FinCEN ADVISORY

FIN-2025-A003 **August 28, 2025**

FinCEN Advisory on the Use of Chinese Money Laundering Networks by Mexico-Based Transnational Criminal Organizations to Launder Illicit Proceeds

Suspicious Activity Report (SAR) Filing Request:
FinCEN requests that financial institutions reference this Advisory in SAR field 2 (Filing Institution Note to FinCEN) and the narrative by including the key term "**CMLN-2025-A003**" and select, as applicable, SAR field 38(n) (Suspicious Use of Informal Value Transfer System); SAR field 38(s) (Unlicensed or Unregistered MSB); SAR field 36(l) (Trade Based Money Laundering/Black Market Peso Exchange), and any other applicable check box.

The U.S. Department of the Treasury's (Treasury) Financial Crimes Enforcement Network (FinCEN) is issuing this Advisory to urge financial institutions[1] to be vigilant in identifying and reporting suspicious transactions potentially related to the use of Chinese money laundering networks (CMLNs)[2] by the Jalisco New Generation Cartel (CJNG), the Sinaloa Cartel, the Gulf Cartel, and other Mexico-based transnational criminal organizations (TCOs)—frequently known collectively as the "Cartels"—to launder illicit proceeds. CMLNs are considered professional money launderers (PMLs)[3] and play a vital role in laundering the Cartels' drug proceeds in the United States. This is, in part, due to the speed and effectiveness of CMLNs' money laundering operations, as well as their willingness to absorb financial losses and assume risks for the Cartels and other clients.[4] Further, CMLNs operate around the world and may coordinate with other international PMLs, such as shadow banking networks and Colombian peso brokers.[5] According to Treasury's 2024 National Money Laundering Risk Assessment, CMLNs are one of the most significant money laundering threat actors facing the U.S. financial system.[6]

1. *See* 31 U.S.C. § 5312(a)(2); 31 CFR § 1010.100(t).
2. CMLNs may also be referred to as Chinese money laundering organizations (CMLOs). Treasury and some law enforcement agencies have moved to characterizing them as "networks" due to their horizontal structure and decentralized nature. *See, e.g.*, U.S. Drug Enforcement Administration (DEA) "2025 National Drug Threat Assessment" ("2025 NDTA") (May 2025), at p. 6.
3. Professional money laundering encompasses individuals, organizations, and networks involved in third-party money laundering for a fee or commission. *See* Treasury, "2024 National Money Laundering Risk Assessment" ("2024 NMLRA") (Feb. 2024), at p. 26.
4. *Id*. at p. 29.
5. *Id*. For more information on Colombian peso brokers, *see* U.S. Department of Justice (DOJ), "Colombian Money Broker Sentenced to Nearly a Decade in Prison for Role in International Money Laundering Conspiracy" (June 20, 2025).
6. *See* 2024 NMLRA, *supra* note 3, at pp. 29-30.

This Advisory supports FinCEN's work to bring awareness to, and counter, TCO-related revenue streams[7] and is consistent with two of the eight national anti-money laundering and countering the financing of terrorism (AML/CFT) priorities (*i.e.*, drug trafficking organization (DTO) activity and TCO activity).[8] Further, on January 20, 2025, the President issued Executive Order (E.O.) 14157 designating certain international cartels and other TCOs as Foreign Terrorist Organizations (FTOs) and Specially Designated Global Terrorists (SDGTs).[9] The Cartels functionally control nearly all illegal traffic across the southwest border of the United States, and their activities threaten the safety of the American people, the security of the United States, and the stability of the international order in the Western Hemisphere. Treasury is committed to countering the activity of the Cartels and related actors.

This Advisory: (i) provides an overview of CMLNs and their connection to the Cartels, (ii) discusses financial typologies associated with CMLNs laundering the Cartels' illicit proceeds, (iii) highlights red flag indicators, and (iv) reminds financial institutions of their reporting requirements under the Bank Secrecy Act (BSA). The information contained in this Advisory is derived from FinCEN's analysis of open-source reporting, BSA reporting, and information from law enforcement partners.

