Testimony of Ari Redbord, Global Head of Policy, TRM Labs

Joint Hearing by the Subcommittee on Border Security and Enforcement and the Subcommittee on Cybersecurity and Infrastructure Protection on Online Scams, Crypto Fraud, and Digital Extortion: An Examination of How Transnational Criminal Networks Target Americans

April 21, 2026

Introduction

Chairs Guest and Ogles, ranking members Correa and the ranking member of the Subcommittee on Cybersecurity and Infrastructure Protection, and distinguished members of both subcommittees, my name is Ari Redbord. I am honored to appear before you on behalf of TRM Labs, where we work every day with law enforcement, financial institutions, and national security agencies to detect, investigate, and prevent illicit activity in the digital asset ecosystem and beyond.

Before joining TRM, I spent more than a decade as a federal prosecutor at the United States Department of Justice and later served as a senior official at the US Treasury Department's Office of Terrorism and Financial Intelligence. In those roles, I confronted terrorist financiers, sanctions evaders, narcotics trafficking organizations, and transnational criminal enterprises operating across jurisdictions and continents.

I do not say this lightly: I have never seen a financial crime threat as pervasive, as economically destructive, or as dangerous to ordinary American families as the one I am here to describe today.

I want to begin with something that I think gets lost in the conversation about transnational criminal organizations. We talk about TCOs operating from compounds in Southeast Asia. We talk about Chinese underground banking networks processing hundreds of billions of dollars. We talk about North Korean hackers operating thousands of miles away.

All of that is real, and I will address each of those threats in detail.

But I want this committee to understand who is actually being harmed. It is a grandmother in Ohio who sent tens of thousands of dollars to someone she believed was her grandson in distress, only to learn it was a scammer exploiting her trust. It is a 40-something in North Carolina who believed she had found both a relationship and an investment opportunity, after months of daily communication, and lost everything he had, including money borrowed from her parents. It is a veteran in Texas who transferred his home equity to what he believed was a legitimate investment platform after weeks of engagement with someone posing as a trusted advisor. It is a family in New York whose life savings were gone in 72 hours, moved across seven cryptocurrency wallets in three countries before they even realized what had happened.

These are not victims of some distant financial abstraction. They are our constituents, and the criminal networks that target them are sophisticated, well-resourced, and operating at industrial scale against the American public.

We need to get this right — and we need to do it together — because these are not abstract losses, they are life savings, homes, and futures of Americans, and the networks taking them are organized, relentless, and scaling faster than our response.

About TRM Labs

TRM Labs is a blockchain intelligence company that works with hundreds of financial institutions, cryptocurrency businesses, and law enforcement and national security agencies worldwide. Our AI-powered platform allows investigators to follow illicit money wherever it moves, tracing cryptocurrency transactions through wallets, exchanges, mixers, and cross-chain bridges to help investigators build investigations and mitigate risk.

We also publish original research on crypto crime trends, threat actor behavior, and the evolving intersection of digital assets and national security, including the annual TRM Crypto Crime Report, which serves as a foundational resource for policymakers, law enforcement, and compliance professionals worldwide.

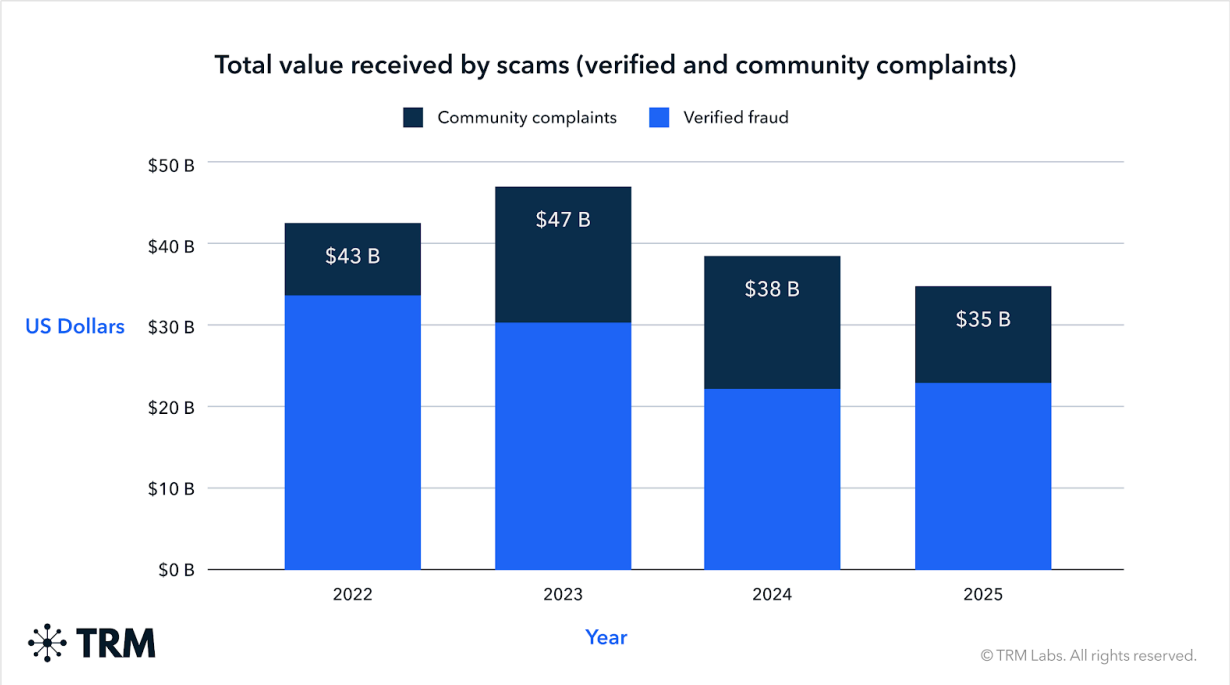
I want to be clear about what blockchain intelligence actually provides in the context of the threats before this committee. When a victim of a pig butchering scam sends cryptocurrency to a fraud platform, that transaction is recorded on a public, permanent, immutable ledger.

The wallet that received those funds can be traced. The subsequent movement of those funds through additional wallets, exchanges, and obfuscation techniques can be followed with the right tools and training. Unlike cash, which disappears into the financial system anonymously, cryptocurrency leaves a trail. The challenge is not that the evidence does not exist. The challenge is that law enforcement, financial institutions, and policymakers do not always have the tools, the legal authority, or the coordination frameworks to act on that evidence fast enough to matter.

