TESTIMONY OF
Carole House[1]
BEFORE THE
UNITED STATES HOUSE FINANCIAL SERVICES COMMITTEE
SUBCOMMITTEE ON NATIONAL SECURITY, ILLICIT FINANCE, AND INTERNATIONAL FINANCIAL INSTITUTIONS

Hearing on Modernizing the Bank Secrecy Act (BSA) for 21st Century Illicit Finance
May 21, 2026

Thank you Chairman, Ranking Member, and distinguished Members of the Subcommittee, for holding this hearing and the honor of the invitation to testify on modernizing critical illicit finance frameworks in the face of an ever-dynamic threat, technology, and policy landscape. I applaud your leadership in convening the Subcommittee on this important issue. I have spent my career at the intersection of national security, emerging technology, and economic statecraft, including through service in three tours at the White House, at the U.S. Treasury Department, U.S. Senate Homeland Security Committee, chairing and advising three regulatory agency committees on emerging tech, and as a U.S. Army Captain. I hope my testimony will be helpful in considering some of the most important aspects of anti-money laundering and countering financing of terrorism (AML/CFT) reform, as you navigate the incredibly complex issues at play here relating to security, innovation, and personal liberty.

The financial integrity architecture the United States built over the past five decades is not, at its core, a compliance structure. It is the infrastructure through which this country defends its citizens, projects economic power, and holds adversaries accountable. It is what enables us to freeze the assets of a sanctions evader, trace the proceeds of a fentanyl network back to its source, recover funds stolen from fraud victims, and deny revenue to the state actors funding weapons of mass destruction (WMD) proliferation programs with stolen funds. Every major threat identified in Treasury's National Money Laundering Risk Assessment, in the ODNI's annual threat assessment, and in the bipartisan work of the House Select Committee on China runs, at some point, through the financial system.[2] The architecture we built to track and disrupt the activity of these threats – whether Chinese infiltration of AI supply chains, narco- and human-trafficking networks, arms control circumvention – runs in mutual support of rule-of-law systems with benefits that extend well beyond national security. Sanctions enforcement, civil fraud recovery, credit decisions, tax administration, and counter-fraud programs all depend on a common underlying principle: that certain financial activity is documented and available to those with lawful authority to access it, under conditions appropriate to the purpose. Remove that principle and you do not just weaken AML enforcement. You weaken every accountability system built on top of it.

These frameworks also implicate genuine democratic values that demand honest engagement: privacy, personal liberty, and the burden that compliance obligations place on individuals and institutions. Getting

---

[1] The views expressed here are my own. *Background:* Nonresident Senior Fellow, Atlantic Council GeoEconomics Center; CEO, Penumbra Strategies LLC; Senior Research Scholar, Georgetown University; Distinguished Senior Fellow, ACAMS. Former Advisory Roles: Chair, Commodity Futures Trading Commission Technology Advisory Committee; Virtual Currency Advisory Board member, New York Department of Financial Services (NYDFS); Emerging Technology Advisory Committee (ETAC) Member, Idaho Department of Finance; Advisory Board Member, Third Way U.S.-China Digital World Order Initiative; Advisory Board Member, Digital Dollar Project; Senior Advisor, FS Vector. Other Previous Roles: Special Advisor for Cybersecurity and Secure Digital Innovation, White House National Security Council (NSC); Director of Cybersecurity and Secure Digital Innovation, White House NSC; Senior Strategic Policy Officer for Cyber and Emerging Technology, U.S. Financial Crimes Enforcement Network (FinCEN); Presidential Management Fellow (PMF) and Policy Advisor, White House Office of Management and Budget and U.S. Senate Homeland Security and Governmental Affairs Committee; Captain, U.S. Army.

[2] U.S. Treasury, National Money Laundering Risk Assessment 2026; Office of the Director of National Intelligence (ODNI), Annual Threat Assessment of the US Intelligence Community, 2026; U.S. Select Committee on China, Buy What It Can, Steal What It Must: China's Campaign to Acquire Frontier AI Capabilities, April 2026.

modernization right means taking those values seriously, not treating them as obstacles to security but recognizing that well-calibrated financial integrity frameworks advance all of them simultaneously. Privacy protection in this context means ensuring sensitive financial information reaches only those with lawful authority to access it and defining what those conditions should be, not that records cease to exist. Liberty protection means ensuring the system targets wrongdoing rather than imposing indiscriminate burdens on law-abiding Americans. And burden reduction done right (e.g., through better infrastructure, smarter data architecture, and clearer regulatory standards) can improve both outcomes and access at the same time. The tensions here are real but narrower than the current debate suggests, and the connective tissue between security, accountability, and financial inclusion is stronger than is often recognized.

A few key messages I hope to underscore with my testimony:

- **The risk environment (across every component of risk – threat, vulnerability, *and* mitigations) has genuinely changed, and demands frameworks accounting for these evolutions.** Transnational criminal organizations, state actors, and professional enablers are more sophisticated, better resourced, and more technologically capable than at any prior point. Generative artificial intelligence (AI), digital assets, and agentic financial systems are present operational realities being exploited now, and quantum moment (whether in super-charging compute capability or threatening cryptographic security) is fast approaching. If we invest in the right infrastructure and policy levers, they also create genuine opportunities for more effective detection and disruption. Ongoing policymaker interest in focusing on leveraging emerging technologies for benefit and desire to drive greater prioritization for more targeted use of limited resources in high-impact ways can be important steps in addressing this dynamic risk environment.

- **Our adversaries are actively exploiting the seams in our visibility into corporate ownership, commercial relationships, and financial system coverage at growing scale and sophistication.** Congress recognized this trajectory and acted by building authorities and tools specifically designed to gain visibility at the critical junctures adversaries exploit. Those tools remain unfinished five years on, and in some areas are being actively reversed. The result is a growing gap between the sophistication of the threats Americans face and the capability of the frameworks designed to address them; a gap that is widening precisely as the window to close it narrows.

- **Genuine modernization requires an honest evaluation of the existing system's strengths and challenges and the nature of shifts driven in capacity and threat by an evolving technology landscape – though conflating burden reduction with modernization, without meaningful steps toward efficacy, does not benefit Americans or national security.** Reducing compliance friction by building better infrastructure (i.e., authoritative identity verification, machine-readable and structured intelligence sharing, risk-based examination methodology, etc.) improves outcomes while reducing burden. This is a noble aspiration and precisely how we should be thinking about illicit finance framework modernization. However, reducing visibility and dismantling the accountability apparatus without improving underlying infrastructure and without understanding and improving efficacy isn't modernization; it's effect will be a reduction in capability and opening the door to adversaries seeking to harm Americans and U.S. national security interests.

