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

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

"Modernizing the BSA for Financial Crime in the 21st Century"

May 21, 2026

Introduction

Chairman Davidson, Vice Chair Nunn, Ranking Member Beatty, and distinguished members of the Subcommittee, my name is Ari Redbord. I appear before you today on behalf of TRM Labs, where we work every day with law enforcement, financial institutions, and national security agencies to detect, investigate, and prevent financial crime in the digital asset ecosystem and beyond.

Before joining TRM, I spent more than a decade as a federal prosecutor at the Department of Justice and later served as a senior official at the U.S. Treasury Department's Office of Terrorism and Financial Intelligence, working on sanctions, illicit finance, and counter-terrorism financing. I have chased illicit money across jurisdictions and built cases against sanctions evaders and terrorist financiers.

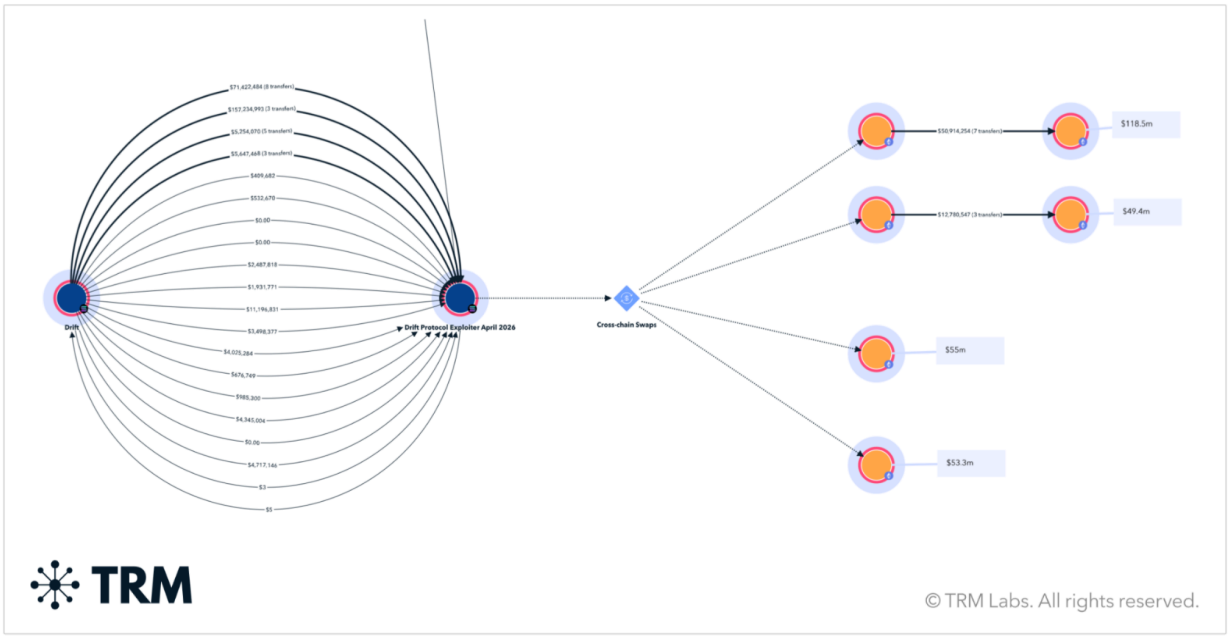
I come before this subcommittee with deep respect for the framework Congress built — and a clear sense of where it needs to go next. Because the framework that helped us win yesterday will not be enough to win today.

Illicit actors are deploying artificial intelligence, moving billions across blockchains in hours, and automating criminal activity at a scale no human investigative team was built to match. Our laws must match that moment or we will lose ground we cannot afford to give up.

We are living through a moment of profound technological transformation, and the single most important thing this subcommittee needs to understand is this: bad actors are early adopters of transformative technology. Criminal networks, rogue states, terrorist organizations, and fraud syndicates have always moved to exploit new technology before the legal frameworks designed to stop them can adapt. What is different today is the scale and speed of that advantage, and the specific power of the technology they are wielding.

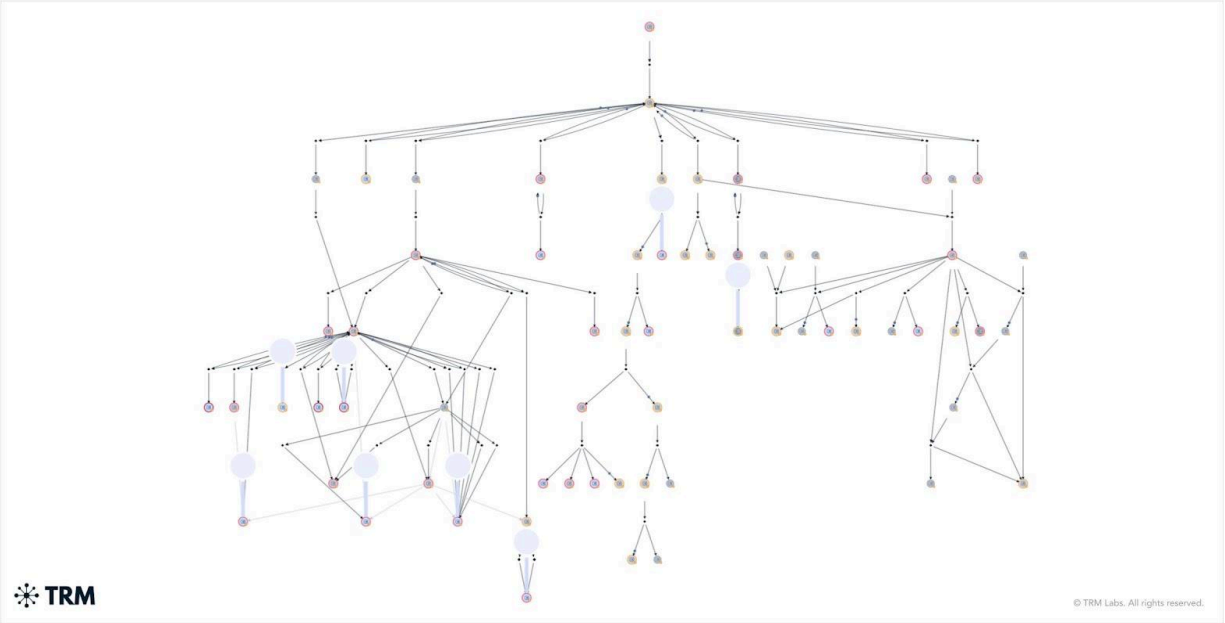
Artificial intelligence has fundamentally changed the economics of financial crime. It generates synthetic identities at industrial scale. It automates scam outreach to millions of victims simultaneously, personalizing each approach with deepfake video and voice cloning sophisticated enough to deceive careful people. It enables ransomware groups to take down critical infrastructure at scale and state-sponsored hackers to launder billions across blockchain networks faster than any human investigative team can follow.