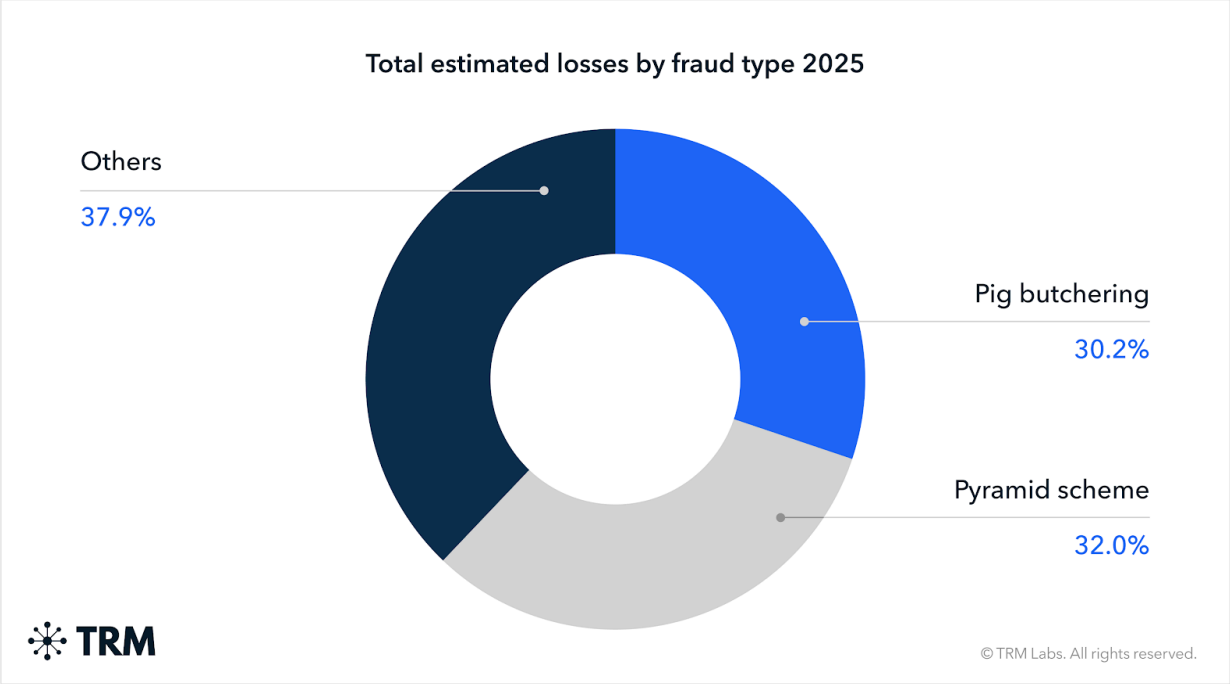
The scope of the problem

TRM's 2026 Crypto Crime Report documented approximately USD 158 billion in illicit cryptocurrency flows in 2025 — a 145% increase from USD 64.5 billion in 2024 and the highest level recorded in five years. Fraud and scams alone accounted for roughly USD 35 billion in confirmed flows to fraud-linked wallets.

The FBI's Internet Crime Complaint Center has documented record losses from cyber-enabled fraud, with investment fraud and romance scams representing the fastest-growing and most devastating categories of victim harm. But those figures capture only what victims report. TRM estimates that only about 15% of victims come forward — deterred by shame, skepticism that law enforcement can help, or simple uncertainty about where to turn. When that underreporting gap is factored in, global annual losses from cyber-enabled fraud against individuals likely exceed USD 200 billion.



Verified fraud activity from TRM Labs and Beacon Network, as well as alleged fraud activity sourced from Chainabuse, a victim reporting platform.



But scams are only one category of illicit activity driven by transnational criminal networks. Sanctions evasion, driven largely by Russia-linked activity and the rapid growth of the ruble-pegged stablecoin A7A5, surged over 400% year over year. Cryptocurrency stolen through hacks reached USD 2.87 billion across nearly 150 incidents in 2025, with North Korea responsible for USD 1.92 billion of that total.

How transnational criminal organizations operate

Pig butchering and scam centers

The dominant fraud typology driving the losses I have just described is commonly known as pig butchering, a term originating from the Chinese phrase "sha zhu pan," which describes the practice of "fattening" a victim financially before the slaughter. Understanding how these operations actually work is essential to understanding both the scale of the problem and the nature of the policy response required.

These operations begin with weeks or months of deliberate, patient relationship-building — conducted over messaging apps, dating platforms, social media, and even text messages sent to wrong numbers — a technique criminals use to establish initial contact. The operator, often working from an organized compound staffed by hundreds of people, establishes genuine emotional connection with the target before any financial matter is raised. Victims describe feeling that they had found a genuine friend, romantic partner, or trusted mentor.

Only after that relationship has been cultivated does the operator introduce investment, typically framed as an opportunity being shared out of personal generosity. Victims are shown a professional-appearing trading platform, given access to fabricated account dashboards showing growing returns, and permitted to make small early withdrawals to establish credibility. When the victim has committed the maximum available funds, including frequently borrowed money or retirement savings, the platform disappears. Customer service stops responding. The money is gone.

What is critical for this committee to understand is that these operations are not the work of individual grifters. They are organized enterprises operating with the discipline and infrastructure of multinational corporations.

The compounds in Myanmar, Cambodia, and Laos are large physical facilities, some housing thousands of workers. In many documented instances, those workers are themselves victims of human trafficking, recruited with false promises of legitimate technology or hospitality jobs and held under threat of violence, debt bondage, or confiscation of passports.

The networks running these compounds are affiliated with Triad-connected organized crime syndicates that have operated in Southeast Asia for decades, and they have brought to cyber fraud the same organizational sophistication they applied to narcotics, gambling, and human trafficking operations. The business model is extraordinarily efficient. Operating costs are low, victim conversion rates are measurable and optimizable, and the proceeds are laundered through established underground banking networks that have moved value across borders for generations.

Investigating pig butchering

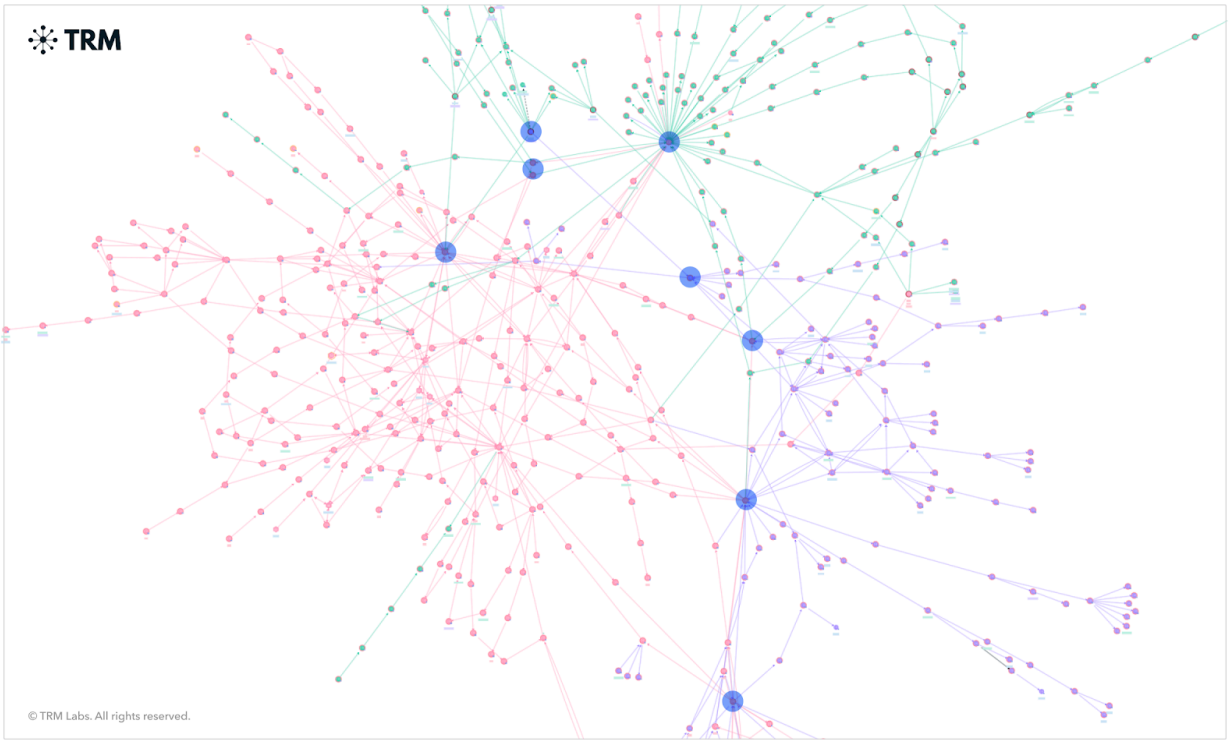
Investigations involving networks of scammers are often complex. TRM's analysis of on-chain transaction data, combined with proprietary source intelligence, has identified several key characteristics of pig butchering scams.

