Chainalysis

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

Before the
Senate Committee on Aging

Hearing on
Made in China, Paid by Seniors: Stopping the Surge of International Scams
January 14, 2026

Chairman Scott, Ranking Member Gillibrand, and distinguished members of the Special Committee: Thank you for inviting me to testify before you today on the pressing issue of international fraud and scams targeting older Americans, largely perpetrated by Chinese Organized Crime syndicates.

My name is Jacqueline Burns Koven, and I am the Head of Cyber Threat Intelligence for the blockchain data platform Chainalysis, where we harness the transparency of blockchains so that banks, businesses, and governments have the data and investigations, compliance, and security solutions they need for this new digital economy to thrive. We track cryptocurrency use by illicit actors, such as those carrying out investment and impersonation scams, and provide data on their financial activity to private- and public-sector customers, including the federal government.

In my testimony, I provide our assessment of the extent of scam activity and the role that cryptocurrencies play, and recommend how we can best mobilize and fight back against the growing scourge of scams that are putting all Americans, especially the most vulnerable among us, at risk. Once again, thank you for the opportunity to provide testimony on this important topic and continue to be a helpful partner on initiatives by Congress to better protect Americans – especially the most vulnerable – against scams and fraud.

Key Takeaways

- Cryptocurrencies are a primary channel for scammers' operations; with the right data, tools, and resources, this should put the government at an advantage.
- AI technology is making scams more effective, but it can also help detect fraud and prevent potential victims from falling victim to scams and sending money.
- Scammers are leveraging a vast, industrialized ecosystem of illicit tools and Chinese-language money laundering networks for their operations.
- Government and industry responses are fragmented and reactive. This crisis requires a unified and technology-enabled response.

The growing intersection of scams and cryptocurrencies: $17B stolen in 2025

Americans, and especially older Americans, have not been immune to the threat posed by a global, organized, and pernicious scam industrial complex that adeptly leverages technological developments in social media, artificial intelligence, and cryptocurrencies.

Cryptocurrencies are often the financial rails of choice for scammers for the same reasons legitimate users use them – transactions are cross-border and instantaneous. But I am here today to emphasize that fraudsters’ use of cryptocurrency should place them at a fundamental disadvantage, given the traceability and freezeability of many of these assets.

At Chainalysis, we analyze transaction data from blockchain networks in conjunction with open-source intelligence to map the ecosystem of legitimate and illicit flows. Our software provides a clear, visual representation of potential scam networks and laundering activities, a level of transparency that isn’t possible for traditional forms of value transfer. Indeed, identifying a single cryptocurrency payment to a scam enterprise can often lead to identifying hundreds of other victim payments, the illicit services they leverage, and, in some cases, the scam compound from which the scammers operate. This visibility also enables us to estimate the amount of crypto funds stolen in fraud and scams over time.

According to Chainalysis data, 2025 was a record year for cryptocurrency scams, totalling an estimated $17 billion worth of cryptocurrency globally. Fraudsters can always be counted on to abuse novel technologies, and scam conglomerates are exceptionally adept at wielding new tools to scale their schemes to defraud Americans. Nobody is better than Chinese organized crime groups. They are the global market leaders in criminal fintech, and the Chinese-language underground ecosystem underpinning them is the most advanced in the world. They provide the entire spectrum of “crimeware” needed to conjure up a scam— social media profiles, mass calling and text spamming tools, stealer malware, data targeting lists with names and phone numbers of potential targets, AI technologies for deepfakes and voicecloning or fake investment platforms, laundering engines, and critical underground banking infrastructure – leveraging cryptocurrency as a form of payment.

The unique intelligence provided by the blockchain should be considered foundational for understanding the fraud problem at both a strategic and tactical level. The inherent transparency of blockchains, combined with the right data and tools, can illuminate the key components of the scam supply chain that support our national scam crisis. This can empower the U.S. Government to understand the scale of the problem, measure the impact of a counterscam strategy, surface investigative leads for the attribution of threat actors behind these campaigns, and identify opportunities for disruption.

Law enforcement and regulatory bodies can disrupt these networks, cut them off from the global financial system, and make it harder for them to profit by targeting illicit entities and networks on the blockchain with sanctions and asset seizure. Blockchain analytics offers unique opportunities to trace illicit proceeds of crime, identify additional victims, and partner with the private sector to disrupt illicit networks and pursue restitution, rather than relying on one-off criminal investigations.

However, despite this huge potential for disruption, scammers are exploiting the disjointed, siloed nature of how the public and private sectors respond to their schemes. To be truly effective, we must pursue a multifaceted strategy that prioritizes uprooting the enabling scam infrastructure and identifying and bringing to justice the individuals responsible for perpetrating the scams.