Overview of Chinese Money Laundering Networks

CMLNs operate in a compartmentalized fashion, leveraging relationships built on trust rather than working through a hierarchical structure to launder money. CMLNs often launder illicit proceeds for a number of TCOs and may engage in some form of additional criminal activity as part of their money laundering operations, such as the provision of fake identification documents to individuals opening bank accounts on their behalf.[10] CMLNs typically comprise both current and former U.S.- and foreign-based Chinese passport holders (*i.e.*, Chinese nationals). CMLNs often recruit members of Chinese or other diaspora populations to participate in their money laundering operations to act as money mules,[11] money brokers, and cash couriers.[12] In the United States, CMLNs appear to have increasingly recruited Chinese students studying at U.S. universities, and

7. *See* FinCEN, FIN-2025-A002, "FinCEN Alert on Oil Smuggling Schemes on the U.S. Southwest Border Associated with Mexico-Based Cartels" (May 1, 2025); FinCEN, FIN-2025-A001, "FinCEN Alert on Bulk Cash Smuggling and Repatriation by Mexico-Based Transnational Criminal Organizations" (Mar. 31, 2025); FinCEN, FIN-2024-A002, "Supplemental Advisory on the Procurement of Precursor Chemicals and Manufacturing Equipment Used for the Synthesis of Illicit Fentanyl and Other Synthetic Opioids" (June 20, 2024); FinCEN, OFAC, and FBI, FIN-2024-NTC2, "FinCEN, OFAC, and FBI Joint Notice on Timeshare Fraud Associated with Mexico-Based Transnational Criminal Organizations" (July 16, 2024).
8. *See* FinCEN, "Anti-Money Laundering and Countering the Financing of Terrorism National Priorities" (June 30, 2021).
9. *See* White House, "Designating Cartels and Other Organizations as Foreign Terrorist Organizations and Specially Designated Global Terrorists" (Jan. 20, 2025); U.S. Department of State, "Designation of International Cartels" (Feb. 20, 2025).
10. *Id.*; *see also* U.S. Immigration and Customs Enforcement, Cornerstone Report Issue #48, "Chinese Money Laundering Organizations (CMLOs) - Use of Counterfeit Chinese Passports" ("Counterfeit Chinese Passports") (Jan. 2, 2024).
11. Money mules are people who are used, wittingly or unwittingly, to transfer value, either by laundering stolen money or physically transporting goods or other merchandise. *See* FATF, "Professional Money Laundering" (July 2018), at p. 22. According to law enforcement, criminal organizations often target students as potential money mules. *See generally* Federal Bureau of Investigation (FBI), "Money Mules" (as of Aug. 27, 2025).
12. *See* DOJ, "Final Three Members Charged in Prolific Chinese Money Laundering Scheme Plead Guilty to Laundering Tens of Millions in Drug Proceeds" (July 7, 2025).

some of these students may have continued to participate in CMLN operations after graduating.[13] CMLNs may target individuals on student visas in particular, since such individuals are often restricted from obtaining certain types of lawful employment in the United States.[14] In some cases, individuals recruited by CMLNs may not understand that their actions are illegal, but rather were lured into participating in the schemes under the incentive of having a source of income and assisting other Chinese citizens or nationals in accessing U.S. dollars (USD).

A primary goal of CMLNs is to obtain large quantities of USD and other currencies to meet the demand for these currencies by Chinese citizens seeking to evade the People's Republic of China's (PRC's) currency controls.[15] This demand for USD has led CMLNs to partner with illicit actors, such as the Cartels, who have access to large sums of USD that they need to launder.[16] CMLNs assume much of the risk of transporting and laundering large volumes of cash inside the United States, while providing near-instant transfers of value back to their clients by engaging in informal value transfer systems (IVTS)[17] or trade-based money laundering (TBML) schemes.[18] In the United States, CMLNs functionally operate as unregistered money services businesses (MSBs)[19] and serve as money brokers in the global Chinese underground banking system (CUBS),[20] which provides Chinese citizens the ability to move funds out of China despite the PRC's currency control laws. Although CMLNs generate some profit from their money laundering activities (*e.g.*, payment from the Cartels), CMLNs are typically able to offer lower rates than other PMLs because most CMLN revenue comes from selling the illicit cash to Chinese citizens at a high rate.[21]

In addition to laundering drug proceeds on behalf of the Cartels, CMLNs are associated with the laundering of proceeds from other types of illicit activity on behalf of clients, such as marijuana