Once cryptocurrency reaches a scammer's wallet, it is typically shuffled from wallet-to-wallet in a complex web of transactions between scammers and money launderers (sometimes the same people), with each wallet accumulating funds from additional victims along the way. Funds often move circuitously, making it difficult for investigators to follow the money and to separate victim funds from other tokens. These fund movements consistently include multiple hops through intermediary addresses.

Victim funds typically end up reaching a few main exchanges, where they are often swapped for stablecoins before continuing to be cycled through the money laundering network both via the main exchanges and unhosted wallets.

TRM data indicates that cryptocurrency wallets that receive victim funds from individual pig butchering scams are also often associated with other scams. Furthermore, in a random sample of addresses to which victims stated they sent funds, over 75% exhibited signs of sophisticated on-chain money laundering activity.

The below graph illustrates a typical example of a pig butchering scheme studied by TRM Labs, showing the interconnected networks spanning multiple scams. Each color represents the scammer addresses in three different cases. As shown by the connections between the three coloured webs, the scammers appear to be operating multiple scams either in succession or in conjunction. In addition, the scammers appear to be relying on the same underlying money laundering network, with the same addresses appearing in multiple cases.



This TRM graph illustrates a typical example of a pig butchering scheme showing the interconnected networks spanning multiple scams.

Chinese money laundering networks

The proceeds of pig butchering operations, narcotics trafficking, and every other major illicit finance stream documented by TRM flow through the same critical infrastructure: Chinese underground banking networks that have become the dominant professional money laundering system in the world.

TRM's Shadow Bankers report documented that Chinese-language escrow and money laundering networks processed over USD 103 billion in 2025, growing from approximately USD 123 million in 2020. That growth reflects both the explosion of cryptocurrency as a settlement mechanism and the organizational sophistication of the networks operating them.

These underground banking systems operate through what are known as mirror exchange arrangements. A broker collects cartel cash in the United States and provides equivalent value through off-record methods to a counterpart in Mexico or elsewhere, keeping dollars in the United States and making value available abroad without any cross-border wire transfer occurring. Cryptocurrency has made these arrangements faster and cheaper.

Brokers coordinate through encrypted messaging applications like WeChat and Telegram, using code words and cultural reference points that exploit the language and cultural barriers facing Western law enforcement. Transactions are layered through mixers, cross-chain bridges, privacy coins, and rapid micro-transactions across multiple blockchains to break investigative trails.

These networks do not exclusively serve one criminal constituency. They serve Mexican cartels laundering narcotics proceeds, North Korea converting stolen cryptocurrency to usable currency, pig butchering fraud operators moving victim funds to safety, Russian sanctions evaders moving value outside the traditional financial system, and Iranian actors funding weapons procurement networks.

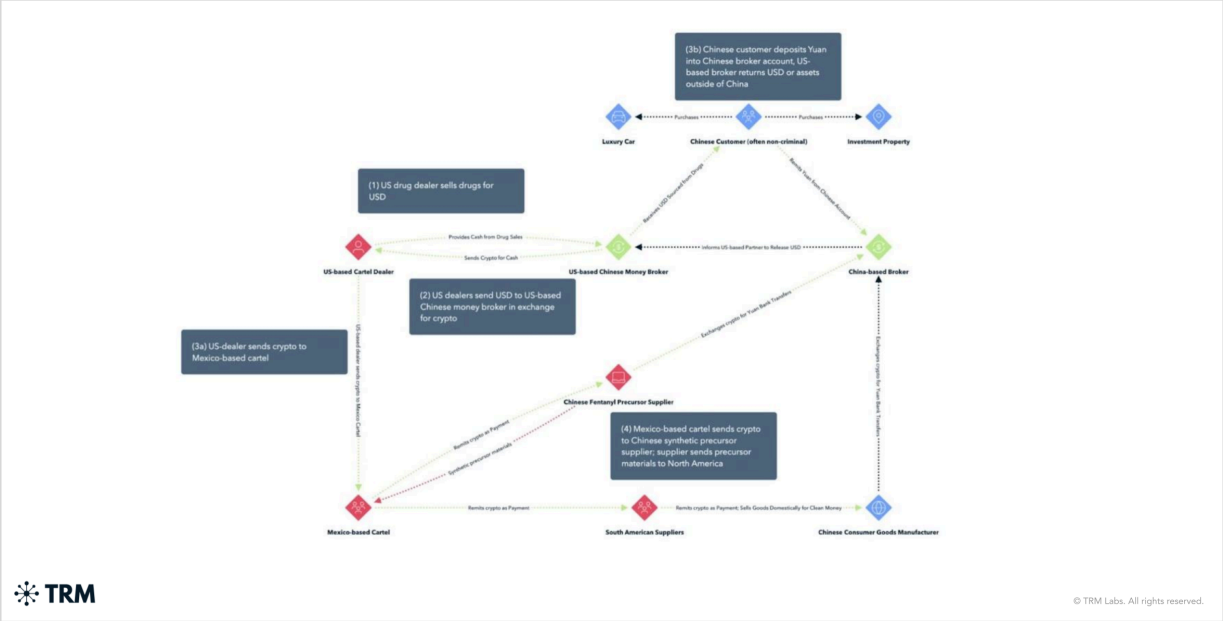
In one documented case that TRM tracked, a Los Angeles-based operation laundered over USD 50 million in Sinaloa Cartel narcotics revenue through Chinese underground bankers using trade-based schemes layered with cryptocurrency transactions. The same brokers who handled that transaction were handling fraud proceeds from Southeast Asian scam operations. The financial infrastructure of transnational crime is not siloed by crime type. It is shared, interconnected, and mutually reinforcing.

FinCEN's designation of Huione Group (a Cambodia-based network) as a primary money laundering concern in 2025 identified that organization as receiving USD 39.6 billion in transaction volume. That single designation illustrates the scale at which these networks operate and the degree to which they have become embedded in the global financial system.