To meet the dynamic and sophisticated threats facing our financial system, the United States must pivot from a model of retrospective compliance to one of proactive, operational disruption. Achieving this requires a synchronized effort to eliminate structural blind spots, dismantle artificial data silos, and deploy modern digital identity infrastructure. The following targeted recommendations provide Congress and regulatory agencies with a strategic roadmap to deliver on the promise of the AML Act (AMLA), restore accountability, and safeguard American national security:

- **Restore accountability where adversaries exploit opacity:** *Corporate and supply chain transparency* – restore and implement the Corporate Transparency Act (CTA) and beneficial ownership transparency as envisioned by Congress and with a framework that benefits financial institutions and the national security ecosystem; *Enabler coverage* – finalize investment adviser obligations; finalize the real estate AML rule and extend targeted AML obligations to professional enablers.

- **Modernize financial intelligence sharing:** *SAR and cross-institution sharing* – finalize the SAR sharing pilot established under the AMLA; expand 314(b) protections in the statute to explicitly cover information related to underlying predicate offenses for money laundering to include fraud, cybercrime, and sanctions violations; broaden information-sharing liability coverage beyond financial institutions to include financial service providers and other entities for purposes of combating financial crime and fraud (i.e., resembling Cybersecurity Information Sharing Act coverage); *Data standards and architecture* – develop structured machine-readable financial crime data standards (e.g., adopt lessons from cybersecurity with the STIX/TAXII standards for real-time sharing of machine-readable cyber and digital footprint indicators) and feedback loops to integrate into domestic and international reporting and information sharing channels[3]

- **Build digital-era identity and compliance infrastructure:** *Identity pilots and infrastructure* – direct FinCEN to establish clear pathways for exceptive relief pilots and measurements of efficacy with roadmaps to approval; launch pilots and public-private partnership initiatives for digital identity services and reliance, privacy-enhancing technology (PET)-enabled information sharing and AI-training, typology- and threat-specific SAR attachment data structures, and for programmable compliance features using existing FinCEN authorities like exceptive relief; modernize customer verification and beneficial ownership infrastructure, ensuring value for national security/law enforcement community and industry stakeholders. *Governance frameworks for emerging technology* – establish governance frameworks for AI-enabled and agentic financial systems; publish AI governance and examiner guidance for AML compliance related to use of and combating threats presented by emerging technologies (e.g., digital identity, digital assets and blockchain, AI, quantum). *Evaluate paradigm shifts and regulatory perimeter adjustments* – evaluate gaps in understanding and traceability of financial flows to assess regulatory guidance or rulemaking measures needed to move the regulatory perimeter elsewhere in the ecosystem or payment technology infrastructure to address key gaps or changes in the role or visibility of intermediaries (e.g., payment processors, defi, etc.)

- **Shift from retrospective compliance to operational disruption:** *Supervision and enforcement* – define measurable outcomes-oriented supervision standards tied to specific operational results rather than procedural proxies; direct strategic enforcement alignment that improves FinCEN's access to critical information as well as enforcement action timeliness and calibration based on risk tiers, extent of violations, and sector-shaping (not sector-breaking) objectives; prioritize and scale FinCEN's Rapid Response Program for automation, expansion to fintech and crypto, and real-time coordination to boost interdiction of fraud proceeds; resource FinCEN appropriately with budgeting and hiring authorities commensurate with its mission scope. *Authorities and coordination* – modernize special measures authorities for digital-era threats (i.e., 311 and 9714 special measure expansion) a to reach primary money laundering concerns operating through fintech and digital asset infrastructure outside traditional correspondent banking frameworks; restore interagency coordination capacity for sanctions and kleptocracy enforcement.

[3] Natalie Loebner, Following the Money: Tools and Techniques to Combat Fraud, July 2025; Cybersecurity and Infrastructure Security Agency, How to Share Cyber Threat Information through AIS; ACAMS International Anti-Fraud and Technology Task Force, Cross Sector Fraud Information Sharing: Pathways to Action, March 2026;

THE THREAT LANDSCAPE: SOPHISTICATED, CONVERGING, AND ACTIVELY EXPLOITING THE GAPS WE LEAVE OPEN

The financial integrity architecture exists to address a set of threats that are not static. Assessing the current threat environment is essential for evaluating any proposed change to the framework designed to address it. Transnational criminal organizations, state-linked proxies and crime groups like cyber and fraud syndicates, and professional enabler networks have systematically mapped the gaps in American financial oversight (e.g., anonymous and obfuscated corporate structures, unregulated investment channels, fragmented digital asset compliance, delayed enforcement, etc.) and built their operations around them. The system fails in a few key ways: *we cannot understand who is involved, we cannot connect what institutions know, and/or we cannot act in time to matter*. Below I've outlined some of the ways major threat actors exploit at least one (if not all three) of those dimensions, illustrating why some of the specific tools I discuss in my testimony exist.

Example AML/CFT Exploits by Priority Threat Actors

Threat Actor/Network	Example Financial Vulnerabilities Exploited and Policy Gaps
Chinese Money Laundering Organizations (CMLOs)/Fentanyl Proceeds	Underground mirror-banking networks; cash-intensive retail front businesses; trade-based money laundering (TBML); digital remittances; real estate *Gaps: unregulated real estate cash purchases; informal value transfer not captured or non-compliant under BSA, insufficient trade-based money laundering (TBML) enforcement and lack of automated customs-to-financial data cross-referencing; gaps in digital remittance and informal value transfer system compliance]*
Russian Oligarchs and Sanctions Evaders	Anonymous U.S. shell companies; investment adviser relationships; luxury real estate; art and antiquities; third-country correspondent networks *Gaps: CTA beneficial ownership information (BOI) exempted for domestic entities; no investment advisor rule delay; real estate rule not finalized; arts and antiquities unregulated*
Democratic People's Republic of Korea (DPRK) State Cyber-Financial Apparatus	Cryptocurrency theft and mixing/bridges/chain-hopping; decentralized finance ("DeFi") protocol exploitation; un/self-hosted wallets; offshore exchanges with weak compliance *Gaps: non- and weak-compliance in many jurisdictions; DeFi jurisdictional exploits; absence of governance frameworks for agentic or autonomous financial systems; offshore exchange jurisdictional arbitrage*
Iranian Sanctions Evasion Networks	US dollar (USD)-denominated stablecoins; cryptocurrency mining; oil proceeds laundering; front companies in third countries *Gaps: sovereignty and compliance gaps for non-U.S. based centralized stablecoin issuers; systemic tracing blind spots in secondary/tertiary nested correspondent banking relationships in regional hubs*
Transnational Criminal Organizations (Cartels/ Jalisco New Generation Cartel [CJNG]/Sinaloa)	Bulk cash; trade-based money laundering; money service businesses; real estate; cryptocurrency for procurement *Gaps: missing outsourced CMLO mirror-swaps; non-financed real estate rule vacated nationwide; fintech platform compliance and coverage inconsistencies lacking real-time, distributed, rapid, cross-institution mule laundering velocity detection*
Industrialized Fraud Networks (Pig Butchering/ Scam Compounds)	Cryptocurrency; payment apps; digital remittances; money mules; shell company layering for proceeds laundering *Gaps: global fragmentation of crypto compliance; digital identity verification gaps enabling automated synthetic account opening; lack of explicit safe harbors for fraud data sharing under the*