North Korea stole more than USD 2 billion in digital assets in 2025 — and has already stolen more about USD 600 million in the first months of 2026 alone — funding a nuclear weapons program with the proceeds of AI-enabled cyber crime.



TRM Labs graph showing the April 2026 Drift protocol hack attributed to North Korea. The attack incorporated social engineering with sophisticated technical capabilities.

Pig butchering scam networks, operating from forced labor compounds across Southeast Asia and now expanding into Latin America and Africa, stripped more than USD 35 billion from American victims last year, driven by AI tools that make industrial-scale fraud operations accessible to criminal organizations that previously lacked the sophistication to run them. Iranian and Russian sanctions evaders are routing hundreds of millions through digital asset infrastructure designed specifically to defeat the controls the Bank Secrecy Act was built around — and using AI to do it faster and with greater operational security than ever before.



TRM's Graph Visualizer showing scammers moving funds, including those from an apparent deepfake giveaway scam, to a centralized exchange

Our laws must adapt to match this moment — and the path forward is clear. We must harness these same transformative technologies for good. AI-powered intelligence can process enormous data sets, trace illicit funds and build out networks at machine speed. Real-time intelligence-sharing can alert financial institutions and law enforcement simultaneously the moment criminal proceeds hit the financial system ensuring interdiction and disruption.

AI investigative tools can compress weeks of manual analysis into minutes, surfacing the network-level patterns that identify criminal infrastructure before it fully activates.

We have built these capabilities. The tools exist and they are working. What is required now are the legal frameworks that accelerate their deployment — authorities that empower financial institutions to act on real-time intelligence, funding that puts AI-powered tools in the hands of every federal agency, and a supervisory architecture that rewards the institutions driving toward genuine risk impact rather than compliance volume.

And critically — we can do all of this without asking Americans to surrender their privacy. The answer to financial crime in the age of AI is better technology and smarter frameworks, not bigger databases and broader surveillance. We must leverage the tools available to ensure that lawful Americans can transact securely and privately, while ensuring that bad actors cannot

exploit those same technologies to evade accountability. Privacy and security are not a trade-off. They are both achievable — and a modernized BSA must deliver both.

That is what I am here to describe today: the data behind the threat, the technology already producing results, and the specific legislative action this subcommittee can take to ensure that U.S. law enforcement, financial institutions, and the private sector are equipped to fight this fight and win it.

About TRM Labs

TRM Labs is a blockchain intelligence company whose platform is used by hundreds of financial institutions, cryptocurrency businesses, law enforcement agencies, and national security organizations worldwide. Our AI-powered tools allow investigators to trace the movement of funds across networks, identify illicit actors, and build the evidentiary record needed to support enforcement action, asset seizure, and prosecution.

We also produce original research on the intersection of digital assets and financial crime, including the annual TRM Crypto Crime Report, which documents illicit cryptocurrency flows, threat actor behavior, and emerging typologies across the global financial system. That research informs the testimony I am providing today.