Mexican cartels and the southern border

Over the last few years, the cartels have integrated cryptocurrency into their operations; the connection to the southern border is direct and concrete. TRM research on cartel cryptocurrency use documented that of more than 120 Chinese companies supplying precursor chemicals for fentanyl and methamphetamine production, 97% were willing to accept cryptocurrency payments.

Mexican cartels, including the Sinaloa Cartel and its affiliated networks, are using cryptocurrency to purchase the chemical inputs for fentanyl production from Chinese suppliers to compensate workers and operatives across multiple jurisdictions, and to launder drug proceeds through layered wallet transactions and Chinese underground banking arrangements.



TRM Graph Visualizer, with explanations, showing how the cartels and Chinese brokers use cryptocurrencies to launder drug money.

These are not isolated transactions. They are systematic. In June 2024, a Department of Justice indictment charged Edgar Joel Martinez-Reyes with leading a network that used trade-based money laundering and cryptocurrency purchases to clean drug proceeds, with law enforcement seizing USD 5 million in cash and significant drug quantities in connection with that case. In January 2024, Martin Mizrahi was convicted of converting bulk narcotics cash into Bitcoin and layering transactions through multiple wallets.

OFAC has made its first public identifications of cartel cryptocurrency addresses on the Ethereum blockchain and has sanctioned 17 cryptocurrency addresses linked to fentanyl precursor suppliers.

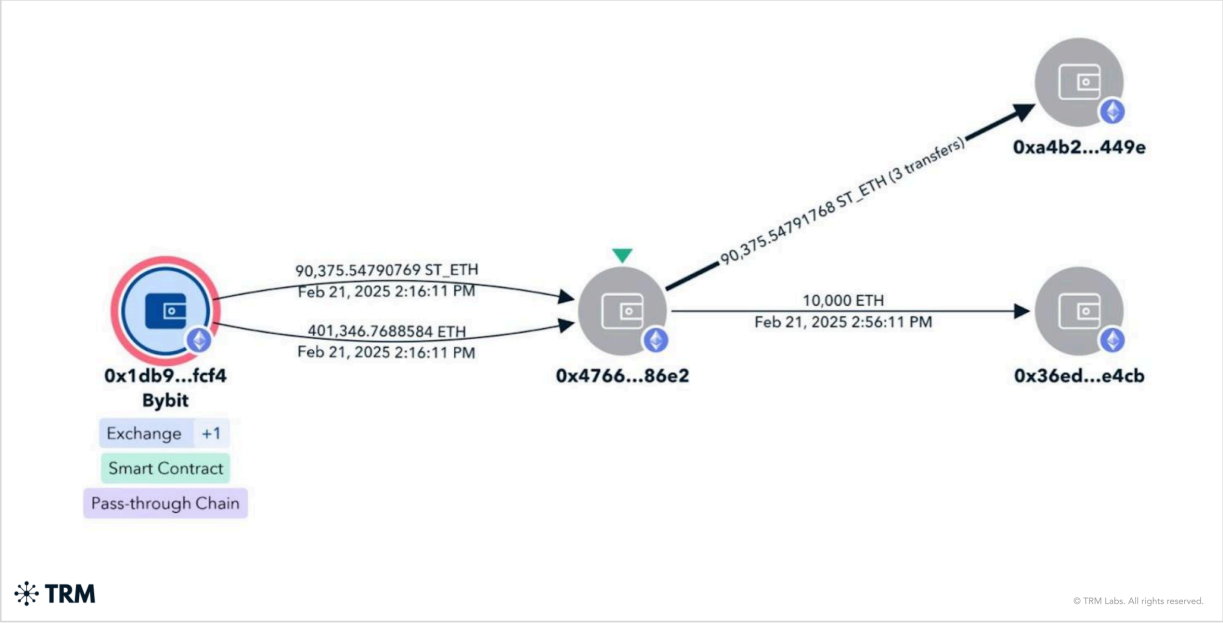
The implication for this committee is that the digital technology question and the border security question are not two separate inquiries. The financial infrastructure enabling fentanyl trafficking into the United States and the financial infrastructure laundering the proceeds of fraud committed against American citizens are substantially the same infrastructure.

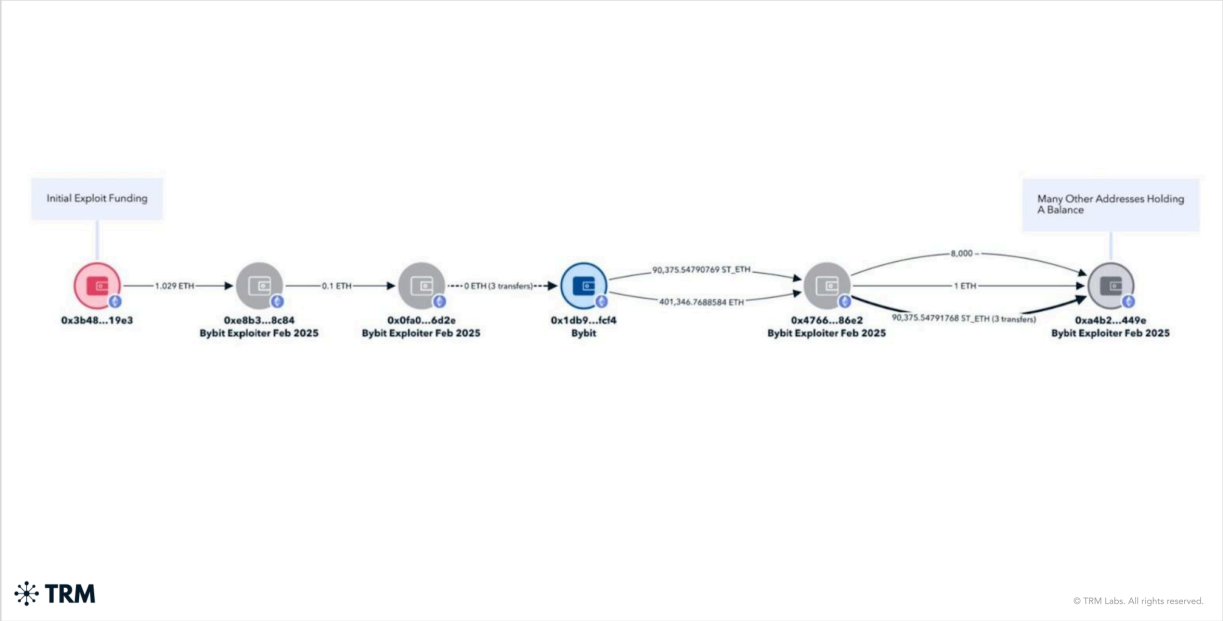
North Korea: A national security imperative

North Korea stole approximately USD 1.92 billion in cryptocurrency in 2025, including the February 2025 hack of Bybit, where USD 1.46 billion was taken in what stands as the largest single cryptocurrency theft in history.