	314(b) statute; absence of standardized inter-institution data sharing tracks]
Chinese Military-Linked Technology Procurement Networks	U.S.-registered shell companies; front companies in third countries; investment vehicles; export control circumvention through layered corporate structures *Gaps: CTA BOI exempted for domestic entities; venture capital and private equity investment advisers lacking comprehensive programmatic coverage until 2028; operational silos between FinCEN financial intelligence and BIS export control triggers*[4]

THE PARADIGM SHIFTS: WHAT IS ACTUALLY NEW, WHAT THE RISK IS, AND WHERE OPPORTUNITY LIES

Not every emerging technology creates a fundamentally new policy problem. Some accelerate existing risks, some shift the threat landscape while opening new defensive opportunities, and some change far less than their advocates or critics claim. The best regulatory approaches to emerging technology (like the best AML programs) are risk-based: demanding that institutions own and understand the specific risk profile of not only their business and their customers, but their use of – and how they are targeted with – emerging technologies, not simply apply uniform obligations across the board. Risk-based approaches should not mean inherently permissive, but should mean *precise* and honed for the unique circumstances of that institution, customer, or technology. Several developments are materially changing both the tech-enabled threat environment and the tools available for defense. The policy response must account for both dimensions rather than treating new technology as either uniformly threatening or uniformly beneficial.

Emerging Technology Structural Shifts and Risks/Opportunities – Key Examples

Technology	Example Structural Shift (Legacy Reality v. New Paradigm)	Risk (if Governance Fails) and Opportunity (if Framework Built Well)
AI and Agentic Commerce	*Legacy:* Human-driven fraud bound by manual onboarding speed limits; human and legal persons making conscious, real-time transaction authorizations *New:* Automated, industrialized identity synthesis operating at near-zero marginal cost; software agents executing machine-speed transaction structuring without human or legal person review but potentially with delegated authority	*Risk:* Deepfake "know your customer" (KYC) bypass and automated social engineering overwhelm rules-based controls ; core BSA compliance assumptions challenged when code is a transacting party, leaving unsettled answers about responsibilities and liabilities throughout the tech stack and delegating/directing parties for consumers, regulators, and law enforcement *Opportunity:* Machine learning (ML) graph analytics reveals complex, multi-institution networks invisible to legacy rules; automated compliance protocols can flag and dynamically restrict anomalous agent behaviors
Digital Assets, Stablecoins, and DeFi	*Legacy:* Centralized financial institutions acting as focus for accountability and friction-reducing services for consumers; traditionally bifurcated financial and information transfer rails; cross-border sovereign transfers tethered to domestic clearinghouses *New:* Programmable financial assets that co-locate financial and non-financial rails; composable, decentralized code protocols	*Risk:* Lack or obscurity of intermediaries and enforce-able points of accountability creates structural governance gaps exploited by cybercriminals and state actors; billions in parallel/shadow dollar networks used for sanctions evasion, fentanyl procurement, and laundering of generational wealth stolen from Americans *Opportunity:* Public ledgers enable real-time, programmatic transaction tracing and automated

[4] *Sources for table analysis:* Drug Enforcement Agency (DEA), National Drug Threat Assessment, 2025; FinCEN, Chinese Money Laundering Networks: 2020-2024 Threat Pattern & Trend Information, August 2025; FinCEN, Advisory on Kleptocracy; Multi-lateral REPO Task Force, Global Advisory on Russian Sanctions Evasion, March 2023; United Nations (UN) Security Council, Panel of Experts Reports on DPRK, 2024; Federal Bureau of Investigation (FBI) Internet Crime Complaint Center (IC3), Internet Crime Report 2025; House Select Committee on China, DeepSeek Unmasked, April 2025, and Buy What It Can, Steal What It Must: China's Campaign to Acquire Frontier AI Capabilities, April 2026; US-China Economic and Security Review Commission (USCC), 2025 Annual Report; ODNI, Annual Threat Assessment of the US Intelligence Community, 2026.

	distributing and shifting accountability and nature of intermediation across global technology stacks; near-instant global P2P liquidity networks operated by offshore issuers outside U.S. supervisory reach	screening; programmable on-chain enforcement logic allows automated, global conditions checks for controls like sanctions and KYC screening
Quantum Computing	*Legacy:* Financial tracking relies on standard computers that struggle to spot complex patterns across massive databases, while everyday encryption keeps data safe for decades. *New:* Next-generation quantum computers can analyze massive, interconnected data all at once, but their extreme power can easily crack the standard encryption protecting our financial data.	*Risk:* Hackers and foreign adversaries can steal and save encrypted banking data today, waiting for quantum computers to come online and unlock it later ("harvest now, decrypt later" typology), rendering legacy security protocols obsolete. *Opportunity:* Financial institutions can upgrade to quantum-secure cryptography to protect data and transaction integrity, while using advanced computing to instantly catch hidden criminal networks across the global banking system
Privacy Enhancing Technologies (PETs)	*Legacy:* Financial privacy means keeping customer records locked away in separate, private bank silos to shield sensitive information from outside eyes. *New:* Advanced coding allows banks to mathematically check and prove compliance rules are being met without ever having to expose or share the underlying personal data	*Risk:* If these tools are poorly designed, criminals can use them to build completely uncrackable financial blind spots that stop authorities from tracking dirty money, prevent companies from understanding their counterparty risk, and deny consumers and counterparties recourse for recovery for criminal and civil proceedings *Opportunity:* With sufficient governance and calibrated identity/attribute discoverability frameworks, financial institutions can securely verify identities and screen for protections like sanctions in real time, and government authorities can share and access sensitive data, while maintaining necessary privacy and minimizing sensitive data access[5]