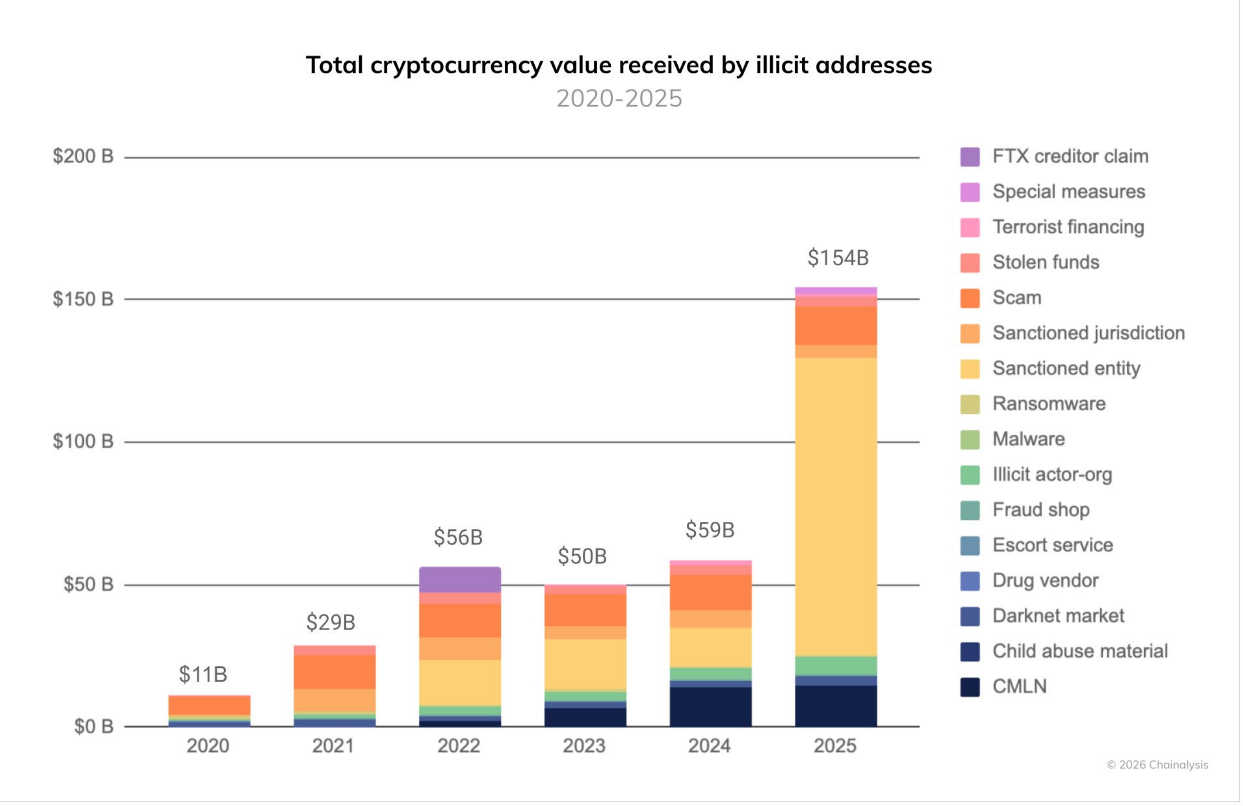
Finally, we need to focus on prevention. AI-powered fraud prevention technology can stop victim funds from being stolen by scammers. But financial institutions and cryptocurrency businesses need guidance on when and how to intervene when they suspect their customers may be in the process of being scammed. On one hand, providing some friction may be critical to preventing funds from being sent to scammers. On the other hand, financial institutions may be hesitant to limit what their customers can do with their own money. Part of the solution involves using data to help financial institutions stop their customers from sending to likely scams at the point of transaction, rather than trying to anticipate what their customers are doing based on behavioral red flags alone. But even so, regulatory guidance on what these businesses can and cannot do to protect their customers is needed.

As such, our recommendations include:

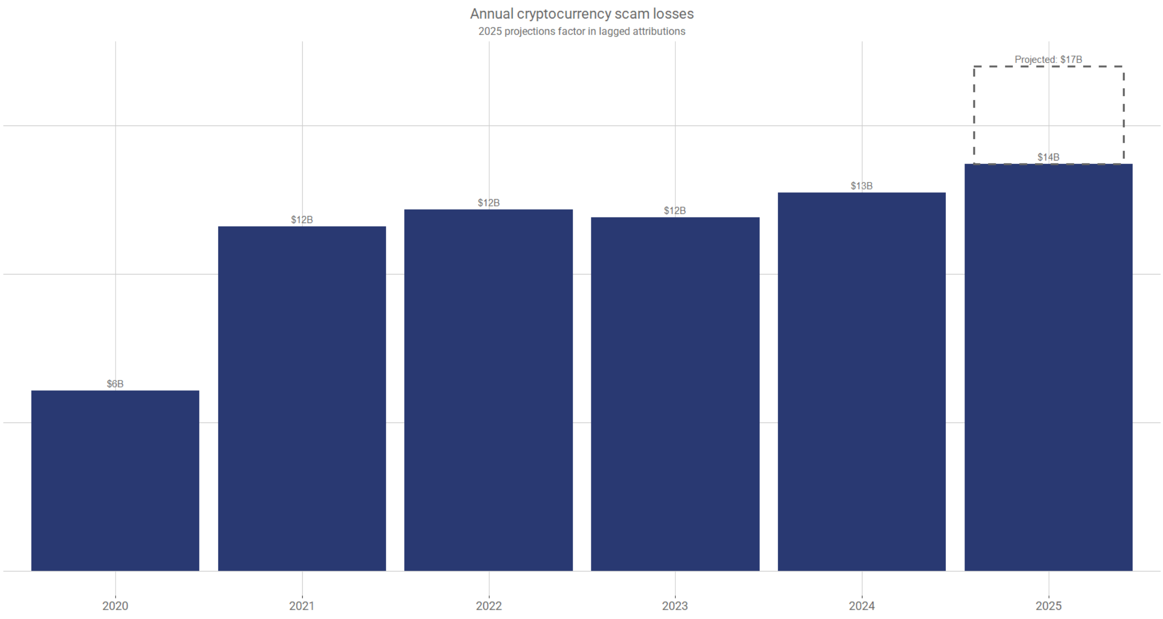
1. Mobilize a whole-of-government and industry national anti-scam strategy that prioritizes enhanced reporting and collaborative information sharing that can best disrupt scam conglomerates;
2. Leverage technologies designed for both the prevention and remediation of scams;
3. Ensure financial institutions and crypto businesses are incentivized to assist in the prevention of transactions to scams and have appropriate guidance to enable them to do so;
4. Advocate to close gaps in the implementation of AML/CFT standards by FATF members, especially countries that scammers rely on to launder funds defrauded from Americans.

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. In 2025, we estimate that the total amount of cryptocurrency received by illicit actors will be over $154 billion. This number will inevitably increase as we identify more illicit transactions associated with activity in 2025.



In each of the past five years, scam operators received over $12 billion in cryptocurrency payments, and 2025 is estimated to be a record year for cryptocurrency scam revenue. Our data shows at least $14 billion worth of cryptocurrency scammed globally, and we expect that figure will exceed $17 billion as we retroactively identify more scams, based on historical trends.



