UNITED STATES HOUSE OF REPRESENTATIVES

HOUSE COMMITTEE ON FINANCIAL SERVICES

"CONVERGING CRIMINAL ENTERPRISES: CHINESE MONEY LAUNDERING NETWORKS AND CARTEL FINANCING IN THE U.S. FINANCIAL SYSTEM"

JUNE 9, 2026

STATEMENT OF LOUIS G. DETITTO

I. INTRODUCTION

Modern transnational organized crime is increasingly driven by financial architectures designed to exploit institutional fragmentation. Traditional anti-money laundering (AML) systems were built to detect more linear transaction patterns, but Chinese Money Laundering Networks (CMLNs) operate across fragmented corporate, regulatory, and digital environments, using the seams between institutions as cover rather than relying on any single point of failure. (U.S. Department of the Treasury, 2024)

The challenge these networks present is therefore not simply one of volume, but of structure and convergence. CMLNs connect cartel proceeds, Chinese capital flight, fraud, cyber-enabled crime, shell companies, student account holders, front businesses, and cross-border trade into adaptive laundering systems that can appear routine when viewed in isolated parts but function as coordinated financial infrastructure at scale.

The core difficulty in disrupting these networks lies in institutional fragmentation. Financial institutions, law enforcement, intelligence agencies, and regulators may each hold part of the picture, but legal, organizational, and technical barriers often prevent those pieces from being integrated. As a result, CMLNs and their criminal partners can distribute activity across institutions and jurisdictions, exploit the blind spots built into the system, and remain resilient unless they are addressed through network-level analysis, secure information sharing, and coordinated public-private disruption.

II. BACKGROUND

For the past 20 years, I have worked at the intersection of national security, finance, and advanced analytics, with a focus on organized crime and network intelligence. I have led major efforts across the public and private sectors to identify, disrupt, and mitigate money laundering, fraud, threat finance, and other forms of organized criminal activity. As a federal law enforcement officer, I conducted intelligence-driven investigations into domestic and transnational criminal organizations involved in narcotics trafficking, weapons trafficking, and

money laundering. I have also used telecommunications and digital communications data to map networks, trace cross-border illicit trade, and identify emerging threats at scale.

In the private sector, I worked at a global financial institution, where I led and oversaw thousands of complex money laundering and fraud investigations, many involving active law enforcement and national security concerns. I have also applied data analytics and investigative methods aligned with the Anti-Money Laundering Act of 2020's national priorities to identify emerging risks involving Chinese Money Laundering Networks (CMLNs), transnational crime, drug trafficking organizations, terrorism financing, sanctions evasion, virtual assets, fraud, cyber-enabled crime, human trafficking, corruption, and malign foreign influence. In recent years, I have focused on the growing national security threat posed by the relationship between cartels, Transnational Criminal Organizations (TCOs) and CMLNs and have worked to counter its rapid escalation.

III. CMLNs AS FINANCIAL ENABLERS: SCALE, INFRASTRUCTURE, AND ADAPTATION

CMLNs have become key financial enablers for cartels and other transnational criminal organizations, providing fast liquidity and near-instant value transfer in exchange for illicit proceeds. They use networks of licit and illicit businesses to launder funds and help these organizations expand their influence inside the United States. (FinCEN, 2025; DOJ, 2024)

Using proceeds from drug trafficking, fraud, and other crimes, CMLNs build durable infrastructure in the United States, including:

- Commercial and residential real estate, including apartment complexes and rental properties
- Businesses that mix licit and illicit activity, including operations tied to counterfeit goods
- Farmland, including legitimate agricultural operations and illicit marijuana grows

This infrastructure provides permanent presence and recurring income that reinforce these networks' reach and staying power.

Generative AI and other emerging technologies are making these networks faster, more efficient, and more difficult to disrupt. CMLNs are using them to create deepfakes for fraud, spoof biometrics in real time to bypass Know Your Customer controls, generate convincing forged financial documents that avoid AML scrutiny, and refine trade-based money laundering schemes through localized legal and trade analysis. (FinCEN, 2025)

CMLNs operate through rapid, repeatable, and scalable processes that strain institutional defenses. They rely on volume, speed, and complexity to move with minimal friction. On a rolling basis, they open dozens, hundreds, or even thousands of accounts across banks,

cryptocurrency exchanges, online casinos, money services businesses, and other financial or digital channels to store, transfer, and distribute funds globally. They also establish shell companies across multiple jurisdictions in the United States and abroad to accelerate and disguise the flow of money. By the time one institution detects and reports suspicious activity, the funds have often already moved through other institutions in the United States or overseas, making it rare for any single institution to see the full laundering cycle from origin to destination. (FinCEN, 2025)