13. *See* FinCEN, Financial Trend Analysis, "Chinese Money Laundering Networks: 2020 – 2024 Threat Pattern & Trend Information" ("FinCEN CMLN FTA") (Aug. 28, 2025), at pp. 19-20.
14. *See* U.S. Citizenship and Immigration Services, "Students and Employment" (last updated April 8, 2025).
15. China instituted strict capital control measures in 2016, when it recorded a surge in capital flight. China's foreign exchange rules cap the maximum amount of renminbi (RMB) that Chinese citizens are allowed to convert into other currencies at approximately $50,000 each year and restricts Chinese citizens from directly transferring RMB abroad without prior approval from the Chinese State Administration of Foreign Exchange. Consequently, many Chinese citizens attempt to circumvent these currency control laws for a variety of reasons. *See* U.S. Department of State, "2024 Investment Climate Statements: China" ("China Investment Climate Statement") (July 2024).
16. *See* Treasury, "Treasury Sanctions Mexico- and China-Based Money Launderers Linked to the Sinaloa Cartel" (July 1, 2024).
17. An IVTS is "any system, mechanism, or network of people that receives money for the purpose of making the funds or an equivalent value payable to a third party in another geographic location, whether or not in the same form." The informal nature of the system means that the movement of value occurs outside of the formal financial system. An IVTS is not inherently illicit, and can be used for legitimate (*e.g.*, sending remittances) or illegitimate (*e.g.*, money laundering) purposes. *See* FinCEN, Issue 33, "Informal Value Transfer Systems" (March 2003), at p. 1; *see also* 2025 NDTA, *supra* note 2, at p. 64; DEA, "2024 National Drug Threat Assessment" ("2024 NDTA") (May 9, 2024), at p. 47.
18. TBML is the process of disguising the proceeds of crime and moving value through the use of trade transactions in an attempt to legitimize their illicit origin. *See* Financial Action Task Force (FATF), "Trade-Based Money Laundering" (June 23, 2006), at p. i; *see also* 2024 NDTA, *supra* note 17, at pp. 46-47.
19. As an MSB, any non-exempt person engaged in money transmission must register with FinCEN within 180 days of starting to engage in money transmission. *See* 31 CFR § 1022.380.
20. The CUBS is a type of IVTS. *See* FinCEN CMLN FTA, *supra* note 13, at p. 8; *see also* 2024 NDTA, *supra* note 17, at p. 47.
21. *See* 2024 NMLRA, *supra* note 3, at pp. 29-30.

trafficking, human trafficking, and fraud.[22] CMLNs may also be involved in certain other criminal activities in addition to money laundering, such as healthcare fraud and illicit gaming.[23] Engaging with a variety of illicit actors grants CMLNs access to cash flows from numerous sources and locations. CMLNs also coordinate and network with CMLNs or PMLs in other countries through IVTS and TBML to launder illicit proceeds, which obviates the need to physically transport cash or execute cross-border wire transfers.[24]

The complex networks and operations of CMLNs, as described in further detail below, threaten the U.S. financial system and facilitate the laundering of illicit proceeds into the United States and internationally.

Drivers of Chinese and Cartel Money Laundering

The rise in the prominence of CMLNs, including their business relationships with the Cartels and other TCOs, has been driven, in part, by laws passed by the Government of Mexico (GOM) and the PRC, that restrict financial flows. Instituted in 2010 and revised in 2014, the GOM's currency restrictions prevent large amounts of USD from being deposited into Mexican financial institutions.[25] These restrictions have hindered the Cartels' ability to launder illicit USD proceeds through the formal Mexican financial system, leading them to seek out PMLs that operate in the United States. The PRC's currency control laws[26] restrict the amount of Chinese renminbi (RMB) that Chinese citizens are allowed to convert into other currencies each year and prevent direct transfers of RMB abroad without prior approval. Likewise, these laws have increased Chinese citizens' demand for access to USD in a way that circumvents the PRC's control over the funds. This policy has driven Chinese citizens to increasingly rely on the services of CMLNs to provide access to USD through informal transactions. Ultimately, Chinese citizens' demand for large quantities of USD and the Cartels' need to launder their illicit USD proceeds has resulted in a mutualistic relationship wherein the Cartels sell off their illicitly obtained USD to CMLNs who, in turn, sell the USD to Chinese citizens seeking to evade the PRC's currency control laws.[27]