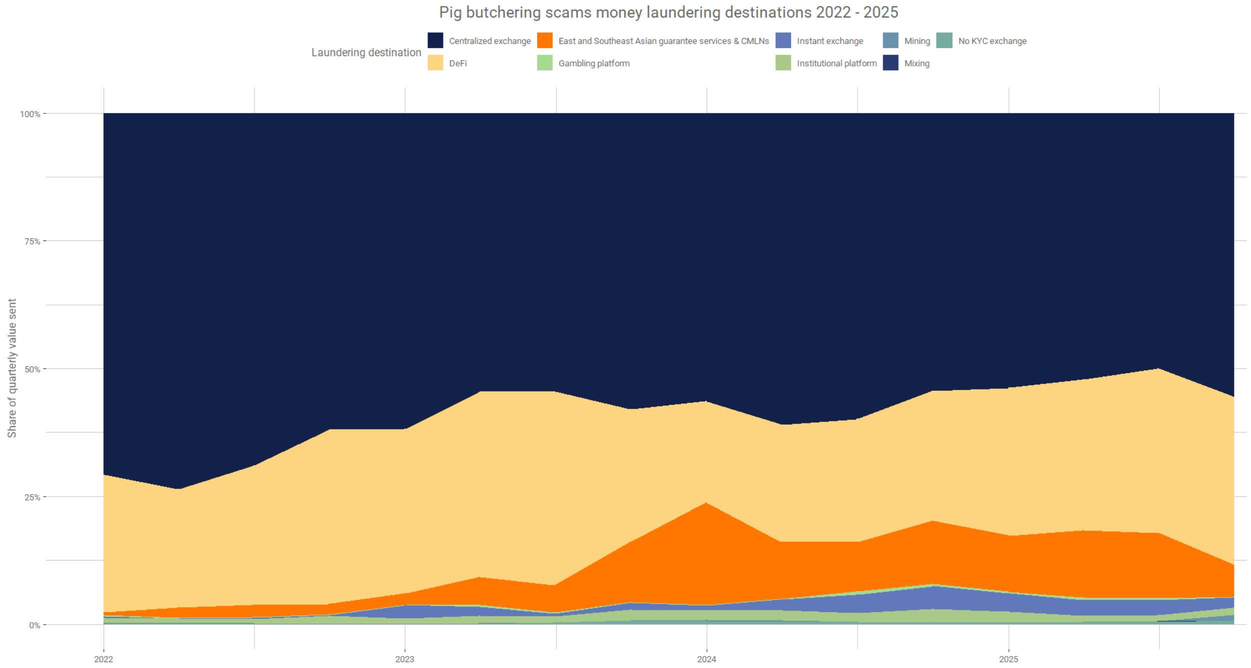
Overall scam inflows have also surged, particularly through impersonation tactics that saw a staggering 1400% year-over-year growth. While high-yield investment programs (HYIP) and pig butchering remain dominant categories by volume, we're seeing increasing convergence across scam types as fraudsters leverage AI, sophisticated SMS phishing services, and complex money laundering networks to target victims more effectively than ever before.

These tools and services underpinning all manner of scams are paid for with cryptocurrency, including the mass text phishing scam impersonating E-ZPass that targeted millions of Americans in 2025. To pull this off, the Chinese Smishing Triad leveraged software from "Lighthouse," a Chinese-language vendor on Telegram that accepts cryptocurrency in exchange for "phishing for dummies" with hundreds of templates for fake websites, domain setup tools, and features designed to evade detection. The scale of Lighthouse phishing attacks is staggering. In 20 days, approximately 200,000 fraudulent websites created using Lighthouse were used to attract 'well over 1,000,000 potential victims' in at least 121 countries.

Human trafficking is also behind some of the most pernicious scams. Chainalysis collaborates with Non-Governmental Organizations such as the International Justice Mission, which operates in the world's corruption hotspots, including the Golden Triangle, enabling Chainalysis to identify cryptocurrency wallets belonging to crime syndicates operating within specific compounds. These wallets tell of the horrors not only of the scam victims themselves but of the estimated hundreds of thousands of human trafficking victims behind the scam compounds. Chainalysis has previously detailed how we have traced a single ransom payment in cryptocurrency made by a trafficking victim held captive in the KK Park compound in Myanmar to a centralized wallet commingled with hundreds of millions of dollars in scam proceeds. We’ve now identified cryptocurrency wallets belonging to compounds across multiple countries and continents.

The International threat: Scam laundering leverages offshore exchanges and Chinese-language money laundering services, with a strong regional nexus to East and Southeast Asia

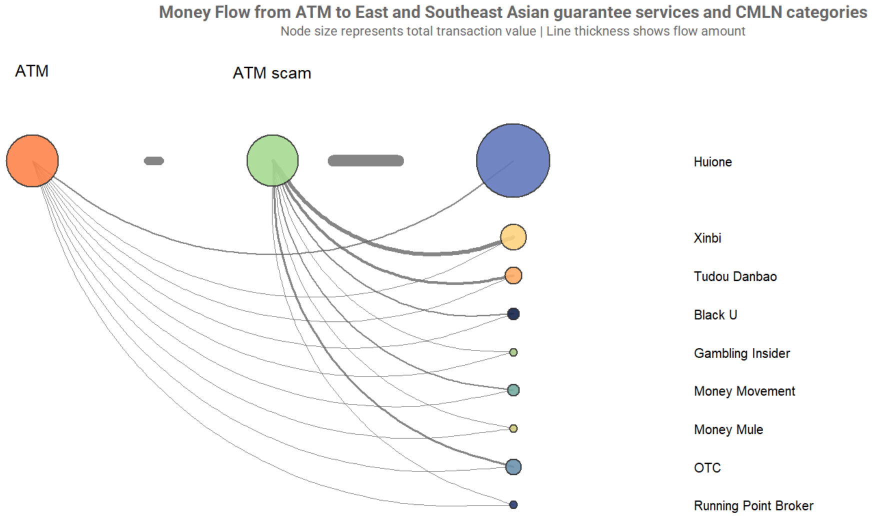
We not only track the amount of cryptocurrency funds received by scam operators but also where those funds are directed for purposes of laundering or cashing out to fiat currency. In the last few years, centralized exchanges (CEXs) have been the primary destinations for laundering funds from scams; however, Decentralized Exchanges and Chinese Money Laundering Networks (CMLNs) have seen increased adoption among scammers. The regional connection of the scamming syndicates is evidenced by the off-ramping patterns we observe, with a significant portion of the proceeds from pig butchering scams flowing to CMLNs. 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.