In recent years, illicit financial networks have moved away from the centralized, hierarchical structures once associated with traditional syndicates and toward decentralized, highly distributed models. Modern laundering operations now move simultaneously across dozens of global banks, in multiple jurisdictions, and through a growing mix of digital and informal financial channels. This shift is deliberate. Even when individual actors move large, obvious sums through linear pathways that trigger AML alerts, these networks rapidly disperse activity through layered transactions, indirect connections, and specialized actors spread across the system. The objective of these networks is therefore not simply to obscure individual actions, but to obscure the relationships that link those actions together. The risk becomes visible only when these separate elements are connected and analyzed as coordinated actions and viewed as part of a broader trend or network.

IV. PROFESSIONAL ENABLERS AND PLAUSIBLE DENIABILITY – SEGREGATED ROLES

Professional enablers, including accountants, lawyers, realtors, and investment bankers, can use their expertise to help CMLNs exploit weaknesses in the economic, legal, and financial system. A defining feature of CMLNs is their deliberate use of structure to create plausible deniability. They divide financial pipelines into separate segments, rely on intermediaries, and tightly compartmentalize information, leaving frontline participants with only a narrow view of the broader operation.

Low-level actors, such as cash couriers, account openers, students, and small-scale wire transmitters, often know little about the network's full scope, purpose, or leadership. Because their tasks can resemble legitimate commerce or gig-economy work, they can plausibly claim ignorance during interactions with law enforcement. This insulation protects senior organizers and makes it harder for investigators to prove knowledge of criminal intent higher up the chain.

V. INSTITUTIONAL SEGMENTATION AND STRUCTURAL VULNERABILITIES

Modern laundering networks succeed in part because they exploit the institutional segmentation built into legitimate financial and government systems. Within global banks and regulatory bodies, data is often siloed across separate technology platforms, compliance

functions are split among regional teams, and access is limited by role-based controls. These safeguards serve valid privacy and risk-management purposes, but they also create blind spots across the financial system.

Laundering networks deliberately route transactions through these gaps. An initial cash deposit may occur at one retail bank, layering may pass through a commercial bank in another jurisdiction, and final integration may occur through informal or lightly monitored settlement channels. Because no single compliance officer or law enforcement agency has a complete end-to-end view, coordinated transnational activity often remains invisible or is dismissed as routine noise within individual systems.

VI. CHINESE CAPITAL FLIGHT, CAPITAL CONTROLS, AND UNDERGROUND BANKING

Modern transnational money laundering is closely tied to Chinese capital flight. China's capital controls generally prohibit citizens from moving more than $50,000 USD equivalent out of the country each year without state approval. Yet many wealthy Chinese nationals still seek to diversify assets abroad, purchase foreign real estate, pay for international education, or shield wealth from domestic scrutiny. That mismatch between demand and legal transfer options has fueled the growth of underground banking, which often operate through informal value-transfer networks facilitated by Chinese money brokers and CMLNs.

These networks rely on a trust-based system of ledger balancing rather than physically moving money across borders. For example, a client in Shanghai who wants to move $1 million USD equivalent abroad deposits the same value in Renminbi (RMB) into a domestic account controlled by a Chinese money broker. The broker then uses a matching pool of "mirror cash" held overseas to deposit USD into the client's designated foreign account. No funds cross the Chinese border. Instead, domestic RMB balances are offset against foreign balances in USD or euros. This model creates a constant need for brokers to replenish their overseas cash reserves to satisfy ongoing demand for outbound capital flight. (Department of Justice [DOJ], 2024)

VII. MEXICAN CARTEL CASH, CHINESE MONEY BROKERS AND CAPITAL FLIGHT

This structural need has created a highly lucrative and dangerous partnership between CMLNs and cartels, including the Sinaloa Cartel and the Jalisco New Generation Cartel (CJNG). Mexican cartels and TCOs generate billions of dollars in bulk U.S. cash from domestic narcotics sales, especially fentanyl and methamphetamine. Historically, they struggled to launder these large volumes through Western banks because of strict post-9/11 AML controls and suspicious activity reporting. (Drug Enforcement Administration, 2025; Financial Crimes Enforcement Network, 2025)