These technologically-driven shifts are reshaping where accountability attaches, what detection requires, and how fast exploitation can occur. The governance challenge is not whether to embrace or resist these technologies; that debate is largely settled by market reality. The question is whether the United States shapes their integration into the financial system on terms that preserve accountability and democratic oversight, or cedes that shaping to actors with different interests. Governance built into architecture at the design stage is orders of magnitude cheaper and more effective than governance retrofitted after exploitation has already occurred. That principle isn't unique to finance, but sits at the heart of every major technology transition the national security community has lived through.[6]

THE FRAMEWORK IN PRACTICE: WHO PARTICIPATES, WHAT CAN BE SEEN, AND WHAT CAN BE DONE

Effective AML/CFT frameworks rely upon policy, technological, and operational measures being implemented around core areas such as identity and trust; data, analytics, and detection; and operational coordination and enforcement. These underscore how the key failures in illicit finance frameworks tend to occur when either (1) we do not know who owns or controls something; (2) we cannot connect what

[5] *Sources for table analysis:* Commodity Futures Trading Commission (CFTC) Technology Advisory Committee (TAC), Responsible AI in Financial Markets, May 2024, and Decentralized Finance Report, January 2024; Chainalysis, Crypto Crime Report 2026; Financial Action Task Force (FATF), Virtual Assets Targeted Update (July 2024); Cyber Risk Institute and Financial Services Sector Coordinating Council (FSSCC), Financial Services AI Risk Management Framework, 2026; NIST, Post-Quantum Cryptography Standards.

[6] White House, National Strategy to Secure 5G, 2020; USCC, *U.S.-China Competition in Emerging Technologies, Chapter 3,* 2024 Annual Report to Congress.

different institutions are seeing; or (3) we cannot act on what we know in time to matter. Below I walk through some of the critical elements for each of these areas, along with a specific note on the value of BSA data that is central to this hearing.

Who Participates: Identity, Accountability, and the Beneficial Ownership Gap

A foundational question of any financial integrity framework is whether we know who is actually in the system and understand their risk profile. Increasingly, the answer is no, and the tools Congress built to address that gap are being suspended or reversed, and without corresponding or compensating measures to help address the gaps they are creating.

Beneficial Ownership and the Corporate Transparency Act

In March 2025, FinCEN's interim final rule effectively suspended BOI reporting for approximately 99.98% of domestic entities Congress intended to cover.[7] The formation jurisdiction remains the primary vulnerability, not the nationality of the ultimate owner. Shell companies are formed under U.S. state law, by U.S. registered agents, to obscure the identities of those who benefit from and control them.

The severe national security consequences are well documented[8] by both Congressional offices as well as government agencies. The House Select Committee on China found U.S. chips subject to export controls were potentially funneled to Chinese military programs through U.S.-registered shell companies a median of 140,000 chips to People's Republic of China (PRC)-linked entities in 2024 alone.[9] The Select Committee's DeepSeek report found the AI system was reportedly built using chips acquired through shell structures circumventing export controls.[10] Without BOI data on U.S.-formed entities, BIS enforces export controls largely blind on the corporate structuring side.

Crucially, this blind spot directly paralyzes our ability to disrupt the supply chain of deadly synthetic opioids. FinCEN's analytics reveal that financial institutions reported over $312 billion in suspicious activity tied to decentralized, horizontal CMLOs operating as a service for Mexican cartels like Sinaloa and CJNG.[11] These networks heavily rely on networks of U.S.-registered front and shell companies to execute near-real-time mirror transactions and trade-based laundering schemes, effectively washing fentanyl proceeds outside formal banking channels before law enforcement can trace the source.

Especially in light of the CTA's constitutionality being upheld[12], Congress could act to make its intent unambiguous: the CTA was enacted with broad bipartisan support precisely to address the shell company vulnerability I've discussed and noted in assessments by this and prior Administrations and this Congress. Congress maintains the authority to require its implementation and consider whether statutory clarification or refinements are needed to ensure the law operates as Congress intended.

Investment Advisers, Real Estate, and Professional Enablers

Investment advisers manage approximately $146 trillion[13] in assets yet remain substantially outside BSA AML program and SAR filing requirements, a gap that has been flagged repeatedly by the FATF and detailed by the U.S. Treasury as a primary kleptocracy and sanctions evasion vector.[14] The U.S. Treasury's

[7] Congressional Research Service (CRS), R47255, March 2026; FACT Coalition, FATF Evaluation Fact Sheet, May 2026.
[8] Transparency International, United States: Reinstating Corporate Secrecy Protects Money Launderers and Foreign Criminals – Not Small Businesses, March 2025.
[9] House Select Committee on China, Press Release, Protecting U.S. Tech: China Committee and Bipartisan, Bicameral Leaders Unite to Stop CCP AI Chip Smuggling, July 2025.
[10] House Select Committee on China, DeepSeek Unmasked, April 2025.
[11] CRS, R48786, Chinese Money Laundering Networks, January 2026.
[12] Holland & Knight Alert, Eleventh Circuit Upholds Constitutionality of Corporate Transparency Act, December 2025.
[13] Securities Exchange Commission (SEC), Investment Advisor Statistics, visited May 2026.
[14] US Treasury, National Money Laundering Risk Assessment, March 2026; FATF, Mutual Evaluation Report, United States: 7th Follow-Up Report & Technical Compliance Re-Rating, March 2024.

delay on the investment advisers rule implementation and signaling of forthcoming changes leaves uncertainty to the extent that these controls will take effect.[15] Similarly, the residential real estate sector remains one of the most extensively documented gateways for foreign illicit money to penetrate the U.S. financial system. A landmark study by Global Financial Integrity (GFI), the FACT Coalition, and Anti-Corruption Data Collective analyzed a fraction of known cases, identifying illicit and suspicious funds funneled directly through U.S. real estate across 25 cases with total property value exceeding $2.6 billion.[16] Yet, the regulatory path forward for many of these enablers remains deeply unstable after both postponements and a Federal district court vacating the rule.[17]

Sophisticated illicit finance rarely operates without professional facilitation (e.g., lawyers, accountants, formation agents, and real estate professionals), yet these gatekeepers and enablers remain inconsistently covered despite longstanding FATF and national security concerns.[18] The operational friction we've seen surrounding these frameworks signals that Congress could leverage this opportunity to actively review and reframe how these authorities are designed, ensuring future implementation is tailored, predictable, and aligned with the practicalities of American commerce. Yet, we cannot mistake administrative or judicial complexity for a lack of strategic threat; yielding to compliance fatigue by entirely abdicating oversight over these multi-trillion-dollar sectors is not a policy solution, but an open invitation for our adversaries to exploit the systemic blind spots we choose to leave undefended.