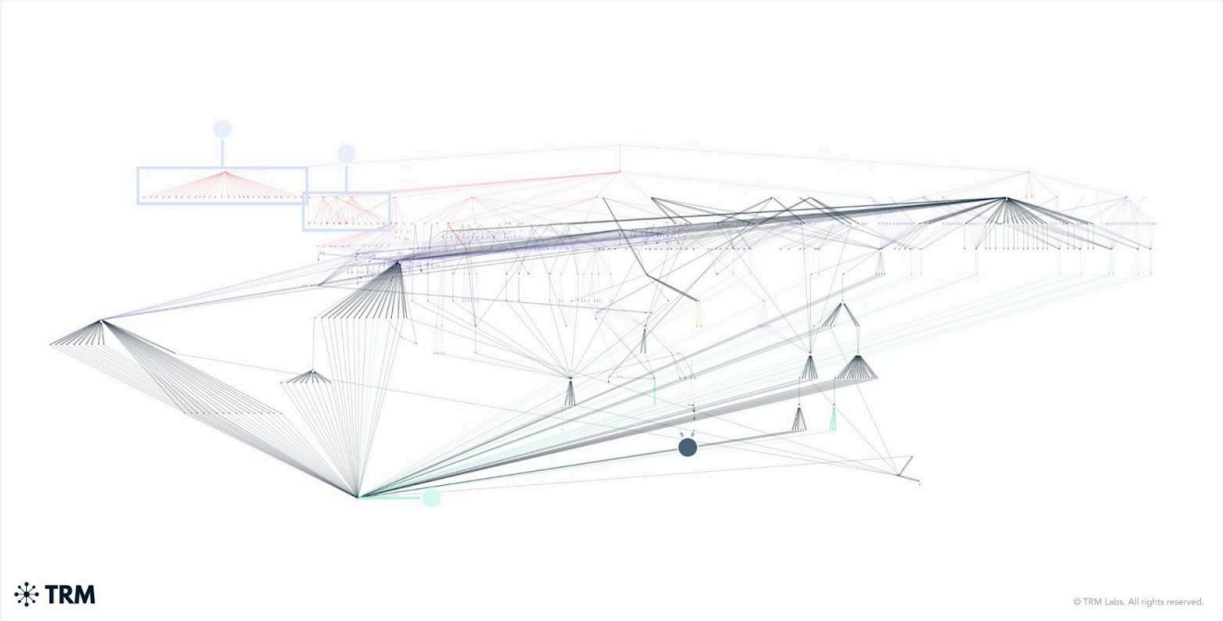
The Speed Problem

The foundational challenge of BSA modernization is speed. Speed of criminal activity, speed of fund movement, and speed of coordinated response.

The Bank Secrecy Act was built on a model in which financial intelligence flowed in one direction: from financial institutions to regulators, through Suspicious Activity Reports, Currency Transaction Reports, and related filings that aggregated over days or weeks into analytical products that fed law enforcement investigations. That model was adequate — even valuable — when financial crime operated on the tempo of wire transfers and correspondent banking, when illicit funds moved through layers of shell companies over weeks, and when investigators had time to assemble the picture before proceeds disappeared.

That model describes a world that no longer exists.

In the age of technology — AI, blockchain — a criminal network can receive fraud proceeds, move them through seven wallets across three blockchains, convert them into stablecoins, route them through a decentralized exchange, and position them for cash-out at an overseas over-the-counter broker — all within 48 hours of the initial transaction.



The rapid laundering process, within days of the record USD 1.5 billion ByBit hack in February 2025, included transfers through multiple intermediary wallets, conversion into different cryptocurrencies, and the use of DEXs, and cross-chain bridges to obfuscate the trail.

TRM data on pig butchering scam proceeds shows that average wallet holding periods have dropped significantly, with funds now moving across multiple wallets and chains within 24 to 48 hours of receipt. By the time a suspicious activity report is filed, reviewed, and converted into actionable intelligence, the money is beyond recovery.

The BSA framework was designed to generate intelligence. What we need today is a framework that generates interdiction and disruption.

The Risk-Focus Problem

The second foundational challenge of BSA modernization is what I will call the risk-focus problem. The current framework, as implemented in practice, incentivizes volume over precision.

Financial institutions collectively file approximately four million Suspicious Activity Reports annually. FinCEN estimates that law enforcement acts on roughly two percent of them. That ratio reflects a symptom of the framework itself

When a bank compliance officer knows that failing to file is a regulatory risk and filing a questionable SAR carries no cost, the rational institutional response is to file broadly and defensively. The result is a system buried in reports that lack the specificity, the context, and the actionability to drive investigations at scale. Law enforcement spends an enormous portion of its analytical bandwidth sorting through low-value filings in search of the few that represent genuine, high-confidence indicators of illicit activity.

The cost is measured not just in wasted resources but in missed threats. Compliance officers at institutions with sophisticated on-chain analytics and AI-powered transaction monitoring are finding patterns that would have been invisible to human reviewers — connections across thousands of transactions, behavioral signatures that identify shell accounts before they transact at scale, links between seemingly unrelated wallet clusters that belong to the same criminal network. That intelligence arrives at the regulatory framework converted into SAR narratives that describe individual suspicious transactions rather than the network-level threat picture that the data actually reveals.

The modernized BSA framework needs to be redesigned around a simple principle: the resources of financial institutions, regulators, and law enforcement should follow the highest-risk actors and activities. Everything else is noise.

That requires a structural shift from activity-based filing toward risk-based intelligence sharing. It requires regulatory acknowledgment that a financial institution with a sophisticated AI-powered compliance program should be evaluated on the quality of its risk management and the effectiveness of its intelligence contribution — not on the volume of its SAR filings. And it requires building the information-sharing infrastructure to make that intelligence actionable before the window for interdiction closes.

The Technology Gap: AI Has Changed Both Sides of This Fight

Artificial intelligence has changed the economics and speed of both financial crime and financial intelligence. Criminal networks, sanctions evaders, ransomware groups, fraud syndicates, and hostile state actors are increasingly using automation and AI to scale operations globally, move funds instantly across jurisdictions, generate synthetic identities, automate scams, and obscure illicit financial activity at a pace that traditional investigative systems were never designed to handle.

Generative AI-enabled scam activity rose 500 percent over the past year, according to data from Chainabuse, TRM's open-source scam reporting platform. Blockchain data confirms the speed acceleration: average wallet holding periods for illicit proceeds have dropped significantly, with funds now moving across multiple wallets and chains within 24 to 48 hours of receipt. AI has compressed the window for interdiction to the point where retrospective reporting frameworks are structurally incapable of generating a response in time.

At the same time, the anti-money laundering and counter-threat finance ecosystem remains heavily dependent on manual processes, fragmented data systems, and retrospective reporting workflows. Investigators and analysts are often required to search across disconnected databases, manually correlate records, and review overwhelming volumes of alerts and suspicious activity reports one at a time. By the time actionable patterns are identified, illicit actors have frequently already moved funds, laundered proceeds, or shifted infrastructure.