Chinese money brokers solved this bottleneck while also addressing their own need for overseas liquidity. In this arrangement, brokers buy bulk cash directly from cartel operatives in U.S. cities at a steep discount. They then use their domestic Chinese networks to transfer equivalent clean RMB from the accounts of capital-flight clients to the cartels' supply-chain accounts in China. Cartels use that RMB to buy chemical precursors from Chinese suppliers, completing a closed and self-sustaining cycle of illicit trade. (Financial Crimes Enforcement Network [FinCEN], 2025)

Because these value transfers largely occur at Chinese banks and are the result of mirror transactions conducted in the United States, the schemes are, by design, not wholly visible to any one US financial institution.

VIII. THE TRIAD NEXUS: HUMAN TRAFFICKING, DRUGS, AND CONTRABAND

This same financial architecture also connects CMLNs to illicit markets associated with Chinese organized crime, such as the Triads. Although modern money brokers may appear to be white-collar operators, their liquidity often derives from Triad-controlled contraband markets. Modern Triads operate diversified poly-crime models that exploit cross-border regulatory gaps and generate both licit and illicit cash for underground banking systems.

One example is the expansion of Triad-linked marijuana grows across North America. By exploiting uneven cannabis legalization regimes, Triad groups operate large illicit grow sites disguised as farms or homes. By evading taxes, licensing requirements, and environmental rules, they undercut legal markets and generate steady cash for Chinese money brokers serving capital-flight clients. The proceeds are often reinvested into residential and commercial real estate, land, and equipment, reinforcing these operations and expanding their domestic footprint. (DOJ, 2024)

Triad networks also intersect with Mexican criminal groups in the trade of synthetic opioids and counterfeit pharmaceuticals. They exploit China's chemical and pharmaceutical sectors to source dual-use precursors that are shipped through complex routes to Mexican cartels for large-scale fentanyl and methamphetamine production. (U.S.-China Economic and Security Review Commission, 2021)

Triad syndicates also produce counterfeit pills or injectables that mimic legitimate drugs such as Adderall, Xanax, Ozempic, and oxycodone, often laced with fentanyl, MDMA, methamphetamine, or other synthetics. Combined with East Asian chemical supply chains and Mexican cartel smuggling routes, this creates an intercontinental production system that fuels addiction while insulating senior syndicate figures from direct exposure in the West.

This model also extends to consumer contraband, especially illicit vaporizers and counterfeit tobacco. Triad syndicates exploit demand for electronic nicotine devices and THC vape oils by flooding United States markets with unregulated, misbranded cartridges, often made in

clandestine factories in southern China and containing unsafe flavoring chemicals or metals. (FinCEN, 2025)

Counterfeit cigarettes and smuggled tobacco remain major revenue sources. Because legal tobacco is heavily taxed in the United States and other Western countries, illicit tobacco offers high margins and often lower penalties than narcotics offenses.

These contraband markets are sustained through trade-based money laundering that routes value back to East Asian commercial hubs. Cash from illicit vapes, counterfeit cigarettes, and synthetic drugs is collected locally and delivered to Chinese money brokers, who use renminbi from capital-flight clients to purchase large volumes of legitimate goods from Chinese factories.

Those goods are then shipped to complicit import-export firms or retail fronts in the West and sold to legitimate consumers. The proceeds enter the banking system as lawful business revenue, allowing Triad syndicates and their money-broking partners to disguise narcotics and counterfeit profits as legitimate commerce.

Triad involvement in human smuggling, trafficking, and forced prostitution further reinforces this model. Human exploitation provides both immediate illicit cash and a captive labor force, and these pipelines are integrated into the same underground banking systems that support cartel activity and capital flight.

Triad cells run multi-jurisdictional human smuggling networks, historically known as “Snakehead” operations, that move people across borders through complex routes. These networks charge high fees, and when migrants cannot pay, smuggling can shift into trafficking through debt bondage.

That debt bondage is used to staff Triad criminal operations. Victims may be forced to work in illicit marijuana grows, manufacturing facilities, construction sites, or cyber-scam compounds under threats of violence, deportation, or harm to their families, reducing labor costs and increasing profits.

Triads also run insulated forced prostitution networks through front businesses such as illicit massage parlors, wellness clinics, and digital escort operations. Victims are recruited with false promises of legitimate work abroad, then stripped of documents and coerced into commercial sex to repay fabricated debts.