"Knowing Your Customer" and Digital Identity as Infrastructure

A significant share of compliance burden is a symptom of broken identity infrastructure,[19] not an inherent feature of AML requirements. Institutions are repeatedly verifying information the U.S. government already knows authoritatively, often through manual document review and layered self-certification that is simultaneously expensive and unreliable. The KYC obligation is not the problem. The mechanism by which it is discharged is, and that distinction requires precision.

- *"Fixing" KYC and the Nuance It Demands:* "KYC" is a colloquial term covering a layered set of obligations that operate differently and present different modernization challenges. At the foundation is identity verification (i.e., establishing that an identity is real, that it belongs to the person or entity asserting it, and that the assertion can be trusted). On top of that sits risk assessment and potential obligations like enhanced due diligence (EDD): understanding a customer's profile well enough to evaluate not only AML/CFT exposure but the broader business risk of the relationship. Then comes ongoing monitoring – continuous reassessment of that profile as behavior, relationships, and circumstances evolve. None of these is a binary yes-or-no check, nor are the elements needed for one of these pieces of KYC the same for the others. Each involves judgment, dynamic data, and contextual analysis that no static credential or point-in-time verification can fully satisfy.

  When practitioners say KYC needs to be fixed, the honest answer is: which part, and fixed how? The obligation *to know your customer* is not likely going away under any serious reform framework (and should not). What is going to change (and should) includes the identity infrastructure and trust framework institutions rely on to satisfy it, as well as considering more nuanced and tiered frameworks for *what information* (or "attributes") different financial institutions and intermediary

[15] U.S. Treasury, Delaying the Effective Date of the Anti-Money Laundering/Countering the Financing of Terrorism Program and Suspicious Activity Report Filing Requirements for Registered Investment Advisers and Exempt Reporting Advisers, 91 Fed. Reg. 36, January 2026.
[16] GFI, FACT Coalition, Anti-Corruption Data Collective, Money Laundering Risks in Commercial Real Estate, May 2024.
[17] Paul Weiss, Economic Sanctions and Anti-Money Laundering Developments – 2025 Year in Review; FinCEN, Residential Real Estate alert, March 2026.
[18] FinCEN, Fact Sheet: FinCEN Issues Final Rule to Increase Transparency in Residential Real Estate Transfers, (2024).
[19] *See* Better Identity Coalition, A Policy Blueprint for the New Administration, 2025.

or infrastructure providers *need to know* about their customer to adequately assess and mitigate their risk profile. The question worth asking is not whether to know your customer but what attributes and credentials, asserted through what trust framework, most reliably establish the things that are more important for risk assessment. A reformed system built on authoritative, interoperable identity infrastructure reduces burden precisely because it makes that determination more reliable and more targeted – not because it asks less of institutions, but because it gives them better tools to answer the right questions.

- *The Privacy and Data Security Symmetry:* Within this infrastructure debate, data collection and data minimization are often pitted against accountability. A common critique from DeFi and digital asset advocates highlights the risk of "honeypots" (i.e., centralized data repositories containing highly sensitive personal data that can become prime targets for cybercriminals and state-sponsored hackers). Data minimization is a deeply valid concern; we must be deliberate about ensuring that only the specific information required to support legal accountability is collected and stored.[20]

  However, a structural inconsistency often undermines a one-vector approach to this argument: the premise that users should comfortably trust firms like digital asset companies to custody millions of dollars in sovereign wealth or digital assets, yet simultaneously claim these same firms are fundamentally incapable of safeguarding the basic customer data required to enable due process, consumer protection, and legal accountability, (or that they should face no issues sending money to counterparties in jurisdictions where they are unwilling to send information to allow for counterparty institutions to understand their own AML/CFT risk exposure) lacks internal logic. Financial integrity cannot be a one-way street where firms claim the sophisticated technical capacity to manage automated global value transfer, yet plead operational poverty when it comes to standard data security and governance.

- *Smart Privacy and PETs:* Real privacy doesn't mean a complete absence of records; it means calibrated discoverability – ensuring sensitive financial details are only exposed to lawful authorities under specific, legal conditions. We already have the tech (e.g., zero-knowledge proofs, homomorphic encryption, multi-party computation, and other PETs) to basically mathematically prove certain facts without exposing the underlying data (think of the ability to screen whether certain attributes of an identity are on a sanctions list). The catch is operational with PETs, which haven't yet really presented real-world frameworks that allow financial institutions banks, regulators, and law enforcement to conduct their relevant level of continuous, real-time risk monitoring, or provided a secure, legally backed way to unmask an identity under conditions like when a valid court warrant is issued. But PETs are likely to be a critical component of future financial systems; we just have to work out issues around the tech but especially the governance.[21]

- *The Deepfake and AI Authenticity Crisis:* Digital identity matters far beyond standard compliance concerns. The U.S., along with the rest of the globe, is facing a massive identity authenticity crisis because generative AI and deepfakes can now easily trick traditional, document-based KYC checks. However, the U.S. is backfooted compared to other parts of the globe[22] because we haven't invested in secure, interoperable, trustworthy, privacy-preserving digital identity infrastructure, such as verifiable credentials and privacy-preserving attribute validation services. Even the measures from President Biden's last cybersecurity Executive Order for improving U.S. Government acceptance of standards-compliant and privacy-preserving digital identity credentials

[20] National Institute of Standards and Technology (NIST), Privacy Framework v1.0, January 2020; CFTC TAC, DeFi Report, January 2024.
[21] CFTC TAC, DeFi Report, January 2024.
[22] Atlantic Council, Exploring the Global Digital ID Landscape, July 2025.

to improve integrity of and fight fraud in government benefits programs were rescinded in 2025.[23] In the absence of any widely scaled "trust-tech" infrastructure at the identity layer, our financial system is vulnerable to highly automated and industrialized fraud.

Solving this identity layer is an absolute prerequisite not only to address AML/CFT and cybercrime (where identity compromise is an extremely common vector of compromise – FinCEN even identified $212 billion in identity-compromise enabled suspicious activity in 2021 alone[24]), but also for unlocking agentic commerce. As major institutions, governments, and Fortune 500 companies embrace the upcoming wave of autonomous AI agents buying and selling things on behalf of humans, these agents will inherently be reliant on some kind of infrastructure to determine human and legal person identity and permissions. Without a secure identity foundation, AI agents will simply scale up fraud at a speed and volume that human investigators can't possibly track, destroying trust in the whole system.

