Ballard Spahr LLP

By Kelly A. Lenahan-Pfahlert and Terence M. Grugan

The Emerging Threat: Chinese Money Laundering Networks and Mexican Cartels

On August 28, 2025, the U.S. Department of the Treasury's Financial Crimes Enforcement Network (FinCEN) released an advisory (FIN-2025-A003[1]) alongside a comprehensive Financial Trend Analysis (FTA[2]). Together, these documents highlight an increasingly sophisticated illicit finance risk: the growing integration of Chinese Money Laundering Networks (CMLNs) into the Mexico-based transnational criminal organizations commonly referred to as "cartels." As these disparate networks find common ground in their financial needs and regulatory pressures, financial institutions worldwide face new compliance challenges that demand not just awareness but robust action.

Understanding the CMLN-Cartel Partnership

FinCEN's analysis highlights how contrasting regulatory environments have driven collaboration between CMLNs and Mexican cartels. Mexican-based drug trafficking groups generate enormous quantities of U.S. dollars in proceeds from narcotics sales, but struggle to deposit these funds locally due to restrictive currency controls. Meanwhile, many Chinese nationals seek to circumvent the PRC's stringent capital controls, which limit conversion of foreign currency to the equivalent of $50,000 (U.S.) per person annually.

The Mexican cartels need a process for moving cash beyond the reach of authorities without drawing scrutiny; Chinese nationals want unfettered access to foreign funds. This mutual interest forms what FinCEN describes as a "mutualistic relationship." CMLNs have taken on the role of "matchmakers" in this relationship. They purchase dollars in bulk at discounted rates from cartel contacts in the U.S. Those dollars are then sold at a premium to Chinese clients seeking overseas liquidity, allowing narcotics proceeds to intermingle with legitimate currency migration flows.

These CMLNs, which currently operate both within the United States and abroad, are able to move vast sums across national borders while minimizing risk through speed and sophistication at scale. Their methods have evolved beyond basic smuggling and informal remittances to leverage advanced tradecraft designed specifically for anonymity and regulatory evasion.

How CMLNs Move Illicit Funds: Core Methodologies

In its analysis, FinCEN identifies three primary methodologies central to contemporary CMLN operations supporting cartel money laundering:

1) *Mirror Transactions: Informal Value Transfer Without Borders*

At the heart of many schemes is the "mirror transaction," which operates similarly to longstanding informal value transfer systems. In a mirror transaction, when a network operator receives illicit U.S.-sourced cash

---

[1] https://www.fincen.gov/system/files/2025-08/FinCEN-Advisory-CMLN-508.pdf

[2] https://www.fincen.gov/system/files/2025-08/4000-10-INV-144549-S3F6L-FTA-CMLN-508.pdf

within the United States, often from cartel associates, an affiliated participant in another country delivers an equivalent amount in local currency abroad. As a hypothetical example, after collecting cartel dollars in Houston, the Houston-based operator may instruct its counterparts in Mexico City or Shanghai to pay pesos or yuan directly to designated recipients. These transactions are conducted entirely outside of formal banking channels, and do not require the physical/digital movement of funds across borders – a notable advantage given increased regulatory scrutiny on cross-border transfers. More recently, mirror transactions have begun leveraging convertible virtual currencies such as Bitcoin or Ethereum for rapid settlement outside the financial regulatory infrastructure.

2) *Trade-Based Money Laundering (TBML): Illicit Finance Via Global Commerce*

Trade-based money laundering is another defining tactic used by CMLNs. Laundered cash originating in U.S. markets is used to purchase bulk quantities of high-value goods, including electronics (*e.g.*, smartphones and tablets) as well as luxury consumer goods (*e.g.*, designer handbags). These goods are then exported via shell companies or complicit import-export firms, frequently located in global trading hubs, such as Hong Kong, where customs oversight may be less rigorous. Once these goods reach foreign markets, they are either sold for local currency through intermediaries with access to overseas retail networks or held as stores of wealth.