Harnessing AI for Good

At TRM Labs, we have built AI-native investigative capabilities specifically designed to address this challenge. These systems utilize enormous and highly diverse datasets — including blockchain intelligence, Suspicious Activity Reports, open-source intelligence, sanctions data, darknet intelligence, corporate registries, commercial data providers, telecommunications selectors, cyber threat intelligence, and internal investigative records — and fuse them into a unified investigative environment capable of operating at machine speed.

Investigators can interact conversationally with data and task AI agents in natural language. An analyst can begin with something as simple as a wallet address, company name, phone number, SAR narrative, email address, domain, or sanctions target. The system can then

automatically orchestrate searches across authorized data sources to recursively build a living network map of related entities, infrastructure, transactions, counterparties, and personas.

The key breakthrough is that these systems do not simply perform isolated searches. They conduct recursive, multi-hop investigations across enormous datasets simultaneously. Starting from a single lead, AI can identify linked wallets, associated exchange exposure, related shell companies, overlapping infrastructure, transaction counterparties, shared operational behavior, and broader criminal or financial ecosystems that would traditionally require teams of analysts working manually across multiple systems over days or weeks.

This allows agencies and financial institutions to move from reactive reporting toward proactive detection and disruption. Instead of simply collecting suspicious activity reports after illicit activity occurs, AI systems can continuously identify emerging typologies, detect anomalous financial behavior, surface hidden networks, and prioritize the highest-risk actors or financial nodes before harms fully materialize. This is a true data led, real time, risk based approach.

These capabilities are also designed to solve one of the central challenges facing modern financial intelligence operations: scale. Financial institutions and government agencies are overwhelmed by volume — thousands of alerts, wallets, transaction records, and investigative leads arriving simultaneously. AI can ingest these datasets in bulk, cluster related activity, identify common typologies, and prioritize the cases most likely to represent meaningful operational opportunities, such as sanctions evasion networks, fraud infrastructure, terrorist financing pathways, or recoverable illicit funds.

AI and Intelligence Fusion

Another transformational capability is cross-domain intelligence fusion. Historically, blockchain intelligence, cyber investigations, open-source intelligence, commercial records, and financial reporting systems have existed in separate silos. AI-native investigative systems fuse these domains together into a unified investigative environment. An investigator examining a suspicious financial network can move seamlessly from blockchain transactions to associated companies, online infrastructure, beneficial ownership records, exchange exposure, communications identifiers, and broader operational ecosystems without manually stitching together disconnected tools.

These systems also support continuous monitoring and real-time operational awareness. Rather than functioning solely as retrospective investigative platforms, they can monitor wallets, entities, typologies, or threat networks continuously and generate alerts when new risk indicators emerge. If illicit funds move through monitored infrastructure, if a sanctions-linked

network activates dormant wallets, or if a fraud cluster begins interacting with new exchanges or counterparties, investigators can be alerted immediately, creating opportunities for earlier intervention and disruption.

Importantly, these capabilities are designed with auditability, explainability, and human oversight at their core. Every investigative step, enrichment, inference, and analytic output can be traced back to underlying source material and investigator review. Human analysts remain in control of consequential decisions, ensuring that AI functions as a force multiplier for investigators rather than a replacement for human judgment, legal process, or regulatory oversight.

This is ultimately what BSA modernization requires. The challenge is no longer whether the United States possesses sufficient financial data. The challenge is whether we can responsibly and lawfully transform that data into actionable intelligence quickly enough to matter. AI-native investigative systems make it possible to move from a retrospective compliance architecture toward a modern financial intelligence capability capable of identifying, prioritizing, and disrupting illicit finance in near real time.

The Public-Private Coordination Gap and Beacon Network

The fourth foundational challenge is coordination. And I want to be precise about what I mean, because "public-private partnership" has become a phrase that obscures more than it reveals.

The traditional model of public-private partnership in the BSA context is information flowing from financial institutions to government through SAR filings, and government guidance flowing back to financial institutions through advisories, typologies reports, and examination feedback. That model is sequential, retrospective, and one-directional. It was designed for a world in which the threat picture was assembled after the fact and intelligence was used to build investigations over months.

What the current threat environment requires is something fundamentally different: real-time, bidirectional intelligence sharing that allows financial institutions and law enforcement to act on the same information simultaneously, at the machine speed.

TRM Labs has built exactly this infrastructure. Beacon Network is the first real-time, global intelligence-sharing system for illicit cryptocurrency activity. The network connects verified participants across the public and private sectors — including approximately 100 law enforcement agencies worldwide, many within the United States — with leading financial institutions and cryptocurrency platforms including Coinbase, Binance, Kraken, PayPal, Ripple, Stripe, Robinhood, Crypto.com, and Zodia Custody. The network covers approximately 85 percent of centralized cryptocurrency transaction volume.

This is all about speed — real time information sharing, fund interdiction, seizure, and disruption.

A verified investigator — law enforcement, a compliance officer at a participating institution, a government agency — flags an illicit wallet address in TRM's system. Flagged funds are tracked across the blockchain in real time. When those funds hit a participating exchange or financial institution, Beacon fires an immediate alert. The institution reviews the risk level and coordinates with law enforcement before processing any withdrawal.

This goes well beyond information sharing in the traditional BSA sense. This is coordinated interdiction — the private sector and law enforcement acting on the same intelligence at the same time, before illicit proceeds can be laundered beyond reach.

The BSA modernization conversation needs to make this model — not the traditional SAR paradigm — the aspiration for what public-private coordination can be.