In recent years, CLMNs have emerged as dominant channels for laundering illicit cryptocurrency, including funds stolen through fraud and scams. Guarantee services operate as one-stop shops for illicit actors needing the technology, infrastructure, and resources to conduct scams. They function primarily as marketing venues and escrow infrastructure for these networks. While they provide trust mechanisms for vendors, they don't control the underlying laundering activity. Huione and Xinbi have dominated the market for the past few years, and many other guarantee services continue to operate freely. Many merchants on these platforms put little effort into masking their illicit activities, advertising the types of services they offer using thinly veiled code words. They openly cater to the scam ecosystem by providing 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.

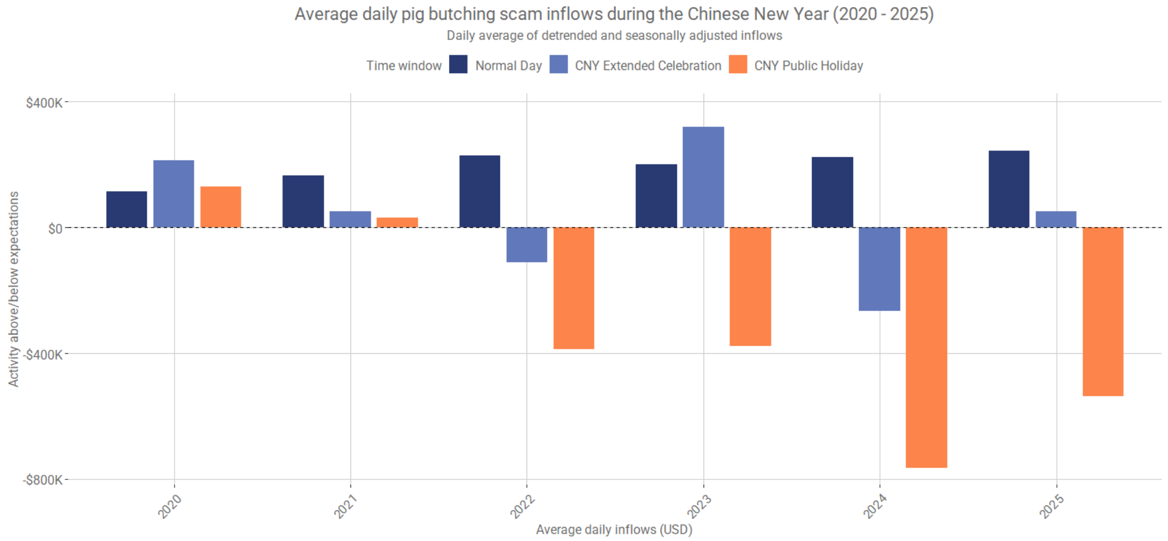
Our on-chain analysis continues to show persistent connections between cryptocurrency scams and operations based in East and Southeast Asia. While the Huione Guarantee platform identified in our 2025 report was effectively shut down following FinCEN's 311 designation — which severed its access to the U.S. financial system — we've observed expansion of similar operations across the region.

Our analysis reveals that funds originating at U.S. crypto ATMs frequently flow into wallets associated with Southeast Asia-based CMLNs and guarantee services, which serve as key intermediaries in the broader global scam infrastructure. While not all on-chain flows from scams to CMLNs can be traced directly to ATM on-ramps, crypto ATMs remain a critical input for scammers targeting older adults, who are often instructed to convert cash into cryptocurrency at these kiosks before funds are quickly transferred. In this context, actors leveraging crypto ATMs as both payment conduits and loci of fraud increasingly depend on CMLNs to launder and integrate stolen funds into the wider financial system, illustrating how traditional elder fraud has evolved into a transnational, crypto-enabled ecosystem.



Stronger state protections that require owners and operators of crypto kiosks to set transaction limits, inform users of risks, provide receipts, and refund qualifying payments could help prevent older adults from falling prey to certain scams.

The chart below shows the centrality of Southeast Asia to pig butchering scams by examining the 'holiday effect' associated with the Chinese New Year public holiday (7 days at the start of the 15-day new year celebration). Starting around 2022, roughly when Huione began to play a central role in laundering funds from scam compounds such as KK Park, there was a notable reduction in pig butchering scam activity during the 7-day public holiday associated with the Chinese New Year. After the data have been detrended and seasonally adjusted, average daily pig butchering activity drops notably during these short windows. This pattern suggests that the Chinese holiday is associated with a reduction in inflows to pig butchering scams, indicating that actors in East and Southeast Asia play an important role in this scam ecosystem.



Recent enforcement actions against overseas money laundering facilitation networks, including sanctions designations and advisories, have shed light on the national security threat that impacts victims worldwide. These actions include the designation of the Prince Group by the U.S. Treasury Department's Office of Foreign Assets Control (OFAC) and the Office of Financial Sanctions Implementation (OFSI) by HM Treasury in the UK, the Financial Crimes Enforcement Network (FinCEN)'s Final Rule designating Huione Group as a primary money laundering concern, and FinCEN's advisory on Chinese money laundering networks.

We applaud these actions, but the threat actors are resilient. As with other genres of illicit on-chain activity, actions against guarantee services can be disruptive, but the core networks persist and migrate to alternative channels when challenged. While Huione's guarantee operations were disrupted after Telegram removed some of their accounts, vendors using Huione have continued to use or advertise on alternative platforms, their operations largely uninterrupted. While these hubs continue to connect vendors and buyers, most vendors promote advertisements across platforms and are not reliant on any specific service. As with legitimate e-commerce platforms, service ratings and reviews create accountability within the illicit ecosystem, and vendors often cultivate their market reputation through public attestations of their reliability and service quality.

