stop scam activity. Chainalysis data is leveraged by financial institutions for transaction monitoring, enhanced due diligence, and when appropriate, enhancing SAR filings. Our data serves as the intelligence driving blockchain transaction monitoring alerts for exposure to suspicious funds coming onto their platforms or customers attempting to send funds to illicit entities from their platforms.

At Chainalysis, we also think it is imperative to move past reactive compliance and fraud workflows at financial institutions and to start developing processes to prevent Americans from falling prey to scams altogether. Chainalysis' acquisition of Alterya enables financial institutions to map the entire lifecycle of fraudulent operations, from initial online scam campaigns and money muling to monetization within financial services and subsequent money laundering and cash-out processes through proactive AI-driven scam detection, financial data, and infrastructure mapping. We utilize artificial intelligence and other advanced techniques to identify scam activities across various online sources, enabling large-scale early "upstream" detection. We construct a comprehensive scam social graph that interconnects fraudulent activities across various platforms, payment systems, and blockchains. Our adversaries are leveraging AI to rob Americans of their life savings, and we must leverage that very technology to beat them at their own game. This is what the future of combatting scams looks like.

Recommendations

1. Modernize and streamline scam reporting and response with the ability to efficiently share information on scams between the public and private sector.

Today scam victims in America have multiple options in federal and local law enforcement where they can report their crime. This has greatly contributed to a fragmented approach to combatting scams and reduces our visibility into the true scale of this war on potential victims both in the US and abroad. A centralized reporting database feeding from state, local, and federal reporting is critical to enhancing efficiency and actionable intelligence for cases leading to the recovery of funds, restitution, and the prevention of additional victims.

Similarly, Suspicious Activity Reports (SARs) are filed by financial institutions but the crucial information contained within these reports about particular scams is not accessible to other financial institutions or the other entities supporting scam prevention. This lack of information sharing creates blind spots and delays in response, enabling scammers to continue their illicit activities unabated. Singapore's Anti-Scam Command (ASCom) is a great model for combatting scams efficiently by eliminating silos and working constructively with over 80 private sector partners. It is imperative that the industry and regulatory bodies work together to break down these information silos and create a more cohesive and collaborative approach to combating cryptocurrency-related scams. This will ensure that the inherent advantages of blockchain technology in tracing and combating financial crime are fully leveraged, and that scammers are not able to exploit the system due to gaps in communication and information sharing.

2. Ensure broad education and training about crypto networks and blockchain intelligence and invest in tech-driven efficiency by leveraging third-party blockchain analysis software and data to swiftly action intelligence and seize funds.

With the broader adoption of cryptocurrency on the rise, including by illicit actors, it is no longer sufficient to isolate knowledge about crypto networks to a small group of technical experts. Rather, government agencies and departments must ensure that a broad spectrum of personnel receive the latest training on how crypto networks operate, how blockchain analysis can supplement traditional analytical and operational workflows, and what actions can be taken to quickly disrupt illicit fund movements through crypto networks. Too often, victims are turned away from local authorities who are ill-equipped or even uninformed as to how to take on crypto cases. Other times, an individual complaint might not get prioritized if law enforcement doesn't have the analytic tools it needs to connect a low-value scam payment to a bigger scam conglomerate netting tens or hundreds of millions of dollars.

Particular offices within agencies that have invested in integrating blockchain analytics into their workflows have achieved massive successes - such as IRS Criminal Investigations and FBI's Virtual Asset Unit. However, the extensive overlap of crypto in all parts of many agencies' missions necessitates a broader cohort of staff to understand the underlying technology and how it is used.

We strongly recommend that US agencies invest in the training and tools to stay on top of the latest scam trends, enhance their visibility into their case to cover the full expanse of the scheme, and empower them to potentially seize illicit fund movements yielding huge dividends back to the US government in the form of billions of dollars of forfeited cryptocurrency.

3. Enact legislation that ensures a unified federal regulatory framework for cryptocurrency businesses.

Chainalysis is encouraged by the momentum within Congress to pass legislation that would create federal regulatory frameworks for stablecoin issuers and cryptocurrency trading businesses. From the perspective of mitigating scam activity, it is important to have a dedicated regulator that can understand the unique operations of the business that they oversee and ensure that processes are in place to best disrupt bad actors and prevent illicit activity.

4. Close gaps of AML/CFT standards implementation for FATF members, especially countries that scammers rely on to launder funds defrauded from Americans.

More capacity building is needed in jurisdictions with weak AML and CFT policies that are providing havens for laundering the proceeds of scams defrauding Americans. In the absence of cooperation, more pressure is needed to disrupt the financial networks and the digital asset services flagrantly abusing laws and regulatory norms. Sanctions have proven to be an effective tool, and sustained enforcement actions targeting every facet of the scam supply chain – especially the offshore institutions defying international norms and AML/CFT processes and standards – would help cut scam perpetrators and their facilitators off from the global financial system.

-

Thank you again for the opportunity to provide testimony on this important topic. At Chainalysis, we continue to support the bipartisan efforts of the Committee, such as the recent passage of the OFAC Licensure for Investigators Act. We hope we can continue to be a partner on helpful initiatives by Congress to better protect against scams and fraud.