These prostitution networks are financially attractive to Chinese money brokers because they generate large volumes of daily retail cash. Brokers can quickly recycle that cash to Chinese nationals seeking capital flight while balancing the ledger through renminbi transfers in China. This integration of human trafficking into the broader Triad-cartel model reflects the efficiency and brutality of modern transnational crime. (FinCEN, 2025)

IX. THE STUDENT 'MONEY MULE' PHENOMENON AND IDENTITY MANIPULATION

To move bulk cartel cash back into the formal Western banking system without triggering alarms, CMLNs use highly segmented identity-based tactics, most notably the exploitation of international students. These networks target Chinese students studying in the United States, Canada, the United Kingdom, and Europe. Because they hold valid visas and legitimate university enrollments, they present as low-risk customers to compliance systems.

Brokers recruit these students through encrypted messaging apps such as WeChat and Telegram, offering commissions, financial incentives, or favorable RMB-to-USD exchange rates for tuition payments. The students are directed to open multiple retail bank accounts at mainstream financial institutions. Once those accounts are active, they either surrender control of them or act as money mules under direct instruction. (FinCEN, 2025)

Brokers then coordinate structured deposits of cartel cash into these student accounts, keeping each transaction below the $10,000 Currency Transaction Report (CTR) threshold in a practice known as smurfing. The funds are quickly moved through peer-to-peer transfers, wire transfers, or official checks to shell companies or escrow accounts, where they are disguised as tuition payments, real estate deposits, or family support. If an account is flagged, the student acts as a buffer, giving both the cartel and the broker plausible deniability and reducing their direct exposure. (FinCEN, 2025)

X. EXPANSION OF SCAM ACTIVITY, FRAUD SCHEMES, AND CONSUMER HARM

The financial infrastructure built to service cartel laundering has increasingly converged with transnational fraud networks, contributing to a major expansion of consumer-facing scams. Among the most prominent is "pig butchering" (Sha Zhu Pan), a highly structured form of investment and romance fraud often linked to Chinese transnational syndicates operating from special economic zones in Southeast Asia. These are not isolated internet scams. They are organized enterprises that use disciplined social engineering, psychological manipulation, and custom digital platforms to extract funds from victims at scale. (Federal Bureau of Investigation Internet Crime Complaint Center, 2025)

Victims are often groomed over weeks or months and persuaded to transfer savings, retirement assets, and home equity into fraudulent cryptocurrency or foreign exchange platforms. Because these transactions are authorized by the victims themselves, traditional bank fraud controls often struggle to intervene, and asset recovery is frequently difficult. The resulting harm extends across households, financial institutions, and the broader economy:

- **Individuals and Families:** Face sudden financial losses, depleted retirement security, prolonged instability, and significant psychological harm.

- **Financial Institutions:** Experience growing operational strain in fraud mitigation, increased legal and reputational risk, and potential customer attrition following major losses.
- **The Broader Economy:** Suffers large-scale wealth extraction as funds are diverted from legitimate markets into transnational criminal enterprises. (House Committee on Homeland Security, 2026)

XI. CONVERGENCE OF FRAUD, MONEY LAUNDERING AND CYBER ACTIVITY

Historically, financial institutions and law enforcement agencies treated fraud, money laundering, and cybercrime as separate operational categories, managing them through distinct compliance teams and specialized investigative units. Today, sophisticated networks operate across all three domains simultaneously, using that convergence to increase speed, scale, and resilience. This shift also requires greater education and cross-training across public- and private-sector investigative functions. (House Committee on Homeland Security, 2026; FinCEN, 2025)

Cyber capabilities are used to steal personal data, commit identity theft, and maintain encrypted communications. That compromised data is then used for various purposes, such as to create synthetic or altered identities that bypass Know Your Customer protocols, open accounts to receive illicit funds, register front companies to perpetuate trade-based money laundering, and obtain public benefits under stolen or fabricated identities.

Chinese organized crime networks use cyber tools to manipulate victims and generate large volumes of liquid illicit revenue. CMLNs then absorb, split, layer, and launder those proceeds alongside cartel drug profits. These schemes include mass SMS phishing campaigns, account-unlock and toll-payment scams, online impersonation fraud, investment scams, and other digitally enabled fraud models that generate funds for the same laundering architecture. (House Committee on Homeland Security, 2026)

This convergence is difficult to detect because cyber, fraud, and laundering signals are dispersed across separate corporate and regulatory systems. The relationship between them is easiest to understand as a three-part operational model:

1. Cyber Tools: These tools harvest personal data, enable identity theft, and support encrypted communications. Their purpose is to make fraud scalable.