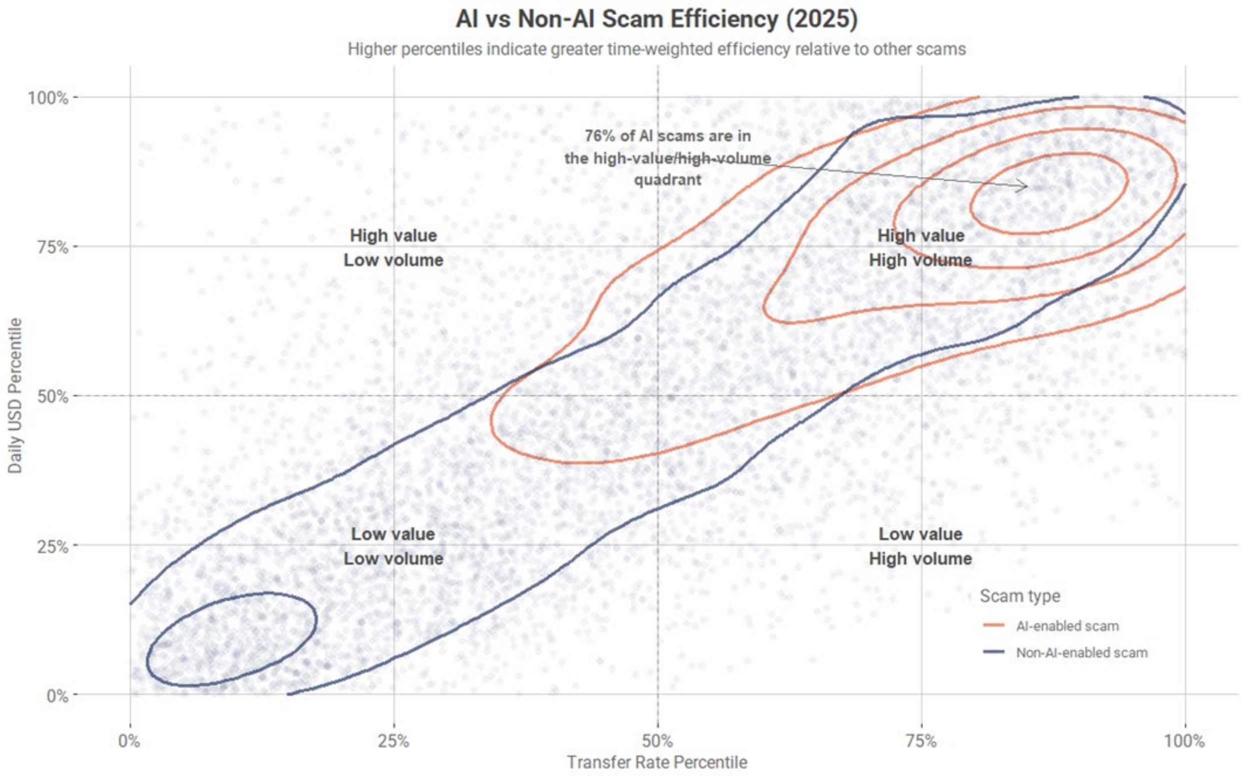
The Local Impact: Elderly US citizens are uniquely vulnerable to the threat of scams, and the role that cryptocurrency can play

Scams targeting older adults represent some of the most financially devastating frauds reported in the US. Recent estimates indicate that Americans aged 60 and older lose billions of dollars annually to financial exploitation and fraud, including nearly $4.9 billion in reported losses in 2024 alone, more than any other age group, according to AARP and FBI data. The FBI's Internet Crime Complaint Center (IC3) further underscores this trend: in 2024, individuals aged 60 and older reported $2.8 billion in losses from crypto-related scams, reflecting both the scale and the growing role of digital assets in modern fraud. While elder fraud encompasses a broad range of schemes, cryptocurrency ATMs have emerged as a notable on-ramp for scams. Reported losses from Bitcoin ATM fraud have risen sharply in recent years, and older victims are disproportionately affected by these kiosk-based conversions. The elderly, who often have significant retirement savings yet limited familiarity with irreversible digital payment methods, remain particularly vulnerable to such tactics.

AI and professional scamming tools increase scam severity

While generative AI can accelerate legitimate innovation, it can also make scams more scalable and affordable for bad actors. We are rapidly moving toward a future in which virtually all scams will incorporate AI into their operations to some degree. While many scams involve buying AI tools through traditional payment channels, a significant subset buys these tools on-chain, making their transactions visible. Exploring the differences between scams with visible on-chain associations to Chinese AI vendors lets us probe the scale and efficiency of AI.

As depicted below, 76% of AI scams are in the time-weighted high-value/high-volume quadrant. This means that a large majority of scams with demonstrable on-chain links to often Telegram-based Chinese AI vendors selling face-swap software, deepfake technologies, and LLMs tend to (1) scale more quickly (i.e., higher incoming transfer rates) and (2) be more severe (i.e., higher daily USD volumes) than scams without these clear on-chain links to AI vendors.