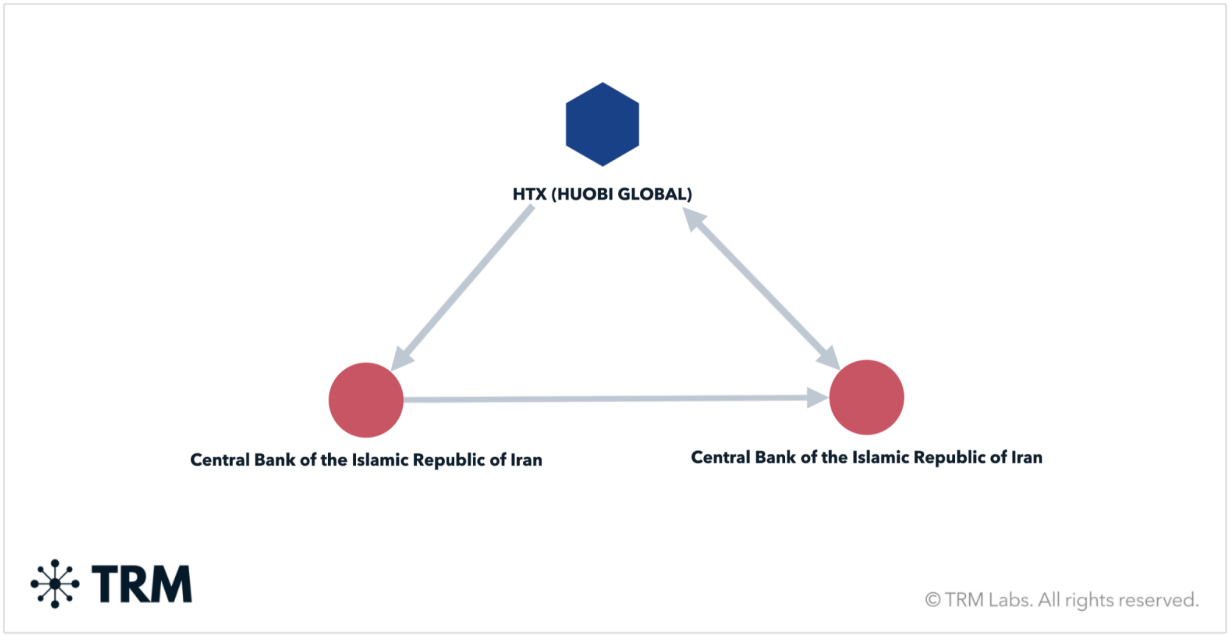
The Stablecoin Ecosystem: A New Model for Financial Crime Units

The emergence of stablecoins as a dominant medium for global value transfer has created both a significant vulnerability in the illicit finance landscape and an extraordinary opportunity for a new kind of financial crime enforcement — one that goes well beyond anything traditional finance can offer.

The opportunity is this: stablecoins are programmable financial instruments. A stablecoin issuer with the technical authority to freeze an address, burn the tokens associated with it, and reissue clean value to the legitimate holder can accomplish something fundamentally beyond what a bank can do. A bank hold preserves illicit proceeds in suspended animation — the funds sit

frozen, remaining a liability, the subject of legal process, and a source of ongoing operational burden. A stablecoin burn-and-reissue eliminates the illicit instrument entirely and recreates clean value. It is a more complete and operationally durable form of interdiction.

The T3 FCU is a model. Announced just last week, the T3 Financial Crime Unit — a collaboration between Tether, TRON, and TRM Labs — has frozen more than $450 million in illicit USDT since launching in September 2024, a 43.9 percent increase in intercepted illicit proceeds over the prior year. The unit has worked with law enforcement agencies across 23 jurisdictions — including the United States, Spain, Germany, the Netherlands, and Bulgaria — on investigations spanning money laundering, exchange hacks, DPRK-linked cyber operations, terrorist financing, drug trafficking, and violent crimes including kidnappings and extortion. In multiple account takeover incidents and violent crime emergencies, T3 FCU identified suspicious transactions and executed asset freezes within 24 hours of requests from global authorities.



Last month, Tether froze USD 344 million associated with the Central Bank of Iran

The Financial Action Task Force recognized T3 FCU earlier this year as an "invaluable resource for law enforcement agencies worldwide," citing it alongside TRM's Beacon Network as a leading model for public-private partnership against illicit activity in digital assets.

What makes T3 FCU structurally significant — beyond the numbers — is the architecture it represents. The unit functions as a dedicated financial intelligence unit embedded within the

stablecoin ecosystem itself, with the technical authority to monitor native token flows across the blockchain, the analytical capability to identify illicit activity in real time, and the operational relationships with law enforcement to act on that intelligence before proceeds can be moved beyond reach. It is a financial crime unit operating at the speed of the blockchain, with tools that government agencies and traditional financial institutions are still building toward.

The BSA framework requires updating to integrate this capability, recognize it within the supervisory architecture, and provide the legal clarity that would allow it to operate at full scale.

Stablecoin issuers with the technical authority to freeze and burn illicit proceeds deserve explicit statutory authority and safe harbor protection when acting in coordination with law enforcement. The gap in that framework is a policy failure — one that is costing law enforcement recoverable assets and victims the restitution they are owed every day that it persists.

The Data Infrastructure Challenge

One of the least-discussed but most consequential barriers to BSA modernization is data infrastructure. The effectiveness of AI-powered compliance tools, blockchain analytics, and real-time risk scoring depends entirely on the quality, consistency, and accessibility of the underlying data.

FinCEN receives approximately four million SAR filings annually. That database represents one of the most significant repositories of financial crime intelligence in the world. It is also, by and large, inaccessible to the private sector participants who generated the underlying information and who could use it to improve their own risk models, calibrate their AI systems, and identify the network-level patterns that individual institution data cannot reveal.