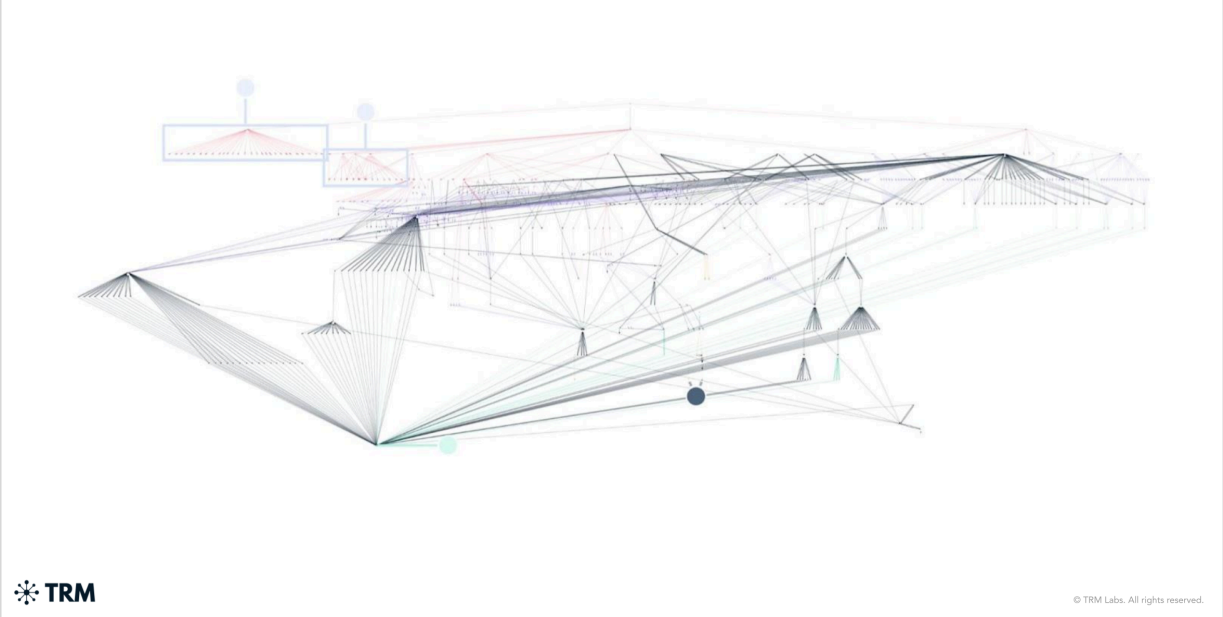
The scale of the theft is matched by the speed and sophistication of the laundering that followed. Within days, nearly all stolen Ether was bridged into Bitcoin using decentralized protocols, reflecting what TRM identified as an unprecedented level of operational efficiency. The funds were then funneled through mixers, cross-chain bridges, and decentralized exchanges, creating rapid layers of obfuscation designed to frustrate tracing and delay interdiction.

Such rapid layering suggests an expansion of North Korea's laundering infrastructure — likely with greater support from underground networks in China to absorb and process the funds. Indeed, once the initial obfuscation was done, a large portion of the assets sat idle, presumably awaiting liquidation through OTC channels that can handle converting tens of millions without detection.





Funds moving off of ByBit after the initial hack, as shown in TRM Graph Visualizer.



The rapid laundering process, as of February 26, 2025, includes transfers through multiple intermediary wallets, conversion into different cryptocurrencies, and the use of DEXs and cross-chain bridges to obfuscate the trail.

This activity reflects a broader evolution in North Korea's laundering playbook. Rather than relying on slower, linear laundering techniques, these actors now move assets through

complex, multi-chain transaction paths almost immediately after a hack. The goal is clear: maximize speed, fragment the trail, and position funds for eventual off-ramping. Following the initial laundering phase, a significant portion of the Bitcoin sat idle, likely staged for liquidation through over-the-counter brokers capable of handling large volumes without triggering compliance controls.

Those OTC networks are central to the ecosystem. North Korea's Foreign Trade Bank representative Sim Hyon-sop has been linked to coordination with China- and Hong Kong-based brokers who facilitate the conversion of stolen crypto into fiat currency through exchanges and shell companies. These networks provide the critical bridge between illicit on-chain activity and the traditional financial system, enabling the regime to operationalize stolen digital assets at scale.

At the same time, Russia-based exchanges have continued to play a key role as downstream laundering venues. Garantex, long associated with illicit finance, rebranded as Grinex within days of an OFAC enforcement action, underscoring how quickly these platforms adapt to sanctions pressure. These exchanges remain preferred destinations for both North Korean and Russian criminal actors, reinforcing the interconnected nature of these illicit financial ecosystems and the challenges of disruption.

This is a state-directed financial strategy — not opportunistic crime. The proceeds from these operations directly support North Korea's nuclear and ballistic missile programs. A single operation yielding USD 1.46 billion represents a meaningful contribution to a weapons of mass destruction program. Disrupting these flows is therefore not simply a matter of financial crime enforcement — it is a national security imperative, requiring coordinated, whole-of-government action at the same level of urgency applied to other systemic threats.

The Russia-China-North Korea nexus

What TRM's data reveals is not a collection of separate criminal threats but an interconnected illicit finance ecosystem in which state sponsors, criminal networks, and technical infrastructure are deeply intertwined. North Korea supplies the hackers and cyber capabilities. Russia provides the criminal marketplace infrastructure and technical tools. China furnishes the financial plumbing through underground banking networks and OTC brokers. Scam center operators in Southeast Asia generate the fraud proceeds that flow through the same networks that launder cartel drug money and North Korean stolen cryptocurrency.

The A7 sanctions evasion platform, operated from Russia, processed at least USD 56 billion in 2025. Nearly 95% of sanctioned entity inflows used stablecoins, meaning that dollar-denominated digital assets are serving as the reserve currency of the global illicit finance system. Blockchain data tells us this.

Artificial intelligence as a force multiplier for criminal organizations

Artificial intelligence has transformed the operational capabilities of criminal enterprises at a pace that demands the most urgent policy response this committee can deliver.

In testimony before the House Judiciary Subcommittee on Crime and Federal Government Surveillance in July 2025, I described how the early adoption of AI by TCOs from scammers to ransomware gangs, poses a civilization level threat.

Generative AI-enabled scam activity rose 500% over the last year, according to data from Chainabuse, TRM's open-source scam reporting platform. Deepfake technology now enables real-time face and voice swapping during live video calls, allowing criminals to impersonate financial professionals, family members, government officials, and even romantic partners with sufficient fidelity to deceive careful, intelligent people.