The process often involves complex layering to obscure both the original source of funds and their final beneficiaries. This is achieved by sending shipments through several different countries, taking advantage of jurisdictions where export-import records are poorly maintained or lack transparency. By moving goods across multiple regions with limited oversight and documentation, criminal organizations make it much more difficult for authorities to trace transactions and uncover the true origins and destinations of illicit funds.

3) *Exploiting Money Mules: Human Nodes in a Digital Network*

The exploitation of “money mules” introduces yet another layer of sophistication to these operations. Large-scale campaigns actively target individuals who may be vulnerable due to temporary visa status restrictions, including international students, as well as retirees and homemakers who possess modest means but maintain clean banking credentials. Anyone willing to participate is recruited, even unwittingly, in exchange for relatively minor compensation. Many money mules open new bank accounts using counterfeit passports provided by network facilitators. Some participate knowingly due to social pressure or family ties, while others fall victim to deceptive job offers promising easy income.

Once operational, accounts receive deposits vastly disproportionate to the account holders’ stated income sources or purported occupation status. Funds are typically wired onward post-deposit rapidly, or else converted into cashier’s checks often used to purchase real estate within high-dollar markets.

Extensive misuse of retail credit card networks compounds layering opportunities: laundered proceeds fund serial shopping sprees exceeding customer profiles. Outstanding balances are settled using new infusions from other network-controlled accounts. Rewards points are converted into further offshore payments, all facilitated via digital platforms popular among PRC nationals.

Red Flags and Compliance Vulnerabilities

FinCEN’s analysis includes critical red flag indicators based upon actual suspicious activity report (SAR) filings observed across multiple years:

Common Indicators Include:

- Accounts opened by individuals presenting Chinese passports and student or visitor visas, followed immediately by unusually large transactions inconsistent with that demographic profile;

- Frequent large-dollar cash deposits, closely followed by wire transfers or cashier check purchases;

- Multiple wire transfers received from persons/entities abroad (absent substantiated relationships);

- Reluctance or refusal during onboarding or enhanced due diligence interviews to disclose the source and/or purpose behind incoming funds;

- Shell companies structured around electronics/export trades reporting income that is out of line with their business size, type, and geography; and

- Businesses repeatedly credited via online marketplaces, yet rarely engaging suppliers or purchasing needed inventory

Notably, legacy rules-based monitoring tools often fail to detect suspicious activity unless multiple red flags appear together over time. This highlights the need for financial institutions to incorporate contextual behavioral analysis alongside existing anti-money laundering (AML) programs for more effective detection.

Five Years of Data Trends – SAR Insights From 2020-2024

The Financial Trend Analysis supporting FIN-2025-A003 studied more than 137,000 SARs filed under Bank Secrecy Act (BSA) requirements between January 2020 and December 2024, with approximately $312 billion flagged suspicious activity potentially linked to CMLN operations across a diverse spectrum of banks and money services businesses.

Key Findings:

Banks as Frontline Gateways

Approximately 85% of relevant SARs were filed by depository institutions, including both large national banks and regional branches located in metropolitan areas with significant immigrant populations. In these locations, bulk cash deposits often occur at amounts below standard detection thresholds. Money services businesses accounted for about 9% of filings, which highlights their increased vulnerability, especially among smaller operators that typically lack the advanced AML controls found in larger banking organizations.

Prevalence of TBML Schemes

Trade-based money laundering (TBML), through the physical movement of goods through the trade system, remains a particular concern in the dataset. More than $9 billion in suspicious activity was specifically linked to TBML schemes, which often featured unusual sources of funding and export/import transactions routed through East Asia, Mexico, and Middle Eastern corridors. In many cases, these transactions could only be loosely connected to beneficial owners who reside offshore.