22. *See* FinCEN CMLN FTA, *supra* note 13, at p. 4; *see also* DOJ, "Seventeen Individuals Indicted Alleging a Sophisticated Nationwide Money Laundering Scheme Originating with Violent Crime in Baltimore City" (Oct. 10, 2024); Superseding Indictment, Dkt. No. 112, *United States v. Tao*, 1:24-cr-289 (D. Md. Oct. 9, 2024); DOJ, "Seven Chinese Nationals Charged for Alleged Roles in Multi-Million-Dollar Money Laundering, Alien Smuggling and Drug Trafficking Enterprise" (June 8, 2025); Indictment, Dkt. No. 1, *United States v. Chen*, 1:25-cr-10284 (D. Mass. July 2, 2025). Proceedings in these matters remain ongoing.
23. *See* CMLN FTA, *supra* note 13, at pp. 15-16.
24. *See* U.S. Department of the Treasury Under Secretary for Terrorism and Financial Intelligence Brian E. Nelson, "Written Testimony for Senate Caucus on International Narcotics Control Hearing Entitled 'Chinese Money Laundering Organizations: Cleaning Cartel Cash'" (Apr. 30, 2024), at p. 1.
25. On June 15, 2010, to counter cartel operations, the Mexican finance ministry, Secretaría de Hacienda y Crédito Público de México (SHCP), announced new AML regulations that restrict the amounts of physical cash (banknotes and coins) denominated in USD that Mexican banks may receive. Generally, individuals in Mexico are limited to depositing $4,000 per month and businesses in border or tourist areas are limited to $14,000 per month; however, certain Mexico-based businesses may be granted exemptions to these depository limits. *See* Secretaría de Hacienda y Crédito Público and Comisión Nacional Bancaria y de Valores, "Overview of the Mexican Financial System and its AML/CFT regulation and supervision" at pp. 52-56.
26. *See* China Investment Climate Statement, *supra* note 15.
27. *See* DEA Chief of Operations William F. Kimbell, "Written Testimony for Senate Caucus on International Narcotics Control Hearing Entitled 'Chinese Money Laundering Organizations: Cleaning Cartel Cash'" (Apr. 30, 2024), at p. 4.

Financial Typologies Associated with CMLNs Laundering Illicit Cartel Proceeds

CMLNs' Use of Mirror Transactions

To launder funds, CMLNs transfer value globally and sometimes simultaneously using a form of IVTS. For example, once a U.S.-based CMLN receives USD from a Cartel for laundering, it coordinates with Mexico-based CMLN counterparts who conduct a reciprocal or "mirror transaction,"[28] in which an equivalent amount of pesos is transferred to the Cartels' Mexico-based accounts, minus a nominal fee. Through this informal value transfer, CMLNs "purchase" the value of the Cartels' illicit USD proceeds in pesos. This mirror transaction occurs nearly instantly and avoids many of the risks involved with cross-border bulk cash smuggling or with depositing large sums of USD in Mexico-based financial institutions and thereby circumvents Mexico's USD deposit restrictions. CMLNs may also use convertible virtual currency (CVC) as an alternative means to conduct mirror transactions with the Cartels.[29] Similar to other mirror transactions, use of CVC avoids the risks associated with physical transportation of cash or depositing bulk USD.

The U.S.-based CMLNs then sell the USD purchased from the Cartels, by advertising it on social media or leveraging personal networks, to Chinese citizens or businesses seeking to evade the PRC's currency control laws.[30] Once identified, the buyer is connected by the U.S.-based CMLN to a China-based operator, who instructs the buyer to transfer an equivalent amount of RMB, plus a significant fee, from their bank account in China to an account controlled by the China-based operator.[31] This RMB transfer internal to China avoids the PRC's currency control laws and effectively "purchases" the control of the USD from the CMLN. Once the transfer is made in China, the U.S.-based CMLN makes the purchased USD available to the Chinese buyers in the United States, typically by laundering the cash through the U.S. financial system.