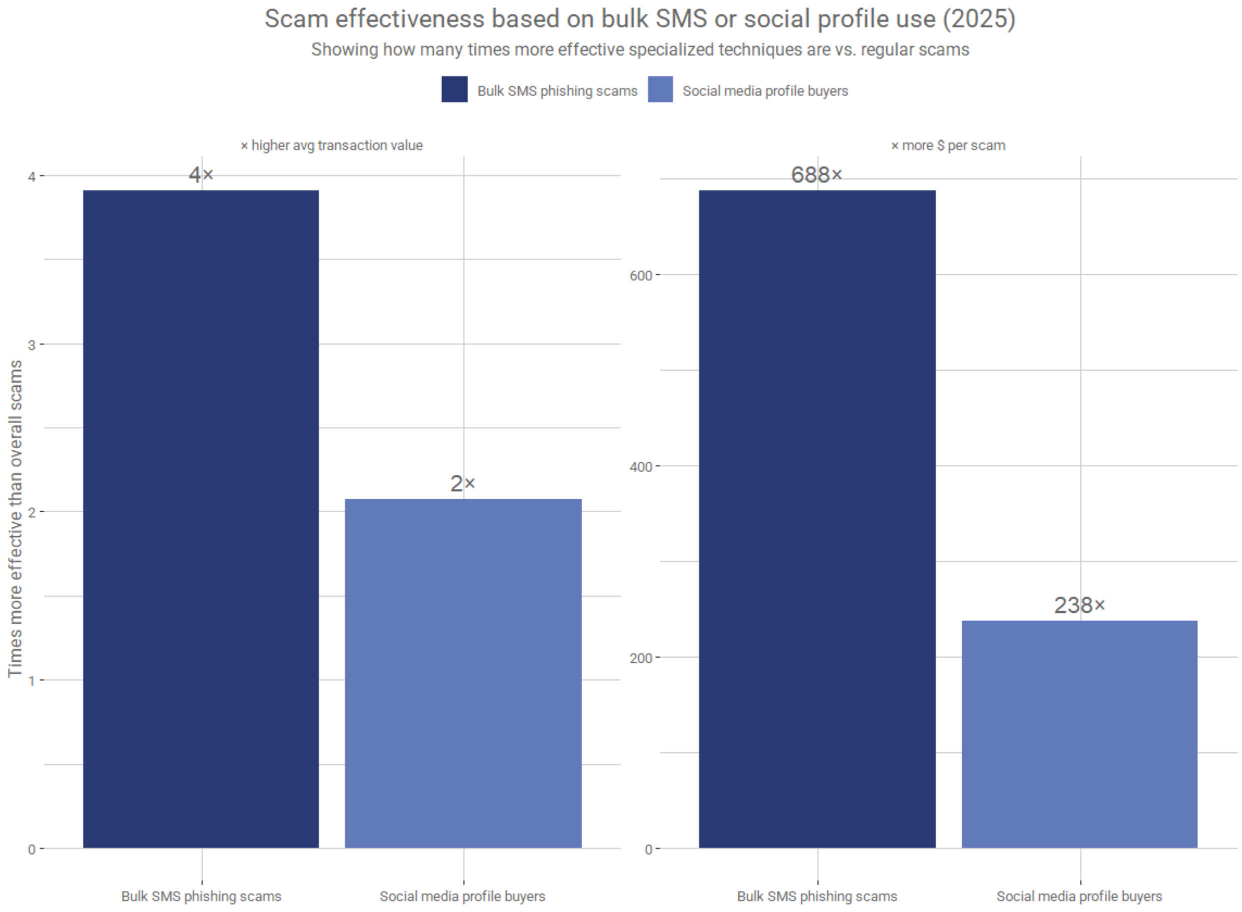


Our analysis reveals that, on average, scams with on-chain links to AI vendors extract $3.2 million per operation compared to $719,000 for those without an on-chain link — 4.5 times more revenue per scam. These AI-related operations also demonstrate significantly greater time-weighed efficiency:

- Higher daily revenue: $4,838 vs $518 median daily revenue
- Increased transaction volume: 35.1 vs 3.89 average transfers per day (9x more transaction activity)

These metrics suggest both higher operational efficiency and potentially broader victim reach. The increased transaction volume indicates that AI is enabling scammers to reach and manage more victims simultaneously, a trend consistent with the industrialization of fraud. In contrast, the increased scam volume suggests that AI is likewise making the larger scams more persuasive.

The professionalization of scamming tools is also a force multiplier to execute industrial-scale scams. Many of these campaigns have a social media angle, given that such platforms provide access to millions of users, and are thus prime targets for sending automated messages. In such cases, scammers may buy bulk social media profiles and use SMS and phishing kits to communicate. Scams leveraging these phishing kits are 688 times more effective in dollar terms and four times more effective in average transaction size than regular scams. Scams that buy bulk social media accounts are likewise 238 times more effective in dollar terms and two times more effective in average transaction value than regular scams.



Chainalysis data and tools as part of the response

The uniquely transparent manner in which blockchains operate opens up powerful opportunities to gain insights into illicit activity occurring on these networks. However, this data is difficult to access without the right tools, training, and data. Over the past ten years, Chainalysis has 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 this work is the support that Chainalysis has provided on hundreds of cryptocurrency cases since its inception, involving seizures and freezing of assets in partnership with government agencies worldwide, helping secure an estimated $34 billion dollars worth of illicit crypto.[1] 2025 saw unprecedented law enforcement action against scams, including two of the largest-ever crypto-related law enforcement actions directly connected to scam operations.

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 tools and data like those Chainalysis provides. These actions mark a shift from reactive victim recovery to systematic dismantling, targeting not just front-line scammers, but also the executives, infrastructure, shell companies, and financial rails that sustain them. Together, they illustrate a new, more integrated phase in scam enforcement: one focused on breaking the economic backbone of crypto-enabled fraud at scale and across borders, rather than treating scams as local, isolated, or purely digital crimes.

- In October 2025, the U.S. Department of Justice unsealed charges against a Cambodian national and Prince Group chairman Chen Zhi for allegedly overseeing Cambodian forced-labor scam compounds that powered large-scale cryptocurrency fraud targeting victims worldwide. According to prosecutors, these compounds operated as vertically integrated fraud factories: trafficked individuals were coerced into running pig butchering investment scams and romance fraud schemes, laundering proceeds through cryptocurrency to obscure attribution and scale operations globally. Critically, U.S. authorities paired these indictments with large-scale financial disruption, including arrests across transnational money laundering networks and actions to seize and forfeit more than $15 billion in illicit proceeds linked to scam activity.
- In November 2025, the UK's Metropolitan Police secured convictions in a landmark crypto money laundering case that led to the world's largest confirmed cryptocurrency seizure, recovering over 61,000 Bitcoin — currently valued at around £5 billion — from Chinese national Zhimin Qian (also known as Yadi Zhang), who orchestrated a multibillion-pound investment fraud in China that victimized more than 128,000 people between 2014 and 2017.
- Also in November 2025, the U.S. Scam Center Strike Force's success in seizing over $401 million in cryptocurrency demonstrates the effectiveness of blockchain intelligence in taking action against transnational scam operations.
- In August 2025, it was revealed that APAC-based law enforcement froze $47 million in pig butchering funds through collaboration with the private sector, following a similarly successful public-private sector collaboration that resulted in the freeze of $225 million in funds.