Congress can direct some concrete steps to make meaningful progress in laying a stronger, more trustworthy identity foundation in AML/CFT. For example, you could direct FinCEN and banking regulators to use their existing tools, such as FinCEN's exceptive relief authority, to launch formal, clear regulatory pilot programs with established on-ramps and off-ramps for approval, measurements for efficacy, frameworks for identity information interoperability, sharing, and reliance. Congress could also ensure that Federal policy promotes targeted measures like Treasury- and DHS-led grant programs to support state-level adoption of secure digital credentials that meet NIST standards. Furthermore, Congress could reinstate the specific public benefits and anti-fraud protections that were lost when the previous administration's cyber-security directives regarding systemic public benefits fraud were rescinded, to include pilots for alerting Americans when their identity is used in Federal benefits applications and privacy-preserving attribute validation services to support financial institution identity verification processes.

What Can Be Seen: Intelligence Architecture, BSA Data, and the Data Imperative

Modern financial crime is networked, which demands that our financial intelligence architecture become equally networked.[25] The most sophisticated criminal operations are specifically designed to remain below the detection threshold of any single institution, distributing activity across platforms, payment rails, and jurisdictions precisely because fragmented visibility protects them. We need to preserve and strengthen the ability of public and private sectors to better put those pieces of fragmented visibility together.

<u>The Value of BSA Data and Why It Should Not Be Casually Reduced</u>

Before accepting arguments that BSA reporting obligations should be substantially reduced, the operational record deserves direct examination. Critics frequently rely on shortsighted metrics that evaluate BSA utility solely by the number of new investigations directly initiated by a single report. This misunderstands the lifecycle of financial intelligence. For example, IRS Criminal Investigation's February 2026 BSA metrics report[26] documented that in FY2025, 94% of IRS-CI cases were searched against BSA data, generating more than 3.9 million database searches, and nearly 67% of investigations had primary subjects associated with currency transaction reports (CTRs).

IRS-CI's report demonstrates how significant value from BSA data is often retrospective and compound, serving as a critical investigative accelerant that maps out networks, identifies hidden assets, and hardens evidence in thousands of *existing* or late-stage investigations long after a report is filed. Furthermore,

[23] Politico, Trump's Cyber EO Kills Biden-Era Digital Identity Policies, June 2025.
[24] FinCEN, Financial Trend Analysis, Identity-Related Suspicious Activity, 2024.
[25] Carole House and Joby Carpenter, Why Governments Need to Treat Fraud Like Cyberwarfare, Not Customer Service, January 2026.
[26] IRS-CI, FY 2025 BSA Metrics, February 2026.

focusing strictly on individual case-matching ignores the strategic power of aggregate data. FinCEN and law enforcement rely on macro-level BSA datasets to conduct financial trend analyses and build complex illicit finance typologies. This aggregate intelligence allows agencies to map systemic vulnerabilities, identify emerging threat vectors, and strategically deploy finite law enforcement resources to high-risk sectors. DEA and FBI financial intelligence functions similarly depend on BSA reporting as foundational investigative infrastructure. The detection signal embedded in that data (including in currency reporting at current thresholds) reflects transaction patterns that have become more anomalous, not less, in an increasingly digital economy.

The case for maintaining the current reporting architecture is not that the system is optimal as designed. It is that the intelligence value embedded in BSA data is demonstrably high, currently irreplaceable by alternative mechanisms, and would be degraded by threshold increases or volume reductions before any substitute detection infrastructure exists to address those shifts in a way that meaningfully words to improve efficacy. Any reduction in reporting obligations should be in consideration of demonstrated law enforcement utility metrics and evidence that alternative detection capabilities are in place where that information would be of national security and law enforcement value, not simply on compliance cost reduction. The operational record supports maintaining the existing framework while investing in the quality and interoperability of the data it generates, not dismantling it.

Cross-Institutional Intelligence Sharing

The SAR sharing pilot authorized under AML Act Section 6212 produced an NPRM in January 2022 and has not been finalized in over four years.[27] This is a high-value yet unfulfilled AMLA promise for driving improved operational financial intelligence. And while there is a great amount of opportunity for liability protections like 314(b) to be used more fulsomely by the financial sector, the 314(b) voluntary sharing framework should also be modernized to keep pace with the scale and sophistication of threats and the complexity of infrastructure and service offerings in modern payments – extending it in the statute to explicitly cover information related to the money laundering predicate offenses such as cyber intrusion, fraud, and sanctions violations, and broadening eligibility beyond traditional financial institutions to the compliance and investigative firms often best positioned to detect early warning of coordinated illicit activity.[28] With Congress's intent via 314(b) being to enable information sharing for prevention and detection of money laundering, I posit that sharing of the underlying criminal activity appear should reasonably and clearly be covered under the scope of the information sharing protection. The Cybersecurity Information Sharing Act succeeded precisely because collective defense requires broad participation. Financial crime defense requires the same logic.

Structured Financial Crime Data Standards and OSINT

The development of STIX/TAXII[29] transformed cybersecurity's collective defense capability by creating standardized, machine-readable, timely threat intelligence sharing. As Natalie Loebner has argued in her Open Banker framework, BSA data is a public good currently trapped in private silos.[30] Shared taxonomies, common data dictionaries, machine-readable typology frameworks, and real-time intelligence exchange would multiply investigative capacity across institutions and agencies. Without this architectural investment, each institution builds detection capability in isolation and the system remains less than the sum of its parts. Congress also should urge Treasury to make clear expectations for integrating valuable, openly available information (open source intelligence or OSINT) into their AML/CFT programs, and

[27] CRS, FinCEN: AMLA 2020 Implementation and Beyond, March 2026.
[28] Carole House testimony, HFSC Hearing on Cryptocrime, 2024; FinCEN, Section 314(b) Fact Sheet, December 2020; CISA, Cybersecurity Information Sharing Act of 2015; ACAMS International Anti-Fraud and Technology Task Force, Cross Sector Fraud Information Sharing: Pathways to Action, March 2026; Consumer Bankers Association, Summary of July 17, 2024 Fraud and Scams Roundtable.
[29] Center for Internet Security, Real-Time Indicator Feeds.
[30] Natalie Loebner, Following the Money: Tools and Techniques to Combat Fraud, July 2025.

especially offer valuable guidance on high-impact types of data related to particular typology or priority threat detection. There are vast opportunities for this integration – corporate registry records[31], open blockchain data, commercial data, social media and news – that similarly functions as a force multiplier the current framework has not enabled through safe harbors or structured access mechanisms. And finally, feedback loops on the utility of specific data and reporting, especially SARs, remains an under-delivered hope from the AMLA that Treasury could prioritize to improve value and reduce effort by both investigators and industry.