Use of Money Mules

As part of the laundering process, CMLNs may use money mules to deposit the illicit USD into accounts they are directed to open at U.S. depository institutions, or at accounts held by U.S.-based Chinese nationals or businesses.[32] In situations where the money mules are opening accounts,

28. The term "mirror transactions" or "mirror transfer" is used by U.S. law enforcement to describe a money laundering typology involving foreign currency exchange. The process typically happens within Chinese underground banking and black market peso exchange schemes and usually involves a money broker or an accountant who conducts two equal, but separate, transactions involving at least two parties who often are unaware of each other. In this scheme, the broker or accountant makes payments to each party using the other parties' currency, "mirroring" or balancing the transactions. *See* 2024 NMLRA, *supra* note 3, at pp. 29-30.
29. *See* 2024 NDTA, *supra* note 17, at p. 47.
30. *See* 2024 NMLRA, *supra* note 3, at pp. 29-30.
31. The China-based CMLN operator will typically sell the RMB obtained from this transaction to Mexican or Chinese importers in Mexico with business in China through a mirror transfer via the Mexico-based CMLN operator to obtain more pesos. This cycle replenishes the Mexico-based CMLN operator's supply of pesos for future transactions. *See* 2024 NMLRA, *supra* note 3, at p. 30.
32. *See* FinCEN CMLN FTA, *supra* note 13, at pp. 19-20; *see also* Wall Street Journal, "Bags of Cash From Drug Cartels Flood Teller Windows at U.S. Banks" ("Bags of Cash") (May 14, 2025).

these money mules may report their occupation during the account onboarding process as "student," "housewife," "retired," "laborer," or other occupations that typically do not engage in large volumes of transactions. CMLNs may also provide money mules with counterfeit Chinese passports to facilitate account opening and engage in other illicit financial behavior.[33] CMLNs may also recruit financial institution employees to act as complicit insiders or infiltrate and place CMLN members within a financial institution to assist in CMLN operations.[34]

CMLN money mules may also engage in "smurfing" operations[35] across multiple depository institution branches to deposit illicit funds into money mule accounts, or into accounts held by U.S.-based Chinese nationals and businesses. CMLN money mules have also been observed depositing large sums of cash during a visit, irrespective of Currency Transaction Reporting requirements.[36] The money mules may also purchase cashier's checks from depository institutions with U.S.-based Chinese nationals and businesses listed as the payee directly. Alternatively, CMLNs may purchase cashier's checks listing the payee as a shell company the CMLNs beneficially own or listing the payee as a U.S.-based company or individual in the real estate industry. CMLNs may use money mules or shell companies to purchase real estate, which may serve as an investment for the CMLN or a wealthy China-based client of the CMLN.[37] They may also deposit the illicit funds into existing money mule accounts (*i.e.*, personal or shell company accounts) and then use wire, automated clearing house (ACH), or peer-to-peer (P2P) transfers to send the money to separate accounts held by U.S.-based Chinese nationals and businesses.[38] These actions are intended to launder the illicit funds and make them available to the Chinese citizens, businesses, or nationals who purchased them from the CMLN. According to BSA reporting, financial institutions that have questioned customers, who are the ultimate beneficiaries or recipients of these funds, have been told that the customer was unable to move their money out of China due to currency control laws, and the customer paid for a service to circumvent these restrictions. While that is partially true, the reality is that the CMLNs keep the beneficiaries' funds in China, and pay them with laundered, illicit funds in the United States.

Trade-Based Money Laundering

CMLNs may also use complex TBML schemes to launder the Cartels' illicit funds. According to law enforcement, CMLNs may use money mules and other recruits to purchase U.S. electronics and other luxury goods (*e.g.*, cell phones, automobiles, clothing, designer handbags, etc.) at various

33. *See* Counterfeit Chinese Passports, *supra* note 10; *see also* FinCEN, FIN-2024-NTC1, "FinCEN Notice on the Use of Counterfeit U.S. Passport Cards to Perpetrate Identity Theft and Fraud Schemes at Financial Institutions" (Apr. 15, 2024).
34. *See* U.S. Department of Homeland Security, Homeland Security Investigations Assistant Director Ricardo Mayoral, "Written Testimony for Senate Caucus on International Narcotics Control Hearing Entitled 'Chinese Money Laundering Organizations: Cleaning Cartel Cash'" ("HSI Testimony") (Apr. 30, 2024), at p. 5; *see also* DOJ, "Queens Man Admits Orchestrating $653 Million Money Laundering Conspiracy, Operating Unlicensed Money Transmitting Business, and Bribing Bank Employees" (Feb. 22, 2022).
35. "Smurfs" are teams of persons who, acting in conjunction with or on behalf of other persons, structure financial transactions for the purpose of evading the requirement to file a Currency Transaction Report.
36. *See* Bags of Cash, *supra* note 32.
37. *See* FinCEN CMLN FTA, *supra* note 13, at pp. 18-19; *see also* 2024 NMLRA, *supra* note 3, at p. 30.
38. *See* DOJ, "Three Members of a Prolific Chinese Money Laundering Organization Plead Guilty to Laundering Tens of Millions of Dollars in Drug Proceeds" (May 1, 2025).