AML compliance and the need for prevention

[1] "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/.

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 a broad swath of private sector businesses motivated to stop scam activity. Chainalysis data is leveraged by cryptocurrency businesses and financial institutions for transaction monitoring, enhanced due diligence, and, when appropriate, enhancing SAR filings.

At Chainalysis, we also think it is imperative to move beyond reactive compliance and fraud workflows and to develop processes to prevent Americans from falling prey to scams altogether. Furthermore, in the same way that we observe criminals adapt to and leverage technological developments to their own ends, so too can we harness and encourage the use of AI technology to help financial institutions and crypto platforms prevent their customers from sending funds to likely scams.

Chainalysis Alterya provides real-time proactive fraud protection for payments and enhanced fraud detection during KYC for exchanges, blockchains, and wallet providers. Alterya has already helped top crypto exchanges decrease fraud by up to 60%, reduce scam-related disputes, and improve the efficiency of manual operations. Alterya utilizes 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 multiple 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.

Alterya monitors $23B+ in monthly transactions and helps protect hundreds of millions of users across crypto and fiat payment rails, focusing on recipient-side risk and money-mule detection, critical for stopping authorized push-payment (APP) fraud, where victims are socially engineered into authorizing transfers from their own accounts to criminals. Over the past 12 months, Alterya has prevented more than $300 million in losses by supporting customers in proactively reducing fraud. This is what the future of combating scams looks like.

Recommendations

We are encouraged that this Committee is considering ways to strengthen the U.S. response to scams and fraud involving cryptocurrency that target older victims. We suggest a multi-pronged approach to address this complex problem, consisting of four key recommendations:

1. Mobilize a whole-of-government and industry national anti-scam strategy that prioritizes enhanced reporting and collaborative information sharing that can best disrupt scam conglomerates;
2. Leverage technologies designed for both the prevention and remediation of scams;
3. Ensure financial institutions and crypto businesses are incentivized to assist in the prevention of transactions to scams and have appropriate guidance to enable them to do so;

4. Advocate to close gaps in the implementation of AML/CFT standards by FATF members, especially countries that scammers rely on to launder funds defrauded from Americans.

Taken together and properly implemented, these recommendations will help limit financial flows to scammers, either by preventing victims from sending funds in the first place or by dismantling the scam operations themselves. Further details on each of these are provided below:

1. **Create a national anti-scam strategy to orchestrate a comprehensive response which includes centralizing U.S. victim scam reporting, streamlining coordinated action to dismantle scam conglomerates and return funds to victims, and facilitating information sharing between the public and private sectors.**

i. Improved reporting mechanisms

Today, scam victims in America have multiple options for reporting their crimes to federal and local law enforcement. This is one factor contributing to a fragmented approach to combating scams and has hindered our response time and visibility into the true scale of the impact on potential victims, both in the US and abroad.

A centralized reporting database that feeds from state, local, and federal sources is critical to enhancing efficiency and actionable intelligence for cases that lead to the recovery of funds, restitution, and the prevention of additional victims. National coordination could streamline the process of connecting a single victim to a larger scheme that has netted thousands of victims and millions of dollars in funds, optimizing opportunities for disruption, the prospect of returning seized assets to victims, and making scammers less profitable overall. Similarly, Suspicious Activity Reports (SARs) are filed by financial institutions, but the crucial information contained in these reports about specific scams is not accessible to other financial institutions or to entities supporting scam prevention. This lack of information sharing creates blind spots and delays in response, enabling scammers to continue their illicit activities unabated.

ii. Prioritizing information sharing and collaboration

Addressing the challenge of crypto-integrated laundering networks demands a coordinated public-private partnership and a paradigm shift from reactive enforcement against individual platforms to proactive disruption of the underlying networks. By combining law enforcement's legal authorities with the private sector's technical capabilities and blockchain analytics expertise, the industry can more effectively identify and dismantle these services operating across multiple platforms, jurisdictions, and communication channels. On-chain transparency provides unprecedented visibility into these operations, enabling stakeholders to assess the cost and risk of operating large-scale money laundering services. Future intervention strategies must prioritize this collaborative approach to achieve meaningful, lasting disruption of crypto-integrated laundering networks, including Chinese-language money-laundering operations.

Public-private partnerships are already having success. Chainalysis's Operation Spincaster program was designed to disrupt and prevent scams through public-private collaboration by proactively identifying thousands of compromised wallets.[2] This actionable intelligence formed the basis for a series of operational sprints across six countries, including 19 public-sector agencies and 18 crypto exchanges. Over 7,000 leads were disseminated during these sprints relating to approximately USD $187 million of losses. These leads were used to close accounts, seize funds, and build intelligence to prevent future scams.

Further, Chainalysis is a member of the National Elder Fraud Coordination Center, the first-ever national effort that analyzes and assembles private and public sector data and resources into the investigative packages needed by law enforcement to investigate and prosecute criminal fraud rings targeting older Americans. These are examples of how formalized efforts to streamline private-public collaboration can optimize outcomes.

Singapore's Anti-Scam Command (ASCom) serves as a potential model for efficiently combating scams by eliminating silos and working constructively with over 80 private-sector partners. The industry and regulatory bodies must work together to break down these information silos and adopt a more cohesive, collaborative approach to combating cryptocurrency-related scams. This will ensure that the inherent advantages of blockchain technology for tracing and combating financial crime are fully leveraged and that scammers cannot exploit the system due to gaps in communication and information sharing.

The recently announced Scam Center Strike Force and proposed legislation, such as the Scam Compound Accountability and Mobilization Act, will help define and execute an international strategy to take on scam compounds globally. This approach should study the scam supply chain holistically and leverage all levers of government, including law enforcement and regulatory actions, to target the entire scam supply chain, from money launderers to gambling syndicates to compounds to phishing kit developers to data brokers.