Digital Assets and Offshore Stablecoin Coverage

I testified to the House Financial Services Committee Subcomittee on Digital Assets, Financial Tehcnology, and Inclusion in February 2024 on cryptocurrency crime issues. For consideration by this Subcommittee, I shall relay some of those same elements, which generally remain unchanged in my assessment:

- *Blockchain Analytics Utility:* "One important distinction between most cryptocurrency systems and traditional financial systems is cryptocurrency's often public and transparent nature – SWIFT, FedWIRE, and cash movements do not publish transactions to public ledgers or records that anyone can see. Cryptocurrency systems offer unprecedented public visibility of certain financial activity. This public visibility has played an important role in mitigating risks in cryptocurrency illicit finance, enabling the rise of cryptocurrency analytics firms and investigative tools and techniques to better and more timely trace and interdict crypto crime proceeds.[32] However, there are limitations to this transparency, such as in that off-chain data and transactions are not visible publicly[33], as well as the use of methods like mixing, chain-hopping, and encryption to obscure the ledger or system of record.[34] There are also disagreements amongst analytic firms on attributions made using proprietary analytic methods and AI/ML clustering models, as well as ongoing concerns with auditability, corroboration, explainability of some of these proprietary solutions that could present serious challenges to best leveraging what information is public on blockchain ledgers.[35] Public transparency of financial information also inherently presents challenges for consumer privacy, especially when considering the pace of open source AI/ML technologies that may increase public attribution of transactions on unobscured ledgers." There are immense opportunities to leverage this unprecedented financial transparency to improve systemic compliance across the cryptocurrency industry – we just haven't gotten there yet with the combined state of regtech, operational coordination, and compliance.

- *Cryptocurrency Illicit Finance Metrics:* "While it is difficult to accurately assess the amount of illicit finance in any financial system, including in cryptocurrency ecosystems, regulatory technology (RegTech) firms as well as financial and law enforcement networks shed some light on the scale of the problem. Some analytics firms estimate less than 1% of cryptocurrency transaction volume to be illicit.[36] However, while these and other RegTech firms are critical to enable investigations by industry and law enforcement, this figure and others from blockchain analytics firms likely underestimate illicit activity. While the figures would represent best estimations from the firms based on information available to them, the numbers would not be comprehensive. They would not account for off-chain data and only include activity already known to the RegTech firms

[31] Kharon, White Paper Supporting Urgent Need for AML/CFT Modernization, September 2025.
[32] *See* United States District Court for the District of Columbia, Case No. 20-sw-314 (ZMF), *In the Matter of the Search of One Address in Washington, D.C., Under Rule 41* (January 6, 2021).
[33] For example, this could include internal cryptocurrency exchange activity or transactions conducted off-chain over the Bitcoin Lightning Network via a Lightning channel.
[34] *See* FinCEN, Advisory FIN-2019-A003, "Advisory on Illicit Activity Involving Convertible Virtual Currency" (May 9, 2019).
[35] *See* Ciphertrace, Defense Expert Report, *United States v. Roman Sterlingov, 21-CR00399 (RDM)* (August 8, 2023).
[36] *See* Chainalysis, "2024 Crypto Crime Trends: Illicit Activity Down as Scamming and Stolen Funds Fall, But Ransomware and Darknet Markets See Growth" (January 18, 2024).

as having been identified to be illicit. In 2020, FinCEN highlighted that it received suspicious activity reporting (SARs) in 2019 associated with cryptocurrency activity amounting to $119 billion, or 11.9% of the total cryptocurrency market.[37] Of course, this number may likely be overestimated, as "suspicious" activity does not mean it is necessarily illicit. However, the FinCEN SAR figure also only accounted for reporting from *compliant, U.S. cryptocurrency service providers*, implicating that global suspicious activity metrics would be much higher, especially if global compliance were in a better state to address pervasive underreporting issues." Governance frameworks should not be calibrated to the most favorable estimate of the problem.

- *Off-shore USD Stablecoin Challenges:* Legislative and regulatory design choices have left a massive, peer-to-peer dollar-denominated ecosystem operating entirely outside direct U.S. jurisdictional hooks.[38] This regime effectively allows offshore issuers to generate billions in a kind of "shadow" dollar liquidity, establishing an unchecked secondary market that expands access to our financial system in some cases to our most critical state and non-state adversaries – including the Iranian Revolutionary Guard Corps (IRGC)[39], the ruble-backed stablecoin A7A5[40] (run by sanctioned oligarch Ilan Shor, and the virtual opening for which Putin reportedly attended[41]), and reportedly a system where Putin attended the launch), and the DPRK (all of which are subject to U.S. sanctions designations). A major challenge presented by this parallel architecture is that it systematically undermines the core mechanics of economic statecraft. Sanctions regimes - especially strict secondary sanctions frameworks - only function when the United States can effectively close off alternative relief valves of global dollar access. If billions of dollars are allowed to circulate peer-to-peer via un-interdicted offshore rails, those relief valves remain wide open.

  While recent retroactive, multi-hundred-million-dollar asset freezes[42] by offshore issuers are often cited as compliance successes (and it is a positive indicator to see such freezes), they still signal a deeper, structural failure. Freezing an historically unprecedented volume of assets after the fact does not demonstrate proactive, system-wide compliance; it would instead confirm that a massive, historic scale of the illicit activity that was already permitted to flow through that infrastructure. It is also fundamentally not the role (nor should it be) of the United States Government or Federal law enforcement to serve as the outsourced, retroactive compliance department for highly profitable offshore entities that choose to build their business models by providing un-monitored dollar-equivalent access to high-risk and even U.S.-sanctioned actors. Evolutions are needed to shift global approaches, and U.S. expectations, from simply retroactive compliance with lawful orders to meeting proactive, continuous compliance obligations.

What Can Be Done: Enforcement, Outcomes, and Operational Capacity

Even the best intelligence architecture fails if institutions and governments cannot act quickly enough to impose meaningful consequences. Modernization is not just about rule and policy but also critically relies upon operationalizing capabilities and incentives to deter bad actors – a capability that is eroding but which we can course-correct for the better of industry, Americans, and U.S. national security interests.