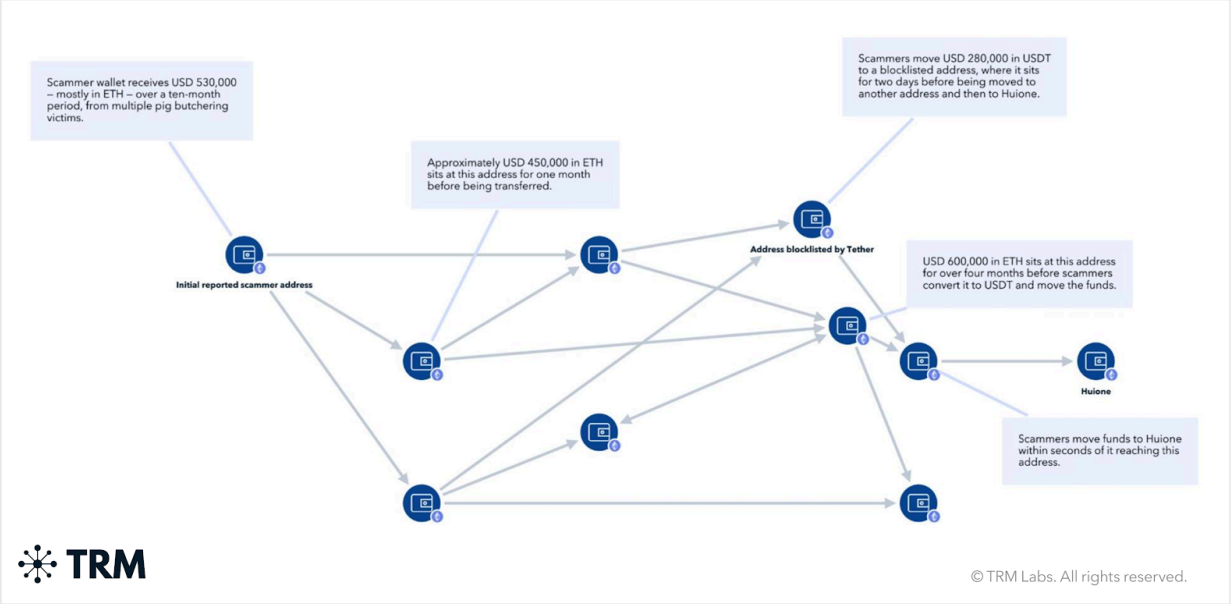
A Hong Kong company lost millions of dollars when employees participated in a board meeting that appeared to include legitimate company executives, all of whom were AI-generated impersonations. Romance scam operators are now deploying AI systems that conduct initial outreach, maintain ongoing emotional engagement across dozens of simultaneous victim relationships, and adapt their communication style in real time based on victim responses, all without a human operator being involved in the conversation.

AI-generated synthetic identity documents are available on criminal marketplaces for as little as USD 15 per document, enabling fraudsters to open accounts at regulated cryptocurrency exchanges and bypass Know Your Customer (KYC) controls at a scale that manual document forgery could never achieve. AI allows criminal networks to operate multilingual outreach campaigns simultaneously, removing the language barrier that previously limited the geographic reach of individual fraud operations. AI-powered ransomware creates polymorphic

malware that evades detection systems by constantly rewriting its own code, and identifies high-value targets based on financial data scraped from public sources.

AI's impact is visible not just in outreach and engagement, but also in laundering tactics. AI accelerates the rotation of infrastructure, the creation of synthetic identities, and the spread of fraudulent domains and social media personas, enabling scam networks to iterate rapidly across platforms and choke off investigative visibility before responses can materialize. In practical terms, what once required teams of human actors now often requires only the right prompt engineering and an AI engine capable of consistent execution.

Deepfake tool used in a scam center in Cambodia and Thailand (Source: UNODC).



TRM graph showing typical scam laundering pattern.

Blockchain data confirms this speed acceleration: average wallet holding periods for scam proceeds have decreased significantly. Funds now move across multiple wallets and chains within 24 to 48 hours of receipt, dramatically narrowing the window for meaningful interdiction and recovery.

Fraud, and the laundering of illicit proceeds, has evolved into a coordinated, AI-assisted industry operating at global scale.

Our response must reflect that reality.

The response to this acceleration in AI cannot be the restriction of AI technology or an attempt to slow innovation. It has to be ensuring that the tools of safety evolve just as quickly as the tools of harm. At TRM, that means pairing advanced AI with human expertise—using AI to map illicit networks in real time, identify patterns, triage risk, and surface early warning signs, while enabling analysts and investigators to act faster and make more informed decisions. AI brings speed and scale, but it is the human judgment layered on top that turns insight into action and drives effective disruption.

These systems operate with guardrails that ensure every action is auditable, every output is traceable, and human analysts remain in the decision-making loop for consequential actions. The private sector has built these capabilities. The question for this committee is whether law

enforcement will have the resources, training, and legal authority to deploy them at the speed the threat demands.

The Executive Order: A critical and historic framework

On March 6, 2026, President Trump signed an Executive Order on Combating Cybercrime, Fraud, and Predatory Schemes Against American Citizens. This order represents the most important federal policy development on cyber-enabled fraud. Its implementation will determine whether the victims I described at the outset of this testimony see a meaningful change in their protection.

The order begins from the correct diagnosis: that transnational criminal organizations are conducting coordinated campaigns of cybercrime, fraud, and predatory schemes against American citizens, that these campaigns are draining American families of their life savings, and that they constitute a national security threat as well as a financial crime problem.

That framing matters because it determines which tools are available in response. A financial crime problem is handled by financial regulators and law enforcement. A national security threat commands the full toolkit of American power, including diplomatic pressure, targeted sanctions, visa restrictions, trade consequences, military and intelligence resources, and whole-of-government coordination.

The EO creates an operational cell within the National Coordination Center to coordinate federal efforts to detect, disrupt, dismantle, and deter cyber-enabled criminal activity. It directs the Secretary of State to engage with foreign governments to demand enforcement actions against TCOs operating on their soil. And it explicitly contemplates consequences for nations that tolerate predatory activity targeting American citizens, including targeted sanctions, visa restrictions, trade penalties, and limitation of foreign assistance.

The order also directs the Attorney General to submit recommendations for a Victims Restoration Program that would provide restitution to victims of cyber-enabled fraud schemes from funds seized from criminal networks. This provision matters enormously to the people I described at the outset of this testimony. The grandmother who lost her retirement account, the veteran who lost his home equity, the family whose savings were gone in 72 hours — they

need to know that law enforcement success means something tangible for them, not just a press release about an indictment.

The reason this order is historically significant is not just its content but its accountability structure. For years, the US government's response to cyber-enabled fraud against Americans was fragmented across dozens of agencies, reactive rather than proactive, and consistently under-resourced relative to the scale of the threat.

Scam center operators in Myanmar, Cambodia, and Laos operated with effective impunity because no single agency had both the authority and the mandate to coordinate a comprehensive response. Every agency involved in this space holds a piece of the puzzle. The FBI handles cyber crime investigations. OFAC handles sanctions designations. DEA handles narcotics trafficking. HSI handles human trafficking and money laundering. The State Department handles foreign policy. FinCEN handles financial intelligence. But without a coordination mandate and a clear accountability chain, those pieces rarely come together into a coherent strategy.

The EO creates that accountability. It names responsible officials, sets deadlines, and signals at the highest levels of government that the full toolkit of American power will be brought to bear on the organizations running these schemes. TRM is committed to working with executive branch agencies and this committee to ensure that the EO has a lasting impact on the victims of these criminal networks.