The BSA Information Sharing provisions under Section 314(b) allow financial institutions to share information with each other when there is a money laundering or terrorist financing concern. Section 314(b) sharing has grown meaningfully over the past decade, but it remains voluntary, episodic, and structured around individual cases rather than the kind of structured data exchange that AI systems require to generate network-level intelligence.

A modernized BSA framework should create the legal and technical infrastructure for structured, machine-readable data sharing among financial institutions, between financial institutions and regulators, and between regulators and the law enforcement agencies that

depend on financial intelligence to drive investigations. That infrastructure should be designed from the outset to support AI ingestion — standardized schemas, consistent entity identifiers, and data quality standards that allow the system to generate outputs rather than just store inputs.

FinCEN's existing analysis capabilities are genuinely valuable, and the financial intelligence FinCEN has provided to law enforcement over the years has supported some of the most significant financial crime prosecutions in American history. The challenge is scaling those capabilities to match the volume of the threat environment. AI-powered analysis of the full BSA database — calibrated around the highest-risk threat categories, updated in real time as new filings arrive, and surfaced to law enforcement in actionable form — would represent a step-change in the intelligence value of the system.

Congress should fund the technology modernization of FinCEN's analytical infrastructure as a national security investment.

The Examination and Supervision Gap

The mismatch between the BSA's compliance framework and the actual risk environment shows up most directly in how financial institutions are examined and how supervisory expectations are communicated.

Today, many institutions experience BSA examination as a process that evaluates the completeness and documentation of their compliance procedures — whether policies are current, whether training was completed, whether SAR filings meet formatting standards — rather than the effectiveness of the institution's risk management in actually identifying and disrupting financial crime.

An institution that files 50,000 SARs a year, few of which are acted on by law enforcement, can pass a BSA examination with distinction. An institution that files 5,000 SARs, all of which are high-confidence, actionable intelligence products that drive investigations, can face examiner criticism for gaps in its monitoring coverage.

That incentive structure produces exactly the wrong compliance behavior. Institutions optimize for examination performance rather than threat impact. Resources flow to documentation, training certification, and SAR volume rather than to the analytical capabilities that would actually improve the institution's ability to identify the criminal networks using its services.

The modernized framework needs to reorient examination and supervision around a single question: is this institution's risk management program effectively identifying and disrupting the financial crime threats it is exposed to? That question requires examiners to have meaningful engagement with the institution's on-chain analytics outputs, its AI-powered risk scoring systems, its network-level entity due diligence capabilities, and its participation in intelligence-sharing frameworks like Beacon. It requires supervisors who understand blockchain, who can read a transaction graph, and who can evaluate whether an institution's AI-powered transaction monitoring is calibrated to the right risk signals.

Treasury should invest in the training and technical infrastructure needed to build a generation of examiners who can evaluate AI-powered compliance programs on their merits. The alternative is a supervisory process that systematically penalizes technological sophistication and rewards volume-based compliance theater.

The SAR Modernization Imperative

The Suspicious Activity Report is the central mechanism through which financial institutions communicate financial intelligence to the government. It is also one of the clearest examples of a tool designed for a different era being stretched beyond its design parameters.

The current SAR form and filing process was designed to capture the facts of a suspicious transaction — who, what, when, how much — and transmit that information to FinCEN for analysis. In the blockchain environment, a single suspicious transaction may be one node in a network of thousands of connected addresses, wallets, and entities. The SAR narrative that describes one wallet sending funds to another wallet tells law enforcement almost nothing about the criminal network those wallets belong to, the victims whose funds they contain, or the entities that will ultimately receive and liquidate the proceeds.

AI-powered tools can generate a fundamentally different kind of intelligence product — one that maps the network around a suspicious transaction, identifies the connected entities, scores their risk based on behavioral signals, traces the flow of funds through multiple hops and across multiple chains, and surfaces the pattern-level signatures that identify this activity as part of a known criminal typology. That intelligence product is far more valuable to a law enforcement investigator than a traditional SAR narrative.

TRM has built tools that can combine on and off-chain data to generate a network-level risk assessment, identifies the highest-priority investigative leads, and drafts an intelligence

narrative that frames the individual transaction within the broader threat picture. The output goes well beyond a SAR — it is a case-ready intelligence product that an investigator can act on.

Congress and FinCEN should work together to create a modernized SAR framework that accommodates AI-generated intelligence products, establishes standards for network-level reporting that captures the full picture of a suspicious activity cluster rather than a single transaction, and creates a feedback loop through which law enforcement can signal which SAR typologies and formats are generating the most actionable intelligence. That feedback loop remains absent in any systematic form, which means financial institutions are filing into a void with no way to learn whether their intelligence products are contributing to enforcement outcomes.

The Privacy Imperative: Less Data, Better Intelligence

BSA modernization presents this subcommittee with a choice that will define the framework for a generation: a compliance architecture that demands more customer data, more collection, more centralized repositories of sensitive financial information — or one that leverages technology to achieve better outcomes with less.

The answer, grounded in both principle and practicality, is less.

Privacy is a feature of well-designed financial systems, not a bug. As more transactions migrate to open public blockchains, the privacy expectations of lawful users — individuals, businesses, institutions — deserve the same respect that the traditional financial system has always extended them. When someone pays with a credit card or bank transfer, the transaction serves its purpose and the counterparty learns what is necessary. The customer's full balance, transaction history, employer, and spending patterns remain private. Public blockchains, by contrast, expose every transaction to every observer — a regression from traditional financial privacy that creates real, documented harms.