Retail Typologies – Daigou Buyers and Credit Card Laundering

Retail and luxury goods purchases, often linked to *daigou* buyer cycles, remain a prominent money laundering typology, even though there were fewer than 20 explicit references in SAR filings. *Daigou* refers to individuals or groups who purchase goods overseas on behalf of clients in China, frequently using informal networks to bypass import restrictions and taxes. Related patterns involving credit card abuse represented over $19 billion in flagged suspicious activity. Many clients participated in repeated high-volume spending sprees by accessing pools of laundered U.S. dollars that were moved outside official Chinese channels through underground broker networks connected to cartel operations.

Crossover With Human Trafficking and Fraud Sectors

More than 1,600 SAR filings indicated possible connections to human trafficking or smuggling operations, with over $4 billion in suspicious transactions transferred directly to business entities associated with labor exploitation sectors. These included massage parlors, spas, and restaurants that were ultimately owned through proxy structures by individuals holding dual residency or citizenship in both China and the United States.

Additionally, adult daycare and health care fraud centered around facilities in the New York area contributed hundreds of additional reports, with nearly $750 million in suspected losses or exposure.

Real Estate Remains Enduring Vehicle for Integration

More than $53 billion in suspicious funds were funneled through property acquisitions. These transactions were carried out either directly, using accounts, wire transfers, or check payments held by money mules and often described as coming from "relatives abroad," or indirectly through shell companies that were created for a single transaction and then abandoned after closing.

According to FinCEN, luxury neighborhoods in Los Angeles, New York, and South Florida remain popular destinations for investors seeking safe havens outside of mainland China's capital restrictions. In these markets, front companies and money mules are frequently used to facilitate real estate deals and conceal the true source of wealth or connections to criminal organizations.

Students as Mules and Layering Agents

Approximately 14 percent of SARs analyzed, representing over $13 billion, involved account holders listed as students, FinCEN reported. These cases frequently showed patterns of repeated account openings, unusually high spending activity, and multiple banking relationships that could not be explained by the available background information.

FinCEN warns that banks, money services businesses, and trade firms should be aware that risks are not limited to traditional criminal profiles. Increasingly, emerging threats involve individuals who appear legitimate, such as students, being used for systematic layering and placement activities that often go undetected by standard screening methods.

Responding to Escalating Complexity – Regulatory Actions and Industry Strategies

The legal and regulatory landscape is rapidly evolving, as authorities intensify their focus on sophisticated money laundering threats. FinCEN's latest guidance reflects these changes, including alignment with Executive Order 14157[3], which designates major transnational criminal organizations (TCOs) and cartel entities as Foreign Terrorist Organizations. This development has significant implications: the Department of Justice and the FBI now view even indirect facilitation, such as unintentional involvement by correspondent banks or remittance partners, as potential material support violations. Such cases are no longer regarded merely as technical breaches of the BSA, and instead may prompt heightened enforcement scrutiny and corrective action. For example, in June 2025, FinCEN exercised new authority to bar certain Mexican financial institutions identified as primary money laundering concerns from any interaction with the U.S. financial system. As a result, all covered entities must rigorously screen both upstream and downstream partners to monitor exposure risks throughout their entire supply chain.

[3] https://www.whitehouse.gov/presidential-actions/2025/01/designating-cartels-and-other-organizations-as-foreign-terrorist-organizations-and-specially-designated-global-terrorists/

For compliance professionals responsible for managing daily operations in this complex environment, several strategic responses are essential:

First, it is critical to continually review transaction monitoring systems and risk models. Institutions should incorporate current red flag indicators from recent advisories and trend analyses, while emphasizing dynamic behavioral surveillance that can reveal suspicious patterns when multiple risk factors overlap over time – especially those that static models may miss.

Second, enhancement of customer due diligence is vital. Firms need to prioritize thorough verification of both beneficial ownership details and sources of funds for new clients or those operating in higher-risk sectors or geographic regions. Documentation requirements should be reexamined regularly, and that documentation should be cross-referenced with external registries and public records to help ensure that reported relationships and income streams are valid.

Third, internal reporting lines and escalation protocols must be robust enough to flag any circumstantial links with sanctioned entities or organizations such as TCOs or CMLNs, even if direct evidence is lacking initially. Staff should feel empowered to raise concerns early so potential illicit activity can be addressed swiftly by cross-functional teams dedicated to compliance reviews.