The Scam Center Strike Force and law enforcement efforts

Beyond the EO, the US government is responding to the global threat of transnational criminal networks that have industrialized fraud. In November 2025, the US Department of Justice launched the Scam Center Strike Force to coordinate efforts to dismantle these networks, disrupt their infrastructure, and recover stolen funds.

What distinguishes the Strike Force is its whole-of-government approach, bringing together law enforcement, financial regulators, and national security agencies to address a threat that spans jurisdictions and financial systems. In addition, the Strike Force leverages the Beacon Network and other private sector initiatives in order to bring every resource to bear.

The DOJ leads prosecutions and asset seizures, while agencies like the FBI, HSI, DEA, IRS-CI and US Secret Service conduct investigations and blockchain tracing. Treasury components, including OFAC and FinCEN, apply sanctions and financial intelligence tools to target the laundering networks that move illicit proceeds, while the State Department supports international coordination. This integrated model reflects the reality that these fraud networks operate across borders and rely on both crypto and traditional financial rails.

More broadly, the initiative signals a shift in how governments are approaching crypto-enabled fraud — treating it as a systemic national security threat that demands sustained, coordinated action across law enforcement, financial, and diplomatic channels.

There are also other efforts. Law enforcement agencies and private sector partners across the US, Asia, and Europe have launched specialized task forces to respond to pig butchering scams, including Operation Shamrock, the FBI's Operation Level Up, and Europol's European Financial and Economic Crime Centre (EFECC).

The Homeland Security Task Force (HSTF), announced in early 2025, represents a whole-of-government response to transnational criminal organizations operating within the United States. Co-led by the FBI and Homeland Security Investigations, the task force integrates federal, state, and local law enforcement into a single operational framework designed to identify, target, and dismantle cartels, foreign gangs, human trafficking networks, and financial crime infrastructure. With more than 8,500 federal agents and analysts working alongside over 440 state and local agencies across all 52 states and territories, the model embeds intelligence, personnel, and operational coordination nationwide to break down silos and enable unified, intelligence-driven action.

In just its first year, HSTF has delivered results at scale, including more than 3,200 arrests, over 200,000 pounds of drugs seized, more than 1,000 illegal firearms recovered, and hundreds of coordinated operations in a concentrated enforcement period.

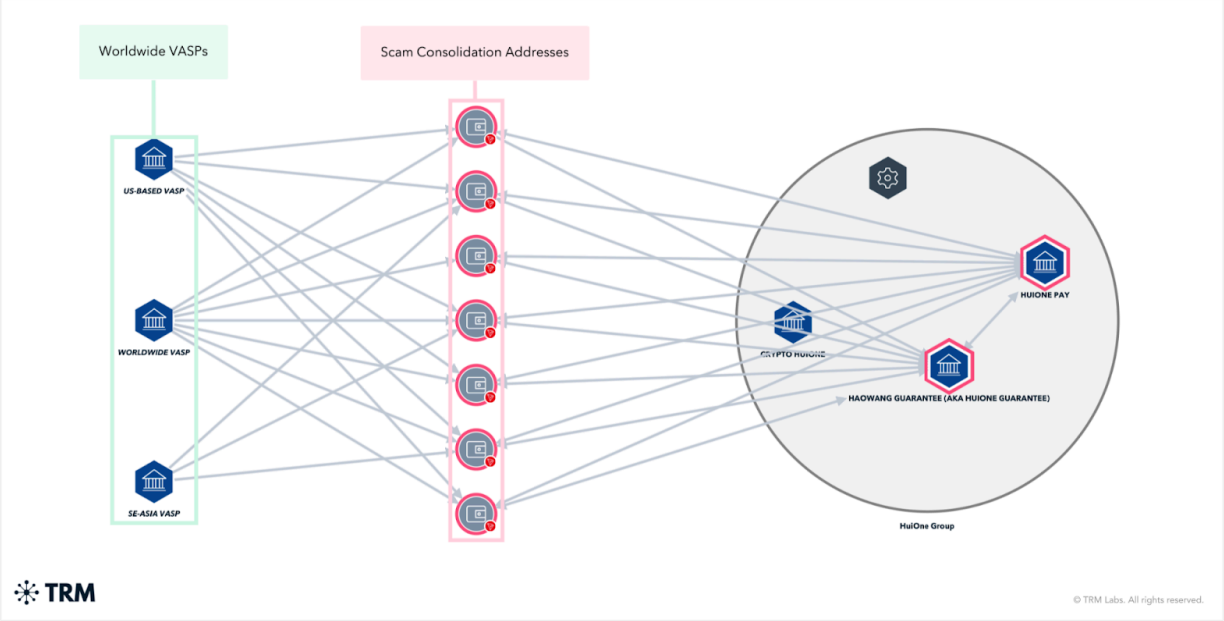
Over the last few years, US authorities have seized billions of illicit proceeds from hacks, ransomware groups, scam networks, and other threat actors. For example, in October 2025, the US Department of Justice announced the indictment of Cambodian national Chen Zhi, founder and chairman of Prince Holding Group, a multinational conglomerate based in Cambodia. Zhi was charged with wire fraud conspiracy and money laundering conspiracy for directing Prince Group's operation of forced-labor scam compounds across the country.

In a parallel action, the DOJ filed a civil forfeiture complaint for 127,271 bitcoin — valued at more than USD 15 billion — now in the custody of the US government. The filing marks the

largest forfeiture action in US history, underscoring both the scale of the criminal network and the unprecedented reach of law enforcement's response.

Concurrently, OFAC is working with the UK Foreign, Commonwealth, and Development Office (FCDO), which sanctioned 146 targets linked to the Prince Group. In addition, FinCEN finalized its Section 311 order against the Huione Group, cutting the organization — and any intermediary bank — off from the US dollar system.

At its core, Operation Prince shows how governments are evolving to confront industrial-scale crypto-enabled fraud — aligning prosecutions, financial intelligence, sanctions, and international coordination to disrupt networks, seize assets, and hold leadership accountable. It underscores that tackling transnational scam networks requires a sustained, integrated approach targeting both on-chain activity and the off-chain enablers that allow these ecosystems to scale.



As shown in TRM Graph Visualizer Huione Group was involved in laundering illicit funds such as cybercrime, cyberfraud, and DPRK-controlled assets.

While the Prince Group takedown is a significant win for global security, similar networks continue to operate worldwide.

Beacon Network

The private sector has built infrastructure that is ready to support the whole-of-government approach outlined in the Executive Order.

TRM's Beacon Network is the first real-time, global intelligence-sharing system for illicit cryptocurrency activity, built in collaboration with leading platforms including Coinbase, Binance, Kraken, PayPal, Ripple, Stripe, Robinhood, Crypto.com, and Zodia Custody. The network connects verified participants across the public and private sectors — including approximately 70 law enforcement agencies worldwide, many within the United States — enabling them to flag illicit wallets and transactions as activity unfolds. By sharing actionable intelligence in real time, Beacon allows investigators and compliance teams to move at the speed of the threat — freezing funds, seizing assets, and disrupting transnational criminal networks before illicit proceeds can be laundered beyond reach.