2. **Encourage the adoption of advanced technologies to combat scammers' growing sophistication and to prevent and remediate scams across fiat and digital asset rails.**

i. Broaden access to data, tools, and training

[2] "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/.

With the broader adoption of cryptocurrency on the rise, including among illicit actors, it is no longer sufficient to confine knowledge of crypto networks to a small group of technical experts. Rather, government agencies and departments must have the resources to 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 be prioritized if law enforcement doesn't have the analytic tools it needs to connect a low-value scam payment to a larger scam conglomerate that nets tens or hundreds of millions of dollars. Furthermore, we must acknowledge that a significant number of scams likely go unreported; however, the transparent nature of the blockchain enables investigators to identify all potential victim payments into a scam and can vastly expand their case with assistance from cryptocurrency businesses.

While the proposed Guarding Unprotected Aging Retirees from Deception (GUARD) Act would expressly allow federal law enforcement agencies to assist in these cases, we believe this should not replace providing tools and training to state and local agencies so they can help victims in their jurisdictions.

Particular offices within agencies have invested in integrating blockchain analytics into their workflows and achieved significant success, among them IRS Criminal Investigations and the FBI's Virtual Asset Unit. However, the extensive overlap of crypto across many agencies' missions necessitates a broader cohort of agencies and their staff to understand the underlying technology, have access to the same tools, and receive training to encourage more successful outcomes.

ii. Adoption of cutting-edge technology, systems, and tools that move beyond reactive enforcement

While the traditional reactive paradigm of enforcement is important, it is not enough for the speed and scale of scams today. The organized crime groups behind scams move quickly and operate in regions that are difficult to access, making real-time prevention mechanisms a vital line of defense. Given these challenges and the sheer volume of victims, some agencies and investigators across the public and private sectors are now turning to advanced proactive detection techniques.

The future of fraud prevention relies on the deployment of novel technologies such as machine learning and AI. Chainalysis Alterya provides financial institutions with the tools 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 solutions. It identifies scammers before they meet their victims, collecting identifying information about the scammers and the fraudulent scheme. This data is then integrated with customers' transaction-monitoring platforms, providing real-time analysis of scam exposure and enabling them to identify and track interactions with scam addresses, assess risk, and take preventive measures.

All relevant agencies and law enforcement should also have this opportunity to move decisively upstream and take the fight directly to scammers. In such a scenario, rather than simply investigating reported crimes, the public and private sectors could best leverage real-time blockchain data, DNS data, and AI technology to identify, disrupt, and potentially prevent illicit activity.

For example, Chainalysis Alterya can help agencies transform scattered victim reports into mapped scam campaigns that connect wallets, domains, social accounts, and other identifiers, giving agencies a single source of truth on how a fraud network actually operates. That same network view becomes the foundation for case triage and victim support—analysts can quickly see which victims are linked, what other identifiers to pursue, and where to prioritize investigative resources. This network view can also power supervisory analytics and market-wide disruption, enabling agencies to track typologies over time, measure exposure across institutions and rails, and coordinate targeted interventions against the scamming infrastructure that makes these frauds possible in the first place.

Congress should ensure that relevant federal, state, and local agencies have the tools, resources, and legal authorities necessary to: (1) access, analyze, and act on blockchain and other digital intelligence; (2) collaborate effectively with financial institutions, crypto platforms, and other private-sector intermediaries; and (3) integrate AI-enabled risk detection into their investigative, supervisory, and consumer protection workflows. This combination of AI-driven analytics and blockchain intelligence can materially improve our ability to detect, disrupt, and deter scams at scale, while strengthening restitution outcomes for victims and raising the cost of doing business for organized scam networks.

3. **Provide guidance to financial institutions and crypto businesses to help them prevent customers from sending funds to scams and intervene when scam-detection technology identifies risk.**

Although the technology exists for cryptocurrency businesses and financial institutions to detect when a customer is trying to send funds to a scam wallet, they lack the legal basis to hold a customer's funds. Even after a crypto business warns a customer that they are trying to send funds to a scam, more often than not, the customer is so duped by the scammers that they will still opt to release their funds to the scammer. The U.S. Government should establish clear, consistent guidelines for how financial institutions and cryptocurrency businesses may intervene when they suspect customers are being targeted by scams, so that firms are not forced to choose between overreaching into consumers' access to their own funds and passively facilitating payments into organized scam networks.

Today, banks and crypto platforms lack standardized expectations and a legal basis around when and how they can slow, block, or scrutinize suspicious transactions, and what forms of customer outreach and friction are appropriate in these scenarios. With better access to data, typologies, and public-private information sharing, these institutions would be far better equipped to strike the right balance between consumer protection and customer autonomy. Congress should therefore direct regulators to issue guidance that encourages the use of advanced fraud-prevention technologies, such as Chainalysis Alterya, which enable financial institutions and cryptocurrency businesses to detect and prevent likely scam payments in real time. These tools have already demonstrated that they can significantly reduce authorized push payment (APP) fraud losses, lower the volume of customer disputes, and help institutions retain customers by protecting them from devastating financial harm while preserving safe access to their own money.

One solution could be to implement an optional, scams-specific hold on funds, backed by liability protections, that allows stablecoin issuers, cryptocurrency businesses, and financial institutions to temporarily stop suspicious transactions as soon as they or law enforcement identify red flags.

4. **Close gaps in AML/CFT standards implementation for FATF members, especially countries that host scam compounds and the services they rely on to launder funds defrauded from Americans.**

More capacity building is needed in jurisdictions with weak AML and CFT policies – particularly across Southeast Asia, where scam compounds operated by Chinese transnational criminal organizations and their local partners have become major hubs for large-scale fraud targeting Americans and other victims worldwide. These same networks increasingly rely on Chinese-language money laundering services as key vehicles for laundering the proceeds of these schemes and cycling them back into the global financial system. 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 that defy international norms and AML/CFT processes and standards – would help cut off scam perpetrators and their facilitators from the global financial system.