2. Fraud Schemes: These operations systematically manipulate victims over extended periods and induce them to route funds voluntarily. Their purpose is to generate liquid capital.

3. Laundering Channels: These channels integrate proceeds through underground banking systems, informal value transfer, and mirroring networks. Their purpose is to validate and shield illicit assets.

The proceeds from fraudulent activity are often co-mingled with the proceeds of other criminal activity, such as marijuana sales, counterfeit pharmaceutical sales, fentanyl trafficking proceeds, and synthetic drug distribution.

XII. CORPORATE STRUCTURES, TRANSPARENCY, AND LEGAL LOOPHOLES

To embed themselves in the global economy, CMLN and cartel laundering alliances rely on complex corporate structures that conceal beneficial ownership. They build webs of shell companies, front businesses, and holding entities across offshore havens and permissive domestic jurisdictions. These companies are often presented as import-export firms, consultants, or logistics providers, enabling trade-based money laundering (TBML) through false invoices, inflated valuations, and manipulated shipping records.

The real owners rarely appear on corporate registries. Instead, they hide behind nominee directors, proxy services, or unwitting money mules. As a result, the challenge is not just collecting ownership records, but analyzing how these entities interact, trade, and move capital across a broader geopolitical network.

XIII. INFORMATION SHARING AND STRUCTURAL COVERAGE GAPS

To counter distributed threat networks, the financial sector relies on information-sharing frameworks such as Section 314(b) of the USA PATRIOT Act. This provision allows participating institutions to exchange information to identify and report activity linked to money laundering or terrorism. While valuable, 314(b) and similar mechanisms are limited by how information is structured, transmitted, and analyzed across institutions. (Financial Crimes Enforcement Network, 2020; Financial Crimes Enforcement Network, 2025)

A major vulnerability is the presence of structural coverage gaps at three levels. First, inter-institutional gaps prevent banks from sharing real-time transaction data unless they meet high internal suspicion thresholds, allowing networks to stay ahead by splitting activity across unrelated institutions. Second, cross-jurisdictional gaps arise when privacy laws, such as GDPR in Europe or data export restrictions in mainland China, block branches of the same institution from sharing investigative intelligence across borders. Third, intra-organizational gaps emerge when retail banking, wealth management, and fraud teams within a single institution fail to integrate their data. CMLNs deliberately route activity through these seams to avoid detection. (FinCEN, 2025)

XIV. SYSTEMIC AND NATIONAL SECURITY IMPLICATIONS

Money laundering, large-scale consumer fraud, and tax evasion are often treated as economic crimes. At their current scale, and in today's geopolitical context, they are also direct threats to

national security. Democratic societies depend on trust in their financial systems, legal institutions, and markets. When transnational criminal organizations and CMLNs exploit those systems, they erode public trust, distort markets, and weaken institutional integrity. (U.S. Department of the Treasury, 2024)

The proceeds from these blended criminal networks are not dormant cash reserves. They are reinvested into legitimate Western economies through residential commercial real estate, logistics infrastructure, and strategic business assets. That accumulation of clean wealth gives illicit networks durable domestic presence, economic leverage, and the capacity to exert corrosive influence within sovereign borders. Countering this threat requires more than isolated enforcement actions. It demands a coordinated, whole-of-government strategy that aligns law enforcement, the Department of the Treasury, the Department of State, and intelligence agencies around a common counter-network mission. (FinCEN, 2025; DOJ, 2024)

XV. THE CORE DETECTION CHALLENGE: SHIFTING FROM ENTITIES TO RELATIONSHIPS

The fundamental hurdle facing global anti-money laundering efforts is not an access problem; it is an aggregation and synthesis problem. The international financial system generates immense quantities of transactional data daily. In my experience, current transaction monitoring systems are exceptionally effective at identifying isolated, anomalous transactions or flagging individual suspicious entities against pre-defined blacklists. However, they face challenges at mapping relational dependencies, detecting highly distributed, coordinated maneuvers, or visualizing hidden network structures.

Consequently, when a laundering network operates by scattering its footprint across hundreds of student accounts, dozens of shell companies, and multiple jurisdictions, traditional compliance frameworks may treat flags as isolated, minor incidents. The systemic risk is consistently underestimated, and responses remain heavily reactive, focusing on closing individual accounts rather than systematically dismantling the transnational financial pipeline.