The network operates through four steps: verified investigators flag illicit wallet addresses in TRM's system; flagged funds are automatically tracked across the blockchain in real time; when those funds reach a participating exchange or financial institution, Beacon sends an immediate alert; and the institution reviews the risk level and coordinates with law enforcement before processing any withdrawal.

The network currently covers approximately 85% of centralized cryptocurrency transaction volume, meaning that when scam proceeds hit a major exchange, there is a high probability that a Beacon alert will fire before the criminal can cash out.

The Scam Center Strike Force and the HSTF — combined with the EO, legal authority to compel holds, diplomatic leverage to pressure host nations, and operational access to Beacon's alerting capability — could represent a fundamentally different kind of enforcement infrastructure than anything the US government has previously fielded against this threat.

Solutions: What Congress can do

The Executive Order creates the framework. Congress must now provide the legal authorities, tools, and resources to make that framework operational and durable.

Enact a digital assets "hold law"

Congress should enact a digital assets "hold law," which would create a legal safe harbor allowing cryptocurrency exchanges to temporarily freeze funds linked to suspected illicit activity, pending legal process from law enforcement. The language for such a law exists today in the Senate Banking Committee's draft of the "Digital Asset Market Clarity Act."

Traditional banks have had this authority for decades. When a bank compliance officer identifies a suspicious wire transfer, they can place a hold while the matter is reviewed. Cryptocurrency exchanges operating under current law lack that clear authority. Every hour of legal uncertainty is an hour that criminal networks use to move funds to the next wallet and beyond recovery. Closing this gap would transform the speed at which the private sector can act on law enforcement intelligence.

Fund and scale real-time intelligence sharing

Real-time disruption and interdiction should be codified as a core pillar of US digital asset policy — embedding networks like Beacon into the regulatory framework as a standard capability across the ecosystem.

These models demonstrate how the private sector's real-time visibility can be paired with government authorities to freeze funds, seize assets, and disrupt illicit activity before it scales. The Senate Banking Committee's market structure discussion draft already moves in this direction, emphasizing enhanced public-private coordination and anti-money laundering obligations as part of a broader effort to address illicit finance risks in digital assets.

To operationalize this, Congress should prioritize policies that scale participation and remove friction. That includes dedicated federal funding to expand real-time intelligence-sharing networks — especially for smaller platforms that are often targeted as compliance weak points — and a formal legal framework that provides liability protection for firms acting on law enforcement intelligence. Illicit actors deliberately migrate to the edges of the ecosystem; closing those gaps requires both resources and clear rules that enable rapid, coordinated action across platforms and jurisdictions.

More broadly, this should be treated as a best practice across the industry. Digital asset firms should be expected to participate in real-time intelligence networks, integrate rapid response capabilities into compliance programs, and act immediately on high-confidence illicit

indicators. The future of effective enforcement is not retrospective analysis — it is coordinated, real-time disruption powered by public-private collaboration.

Deploy AI investigative capacity at scale across federal agencies

Congress should fund the development and deployment of AI-powered investigative tools across IRS Criminal Investigation, FinCEN, OFAC, the FBI, DEA, Secret Service, HSI, national security, and defense agencies. The criminal networks before this committee are deploying AI autonomously and at scale. Responding with 20th century investigative tools against 21st century criminal infrastructure is not a viable strategy. Federal agencies need the funding, the procurement authority, and the legal frameworks to acquire and deploy these capabilities at the speed the threat demands.

Explore cyber "letters of marque"

We live in a moment where the private sector holds much of the critical data and the public sector holds the authorities — but success depends on fusing the two in real time.

Effective disruption requires ensuring government has access to actionable intelligence while enabling trusted private sector actors to move quickly, within clear legal frameworks, to freeze funds, identify bad actors, and dismantle criminal networks as activity unfolds. That reality should drive a more forward-leaning policy approach: granting narrowly scoped, government-authorized authorities for vetted private actors to take targeted action against the technical infrastructure of transnational criminal organizations.

There is a strong conceptual foundation for this model. Historically, governments have extended limited authorities to private actors to address threats that outpaced traditional state capacity. In the digital context, this could take the form of what might be called "cyber letters of marque," "authorized disruption authorities," or a structured "white hat intervention" framework — mechanisms that allow approved entities, operating under strict oversight and accountability, to intervene in real time to disrupt illicit infrastructure, block transactions, or degrade criminal networks.

Today's threat environment — particularly scam center networks that blend state sponsorship, criminal enterprise, and advanced technology — demands this kind of adaptation. These

networks move at machine speed, exploit jurisdictional seams, and leverage both crypto and traditional finance. Matching that threat requires a system where intelligence, authority, and action are aligned — and where public-private collaboration is not just information-sharing, but coordinated, real-time disruption.

Provide tools and training to state and local law enforcement

When a victim of pig butchering walks into a police station, the officer taking the report is often the only law enforcement contact that victim will ever have. That officer needs to know how to capture blockchain identifiers from the transaction confirmations and wallet addresses the victim can provide, how to preserve digital evidence in forms that support subsequent federal investigation, and how to connect the case to FBI, HSI, or Secret Service task forces with cryptocurrency investigative capability. Too many reports taken today result in no actionable investigation because the frontline officer does not have the training to recognize what they have received.

Mandatory blockchain intelligence training and access to tools for federal, state, and local law enforcement would meaningfully increase the proportion of cases that develop into actionable investigations rather than dead-end reports.

Create a victim compensation fund

Congress should create a DOJ-administered victim compensation or restoration fund to ensure that victims of cryptocurrency-enabled scams are made whole to the greatest extent possible. In today's threat environment, law enforcement can often trace and seize illicit proceeds, but the speed, scale, and fragmentation of these transactions make it difficult to tie specific recovered funds back to individual victims. A centralized fund would solve this problem by pooling recovered assets and distributing them equitably across victims, ensuring that relief reaches constituents even when precise attribution is not possible.

This approach is already contemplated in the Executive Order and should be codified into law. All funds recovered through seizures and forfeitures tied to scam activity should first be directed to victim compensation, with any remaining funds used to administer the program and support continued enforcement efforts. This creates a victim-first model that reflects the

realities of modern financial crime while establishing a durable framework for recovery in complex, cross-border cases where traditional restitution mechanisms fall short.

Conclusion

The threat before this committee is real, it is growing, and it is hitting American families with a precision and scale that demands a response equal to the challenge. In my career I have never seen anything like what blockchain intelligence reveals about the operational sophistication and financial resources of the criminal networks I have described today. But I want to leave this committee with something beyond the weight of the problem, because the weight of the problem, while real, is not the whole story.

We can follow the money. The blockchain is a public, permanent, immutable ledger, and the tools to read that ledger and identify the actors behind the transactions exist today. The private sector has built intelligence-sharing infrastructure, real-time alerting systems, and AI-powered investigative tools that are already producing results.

The Executive Order signed in March creates, for the first time, a whole-of-government mandate to bring the full toolkit of American power to bear on the organizations running these schemes. What the grandmother in Ohio, the veteran in Texas, and the family in New York need from this committee is the legal authority, resources, and sustained institutional commitment to deploy these capabilities at the speed and scale the threat demands. I am grateful for the attention this joint hearing brings to these issues and welcome your questions.