Cryptocurrency holders have been targeted for physical attacks, extortion, and theft by criminals who identified them through on-chain wealth visibility. Businesses conducting treasury operations on transparent chains expose competitive intelligence to any analyst with a screen. Privacy is consumer protection, and a modernized BSA framework should recognize it as such.

The insight that should guide this subcommittee is that privacy and compliance are complementary goals, not competing ones. A system can provide strong privacy from public observers while maintaining full lawful investigative access through selective disclosure. Law enforcement does not need real-time public visibility into every transaction to investigate crimes effectively. It needs the ability to obtain specific visibility through legal process when investigating specific actors — and the tools to act on that intelligence at the speed the threat demands. Selective disclosure mechanisms, well-governed and properly scoped, can provide exactly that.

What a modernized BSA framework should resist is the instinct to respond to financial crime threats by requiring more customer data collection. Every database of sensitive financial information is a honeypot. The ransomware groups and state-sponsored hackers before this subcommittee are actively targeting exactly these repositories — the concentrated stores of customer identity data, transaction records, and financial profiles that BSA compliance has historically required institutions to maintain. Each new collection mandate creates a new target. Each new centralized repository expands the attack surface.

The answer to financial crime in the age of AI and blockchain is superior analytics applied to better-structured data — requiring institutions to collect the minimum data necessary, retain it for the minimum period required, and deploy AI-powered tools that derive intelligence from behavioral patterns and network analysis rather than from bulk personal data accumulation.

TRM's white paper on on-chain privacy and financial compliance, published earlier this year, establishes a framework for evaluating privacy regimes — from per-transaction disclosure to asset-level visibility to allow-list models — against the needs of investigators, regulators, and lawful users simultaneously. The central finding is consistent with the principle this subcommittee should enshrine: hybrid models combining selective disclosure with strong governance and appropriate compensating controls can satisfy both user privacy and AML/CFT objectives. The technology to do this well exists today. What is required is a regulatory framework that creates the right incentives — one that rewards institutions for deploying sophisticated, privacy-preserving compliance architectures rather than for accumulating the largest possible stores of customer data in the name of due diligence.

BSA modernization is the opportunity to get this right. Congress should direct Treasury and FinCEN to develop standards that explicitly incorporate data minimization as a compliance principle — establishing that institutions which achieve superior risk outcomes through advanced analytics and targeted data collection are more compliant, not less, than institutions that rely on broad collection and bulk retention. The goal is financial intelligence that disrupts crime. The path to that goal runs through technology, not through surveillance.

Recommendations

The analysis above leads to the following recommendations that I urge this subcommittee to advance. Each is operationally specific, grounded in the threat environment I have described, and will make the American people safer.

Fund AI-Powered Investigative and Analytical Capabilities Across Federal Agencies at Scale

Bad actors are deploying AI autonomously and at scale. Federal agencies deserve the funding, the procurement authority, and the legal frameworks to match that capability. That means investing in AI-native investigative systems that fuse blockchain intelligence, sanctions data, open-source intelligence, cyber threat data, and financial records into a unified environment where investigators can recursively build network maps of criminal infrastructure at machine speed — compressing work that once took teams of analysts weeks into minutes, and generating case-ready intelligence products that enable action before the window for interdiction closes. That investment should reach IRS Criminal Investigation, FinCEN, OFAC, the FBI, DEA, Secret Service, HSI, and the national security and defense agencies whose missions increasingly intersect with financial crime. The agencies responsible for protecting Americans deserve investigative infrastructure that matches the moment. That is a national security priority.

Codify Real-Time Intelligence Sharing as a Core Pillar of U.S. AML Policy

Beacon Network demonstrates what is possible when financial institutions, cryptocurrency platforms, and law enforcement operate on the same intelligence simultaneously. The network connects approximately 70 law enforcement agencies worldwide with leading platforms — including Coinbase, Binance, Kraken, PayPal, Ripple, Stripe, Robinhood, Crypto.com, and Zodia Custody — covering approximately 85 percent of centralized cryptocurrency transaction volume. When illicit funds hit a participating exchange, an alert fires in real time, creating the opportunity for coordinated action before criminal proceeds move beyond reach.

Congress should codify Beacon-style real-time intelligence sharing as a standard expectation across the digital asset compliance ecosystem, with dedicated federal funding to expand

participation to smaller platforms — which are systematically targeted as compliance weak points — and liability protection for firms acting on law enforcement intelligence in good faith. Real-time coordinated interdiction is the model the United States is building toward, and the legal architecture should reflect that.

Enact a Digital Asset Hold Law

Congress should enact a statutory safe harbor allowing cryptocurrency exchanges and financial institutions to temporarily freeze funds linked to high-confidence illicit indicators, pending law enforcement review. Traditional banks have held this authority for decades, and the digital asset ecosystem deserves the same foundation. When a Beacon alert fires and an institution has high confidence that funds about to be withdrawn are illicit, every hour of legal uncertainty is an hour that criminal networks use to move proceeds to the next wallet. The language for such a provision already exists in draft form within the Senate Banking Committee's Digital Asset Market Clarity Act discussion draft. Congress should move it forward, and move it quickly.

Formally Recognize Stablecoin Financial Intelligence Units and Provide Legal Clarity for Burn-and-Reissue Authority.