XVI. PROACTIVE AND SYSTEMIC NETWORK DISRUPTION

To counter the growing alliance between CMLNs and cartels, the compliance system must shift to network-level analysis and systematic detection. That means moving beyond rules-based transaction alerts and adopting a risk-based approach that can connect fragmented data across separate systems. With advanced graph analysis, machine learning, and secure cross-institutional data sharing, investigators can identify the shared patterns and connection points that reveal coordinated criminal activity.

These scalable methods would move defensive systems from a reactive, account-by-account posture to a proactive strategy focused on structural disruption. Instead of catching low-level

money mules after the fraud or drug transaction has occurred, network-level intelligence can identify the clearinghouses and brokers directing the flows earlier, cutting off the financial lifelines of cartels and transnational fraud networks.

XVII. CONCLUSION

CMLNs are not peripheral actors in the illicit economy. They are central financial enablers linking cartel drug trafficking, Chinese capital flight, fraud, cyber-enabled crime, contraband markets, human exploitation, and concealed corporate structures into a single adaptive system. Their resilience stems not only from speed, liquidity, and scale, but from their ability to exploit institutional fragmentation across banks, jurisdictions, technologies, and regulatory regimes.

The central lesson is clear: the United States cannot counter networked illicit finance with siloed tools or reactive enforcement alone. Effective disruption will require sustained, proactive network-level intelligence, secure information sharing, education campaigns, and coordinated public-private action across financial institutions, law enforcement, intelligence, and national security agencies. If we continue to evaluate these activities as separate compliance, fraud, cyber, or narcotics problems, the broader system will remain durable and adaptive. But if we focus on the relationships, brokers, and structural seams that sustain it, we can move from reacting to symptoms toward disrupting the architecture itself and better protecting the integrity of the U.S. financial system.

XVIII. PRIORITY ACTIONS TO COUNTER CMLNs

- Establish a sustained whole-of-government and public-private counter-network strategy that aligns financial institutions, law enforcement, Treasury, State, intelligence, national security agencies, and policymakers around a common mission.
- Adopt network-level AML methods that identify relationships, shared patterns, and coordination across accounts, entities, and jurisdictions rather than relying primarily on isolated transaction alerts.
- Expand secure information sharing among financial institutions, regulators, law enforcement, and intelligence agencies to reduce the blind spots created by fragmented systems and legal boundaries.
- Invest in modern analytical capabilities, including graph analysis, machine learning, and entity resolution, to detect distributed laundering activity earlier and identify the brokers and clearing structures behind it.
- Invest in education and cross-training for public- and private-sector investigators and analysts so they can better understand, recognize, and respond to the convergence of money laundering, fraud, and cybercrime, including the role of organized crime, CMLNs, and network intelligence.

REFERENCES:

Financial Crimes Enforcement Network. (2025). *Financial trend analysis: Chinese money laundering networks, 2020–2024 threat pattern and trend information*. U.S. Department of the Treasury.

Department of Justice. (2024). *Federal indictment alleges alliance between Sinaloa Cartel and money launderers linked to Chinese underground banking*. U.S. Attorney's Office, Central District of California.

U.S.-China Economic and Security Review Commission. (2021). *Illicit fentanyl from China: An evolving global operation*. Briefing Report.

House Committee on Homeland Security. (2026). *Online scams, crypto fraud, and digital extortion by transnational criminal organizations*. Hearing before the Subcommittee on Cyber and Innovation, U.S. House of Representatives.

U.S. Department of the Treasury. (2024). *2024 National Money Laundering Risk Assessment*. U.S. Department of the Treasury.

Financial Crimes Enforcement Network. (2025). *Advisory on the Use of Chinese Money Laundering Networks by Mexico-Based Transnational Criminal Organizations to Launder Illicit Proceeds* (FIN-2025-A003). U.S. Department of the Treasury.

Drug Enforcement Administration. (2025). *2025 National Drug Threat Assessment*. U.S. Department of Justice.

Financial Crimes Enforcement Network. (2020). *Section 314(b) Fact Sheet*. U.S. Department of the Treasury.

Federal Bureau of Investigation Internet Crime Complaint Center. (2025). *2025 Internet Crime Report*. Federal Bureau of Investigation, U.S. Department of Justice.