Fourth, companies need rigorous controls over third-party exposures overseas. This includes adoption of contract language that grants audit rights and that requires documented proof of effective AML programs from all vendors, logistics providers, and supply chain partners operating in affected jurisdictions. Regular audits help validate program strength and protect against vulnerabilities often exploited by professional money broker networks.

Finally, ongoing staff education on emerging threat typologies, including regular updates on sanctions lists, is crucial for maintaining a vigilant workforce across all operational units – not just those directly involved in financial operations, but also those in client-facing roles within day-to-day logistics management.

By adopting these proactive measures, the industry can strengthen its ability to detect threats quickly while responding adaptively rather than reactively within an increasingly complex regulatory context.

Looking Forward – Building Resilience Against Modern Money Laundering Networks

As demonstrated in both the FIN-2025-A003 advisory and the FTA, professional global money laundering groups collaborating with sophisticated Chinese brokers are likely to continue to evolve in response to new challenges and changing enforcement priorities. Unless private sector vigilance increases accordingly, these actors will adapt their methods to exploit emerging vulnerabilities.

Institutions can no longer rely on box-ticking exercises alone: they must evolve toward dynamic risk assessment rooted in contemporary geopolitical context and new technology-enabled evasion tactics embraced by adversarial actors exploiting gaps in fragmented oversight regimes worldwide.

Detection techniques that incorporate international best practices and a nuanced understanding of specific cross-border risks associated with modern money laundering methods, alongside consistent communication and intelligence sharing among financial institutions, law enforcement, and regulatory agencies during early investigations or risk assessments, enable the industry to support the reliable functioning of global payment systems. These measures help mitigate exposure to illicit activities and uphold the integrity of financial networks worldwide.

As the use of underground digital assets and disruptive commerce platforms continues to grow rapidly, it is essential for U.S. and global market participants to maintain a multilayered defense strategy. Building resilience, agility, and a capacity for continuous learning should be central goals in future-proofing compliance frameworks and protecting the integrity of core financial transactions.

Conclusion

The evolving partnership between Chinese Money Laundering Networks and Mexican cartels represents a complex and rapidly shifting threat landscape for financial institutions worldwide. The data and insights from FinCEN's latest advisory and Financial Trend Analysis reveal that these networks are not only expanding their reach through increasingly sophisticated methods, but also adapting quickly to new regulatory measures and market conditions. To counter this challenge effectively, financial institutions must go beyond traditional compliance approaches by adopting advanced detection strategies, while continuing to strengthen due diligence practices and promote ongoing staff education on emerging risks. Collaboration across the industry, alongside law enforcement and regulatory agencies, will be vital in sharing intelligence and maintaining the resilience of global payment systems. By remaining agile, proactive, and informed in their risk management efforts, organizations can help safeguard both their own operations and the broader integrity of international finance against illicit actors who continue to innovate across borders.

****

Kelly A. Lenahan-Pfahlert is an accomplished litigator whose practice centers on white collar criminal defense, internal investigations, and anti-money laundering compliance. She excels in developing case strategies, legal research and analysis, depositions, complex discovery management, and eDiscovery. Kelly's AML expertise includes risk assessment and mitigation, identifying money laundering risks, developing effective controls, drafting internal policies and procedures, and ensuring ongoing regulatory compliance.

Terence M. Grugan is an experienced litigator, investigator and trial attorney. Terence represents clients in criminal and administrative investigations and trials conducted by the Department of Justice, Department of the Treasury, Securities Exchange Commission and states Attorneys General. As the Co-Leader of Ballard's Anti-Money Laundering practice team, Terence counsels financial institutions on Anti-Money Laundering compliance and represents financial institutions in litigation and investigations arising under the Bank Secrecy Act and advises financial institutions on emerging trends including cryptocurrency regulation. Terence also maintains an active corporate litigation practice, representing individual and institutional clients in court actions and arbitrations involving shareholder and corporate governance disputes.