---

[37] *See* FinCEN, 85 FR 83840, Notice of Proposed Rulemaking, "Requirements for Certain Transactions Involving Convertible Virtual Currency or Digital Assets" (December 23, 2020).
[38] Carole House testimony, HFSC Hearing on Navigating the Digital Payments Ecosystem: Examining a Federal Framework for Payment Stablecoins and Consequences of a U.S. Central Bank Digital Currency, March 2025.
[39] Elliptic, Israel Links Crypto Wallets that Received $1.5 Billion to Iran's Revolutionary Guard, September 2025.
[40] Elliptic, A7A5: The Ruble-Backed Stablecoin Crosses $100 Billion in Transactions, January 2026.
[41] Mike Eckel and Ernist Nurmatov, Radio Free Europe/Radio Liberty, The Fugitive Oligarch, The Cryptocurrency, and A 'Wild' Kremlin-Blessed Sanctions Evasion Scheme, December 2025.
[42] For example, *see* CNN, US Freezes $344 Million in Cryptocurrency to be Linked to Iran, April 2026.

Enforcement Timeliness, Calibration, and the Deterrence Problem

FinCEN has historically operated with resources that have not kept pace with its expanding mandate. An agency with such a critically important mission must be adequately supported to safeguard the financial integrity framework that the national security apparatus, and consequently the American public, relies upon. Even under baseline operational conditions, FinCEN and the Federal banking agencies already face acute statutory delays, frequently executing enforcement actions so many years after a violation occurs that their deterrent and sector-shaping impact is severely degraded. Civil enforcement achieves its compounding national security objectives only when it is early, iterative, calibrated, and based on clear, enforced expectations before compliance failures mature into systemic vulnerabilities.

The structural changes introduced in the April 2026 Notice of Proposed Rulemaking (NPRM) governing AML/CFT compliance programs could potentially risk institutionalizing administrative paralysis unless deliberate and accelerating measures to meet this new system of supervision and approval are emplaced.[43] The proposed framework of routing FBAs (which possess independent statutory authority to enforce compliance) through a new consultation process through FinCEN before bringing significant supervisory actions could improve interagency coordination on enforcement but could also inadvertently create a kind of gatekeeping that would further reduce timely oversight and enforcement unless resources are properly committed to the Bureau and broader enforcement regimes.[44] Separately, on support to asset recovery, FinCEN's Rapid Response Program[45] has demonstrated the value of real-time coordination in fraud interdiction to recover funds stolen and defrauded from Americans. That model deserves expansion and sustained resourcing by Congress.

Outcomes-Oriented Supervision: Defined, Not Assumed

Stakeholders broadly support a transition toward risk-based, outcomes-oriented AML supervision. However, the practical challenges of implementing this paradigm shift without sacrificing regulatory clarity remain a primary concern across both regulatory bodies and industry. The current system still lacks actionable, standardized definitions of what an "effective outcome" actually is, too often defaulting back to legacy, forensic check-the-box exercises that neither public nor private sectors are happy with.

There is an immediate opportunity for Congress and regulatory agencies to bridge this gap through steps shifting from rigid, static rules to dynamic behavioral science models.[46] By leveraging next-generation data architecture (e.g., specifically privacy-preserving technologies like federated learning), financial institutions can collaboratively train machine learning models to detect complex illicit behavior patterns across separate entities without compromising consumer privacy or violating data localization laws.

On a tactical level, Treasury could lead a public-private research initiative tasked with establishing concrete, quantifiable performance metrics that move beyond mere transaction volumes. True structural efficacy would be best measured through explicit operational indicators. Some options Laurence Hamilton at Consilient published for consideration: coverage, or the scope of exposure surfaced; precision, or the elimination of false positives, prioritization, meaning ensuring the highest behavioral risks rise to the top of review queues first; and case aging, to measure the latency between detection and law enforcement utility.[47] Dropping false negatives, interdiction and investigative utility and rate could also be valuable. Additionally, regulators should publish clear, sector-specific examination guidance that hones the FFIEC manual, establishes predictable safe harbors for model validation, and partners with international standards bodies to turn outcomes-oriented theory into repeatable, inspectable supervisory realities.

---

[43] FinCEN, *Notice of Proposed Rulemaking: Anti-Money Laundering and Countering the Financing of Terrorism Programs*, 91 Fed. Reg. 7033, April 2026.
[44] Reuters, US Justice Dept Disbands Crypto Enforcement Team, Citing Trump Order, April 2025.
[45] FinCEN, Rapid Response Program Fact Sheet.
[46] Gary Shiffman, The Economics of Violence, January 2020.
[47] Laurence Hamilton, Consilient, The Future of AML Effectiveness: The Metrics Regulators Will Expect in 2026.

International Coordination and the FATF Mutual Evaluation

The United States is undergoing FATF's fifth-round mutual evaluation, with the on-site visit completed in early 2026 and the report expected later this year.[48] Several areas may present concerns given historical issues raised by the FATF in evaluations of the US frameworks, including the effective suspension of CTA BOI functionality, unresolved investment adviser and real estate gaps, declining enforcement intensity, and reduced emphasis on professional enablers. A poor FATF evaluation could present tangible challenges to the U.S. economically and diplomatically. For example, it could give foreign correspondent banks formal grounds to apply enhanced due diligence to U.S.-related transactions, reducing U.S. leverage in multilateral financial diplomacy, and providing adversaries a ready-made argument for alternative financial architectures that could reduce U.S. visibility and sanctions reach.

Dollar primacy does not rest on military power alone. It rests on confidence that dollar-denominated transactions occur within a system governed by rules that are consistently enforced. The AML/CFT architecture and the sanctions toolkit are not separable from that confidence. The U.S. Treasury has continued to engage in the FATF Plenary, and the mutual evaluation process that Treasury has been leading engagement under will have been a good opportunity to demonstrate continued commitment to that framework. This Subcommittee should treat the FATF evaluation report as a priority oversight document and hold a dedicated hearing on its findings once released as part of your deliberations on trying AML/CFT reform.

CONCLUSION

Our adversaries watching this hearing are not hoping the United States modernizes successfully. They are hoping we reduce visibility without improving infrastructure, coordination, or operational effectiveness. They benefit when accountability gaps widen, when enforcement becomes fragmented, and when democratic governments fail to adapt quickly enough to preserve operational advantage.

Congress has already done substantial bipartisan work in response. The task now is to finish that modernization – restoring accountability where visibility has been weakened, building digital-era identity infrastructure, modernizing intelligence sharing frameworks, and ensuring enforcement capacity keeps pace with technological change.

Thank you. I welcome the Subcommittee's questions.

[48] FACT Coalition, FACT Sheet: What to Know About the US FATF Evaluation, and Why It Matters, May 2026.