The T3 Financial Crime Unit has demonstrated what a stablecoin FIU can accomplish when given the right infrastructure and legal foundation. By combining Tether's technical authority to freeze and burn USDT, TRON's blockchain infrastructure, and TRM's real-time blockchain intelligence, T3 FCU has built something genuinely new: a dedicated financial intelligence unit embedded within the stablecoin ecosystem itself, capable of monitoring its native token across the entire blockchain, freezing illicit addresses within 24 hours of a law enforcement request, and permanently removing illicit proceeds from circulation through burn-and-reissue. Since launching in September 2024, T3 FCU has frozen more than $450 million in illicit assets across 23 jurisdictions, intercepting 43.9 percent more illicit proceeds in 2025 than the prior year. FATF recognized T3 FCU this year as an invaluable resource for law enforcement worldwide. A traditional bank hold preserves frozen funds in legal limbo. A stablecoin burn-and-reissue eliminates the illicit instrument entirely and recreates clean value — a more complete and operationally durable form of interdiction.

Congress should formally recognize stablecoin financial intelligence units as a distinct category within the U.S. counter-illicit finance framework — establishing legal standards for freeze, burn,

and reissue actions; creating safe harbors for stablecoin issuers acting under law enforcement direction; directing Treasury to develop operational protocols that govern this capability at scale; and establishing financial crime monitoring as a supervisory expectation for stablecoin issuers above a defined threshold of circulating supply. This is the technological infrastructure of the next generation of financial crime enforcement, and the regulatory framework should reflect that reality.

Restructure BSA Examination and SAR Requirements Around Effectiveness Rather Than Volume

The current BSA framework, as implemented, rewards compliance behavior that produces volume — SAR filings, training completions, policy documentation — rather than risk management that produces results. Institutions filing large volumes of low-quality, unfocused SARs pass examinations with distinction. Institutions deploying sophisticated AI-powered analytics and filing smaller volumes of high-confidence, network-level intelligence products face the same examination process and often the same scrutiny. That incentive structure drives exactly the wrong compliance behavior across the entire industry.

Congress and the regulators should work together on two interconnected reforms. The first is a modernized SAR framework that accommodates AI-generated, network-level intelligence products — moving from single-transaction reporting to cluster-level intelligence that captures the full pattern of a suspicious activity network, with structured data schemas supporting machine ingestion at FinCEN and a systematic law enforcement feedback loop through which agencies can signal which intelligence formats are generating actionable outcomes. The second is a reorientation of BSA examination toward effectiveness-based evaluation — training examiners to assess AI-powered compliance programs on their risk management outcomes, evaluating institutions on the quality and actionability of their intelligence contribution, and recognizing participation in real-time intelligence-sharing networks as a positive supervisory indicator.

Enshrine Privacy and Data Minimization as Core Principles of BSA Modernization

Privacy and security are not a trade-off. They are both achievable — and a modernized BSA must deliver both. The instinct to respond to financial crime threats by requiring more customer

data, broader collection, and longer retention creates the very vulnerabilities we are trying to close. Every centralized database of sensitive financial information is a target. The ransomware groups and state-sponsored hackers before this subcommittee are actively hunting these repositories — and every new collection mandate expands the attack surface they can exploit.

Congress should direct Treasury and FinCEN to enshrine data minimization as an explicit compliance principle — establishing that institutions achieving superior risk outcomes through advanced analytics and targeted data collection meet and exceed their BSA obligations, and that bulk data accumulation in the name of due diligence is a vulnerability, not a virtue. The goal is financial intelligence that disrupts crime and protects Americans. Technology gives us the ability to achieve both a safer financial system and a more private one. A modernized BSA should require less data from Americans, deploy smarter tools to analyze what is collected, and ensure that lawful users can transact securely and privately — while giving law enforcement every capability it needs to identify and stop the bad actors who would exploit those same protections.

The Moment We Are In

I want to close with a word about urgency, because I think the framing of this hearing as a modernization exercise understates what is actually required.

Modernization implies updating an existing framework — adjusting parameters, adding provisions, reforming procedures. What the data shows is that the threat environment has undergone a categorical change, not an incremental one. Criminal networks are operating with the organizational sophistication of multinational corporations, the financial infrastructure of professional money laundering systems that process hundreds of billions of dollars annually, and the technological capabilities of AI-powered enterprises that can automate outreach, synthetic identity creation, fraud execution, and money laundering simultaneously and at industrial scale.

The response to a categorical change is a structural response. The BSA framework needs to be rebuilt around the threat environment of 2026, not optimized for the threat environment of 1996. That means accepting that the primary value of the system is not compliance documentation but financial intelligence that drives enforcement. It means accepting that the primary metric of institutional performance is not SAR volume but investigative utility. It means accepting that the primary model of public-private partnership is not retrospective reporting

but real-time coordinated interdiction. And it means accepting that artificial intelligence is the infrastructure layer through which all of this runs — for the criminals who are already using it, and for the institutions and agencies that must match their capabilities.

TRM Labs has built the tools. The private sector has demonstrated the model. Beacon Network and the T3 Financial Crime Unit have shown that real-time coordinated interdiction produces results at a scale that the traditional SAR paradigm cannot approach. What is needed now is the legislative and regulatory framework that enables these models to operate at the speed and scale the threat demands.

I am grateful to this subcommittee for the attention and seriousness this hearing reflects. The families who have lost their savings to fraud networks, the veterans whose home equity was stripped by synthetic romance scammers, the small businesses whose accounts were drained before their banks' rule-based monitoring systems fired a single alert — they need this framework to work. And it can. The tools exist. The data is there. The question is whether the law will keep pace with the threat.

I welcome your questions.

Ari Redbord is the Global Head of Policy and Government Affairs at TRM Labs. He previously served as a Senior Advisor at the U.S. Treasury Department's Office of Terrorism and Financial Intelligence and as a federal prosecutor at the United States Department of Justice. TRM Labs works with hundreds of financial institutions, law enforcement agencies, and national security organizations worldwide to detect, investigate, and prevent financial crime in the digital asset ecosystem.