stores, some of whom are complicit, across the United States.[39] These purchases may be made using the drug proceeds or with credit cards that are subsequently paid off by the CMLN or by the complicit business owner.[40] Such businesses may have income that is not commensurate with that of other businesses of a similar size.

Once the goods are purchased, CMLNs often use shell or front companies, or complicit businesses, to resell or export these goods in a variety of ways. According to law enforcement, CMLNs may sell goods in the United States through various online marketplaces, at front companies, or at businesses complicit in their schemes. Alternatively, CMLNs may export the goods they purchase to counterparties in Mexico, China, Hong Kong, and the United Arab Emirates, who resell these goods in their respective countries. In some cases, U.S.-based CMLNs may export these goods to Cartel-owned companies in Mexico as an alternative to a mirror transfer. These exports serve as a form of value exchange between CMLN operators that avoids cross-border money movements and serves as a revenue source for the CMLNs.

CMLNs may also use or work with "*daigou*" buyers (meaning "buying on behalf of," *i.e.*, straw buyers)[41] to obtain U.S. goods for Chinese citizens or businesses. *Daigou* buyers may be witting or unwitting individuals and may be current, or former, Chinese nationals residing in the United States. CMLNs typically provide the *daigou* buyer with cash or send a P2P transfer to their account and instruct them to purchase certain goods. The *daigou* buyers are also instructed to ship the goods to a location in China or to a *daigou* operator, an individual that directs multiple buyers, located in the United States. *Daigou* operators typically further export the U.S. goods to China or other countries.

Case Study

Federal Indictment Alleges Alliance Between Sinaloa Cartel and Money Launderers Linked to Chinese Underground Banking

On June 18, 2024, the U.S. Department of Justice announced a 10-count superseding indictment charging Los Angeles-based associates of Mexico's Sinaloa Cartel with conspiring with money-laundering groups linked to Chinese underground banking to launder drug trafficking proceeds. During the conspiracy, more than $50 million in drug proceeds flowed between the Sinaloa Cartel associates and Chinese underground money exchanges. The multi-year investigation into this conspiracy—dubbed "Operation Fortune Runner"—resulted in a superseding indictment, which alleges that a Sinaloa Cartel-linked money laundering network collected and, with help from a San Gabriel Valley, California-based money transmitting group with links to Chinese underground banking, processed large

39. *See* FinCEN CMLN FTA, *supra* note 13, at p. 10.
40. *See* FinCEN CMLN FTA, *supra* note 13, at pp. 10-11. Generally, a trade or business that receives more than $10,000 in cash in a single transaction or in related transactions must file Form 8300. *See* 26 U.S.C. § 6050I; *see also* Internal Revenue Service, "Form 8300 and reporting cash payments of over $10,000" (Sept. 17, 2024).
41. The term "daigou" roughly translates to "buying on behalf of" and involves a practice where current or former Chinese nationals that reside in a different country purchasing goods on behalf of third parties located in China. *See* UK National Crime Agency, "Chinese Underground Banking and Daigou" (Oct. 2019); *see also* HSI Testimony *supra* note 34, at p. 5; FinCEN CMLN FTA, *supra* note 13, at pp. 12-13.

amounts of drug proceeds in U.S. currency in the Los Angeles area. They then allegedly concealed their drug trafficking proceeds and made the proceeds generated in the United States accessible to cartel members in Mexico and elsewhere. Lead defendant Edgar Joel Martinez-Reyes and others allegedly used a variety of methods to hide the money's source, including trade-based money laundering, "structuring" assets to avoid federal financial reporting requirements, and the purchase of cryptocurrency.

According to the superseding indictment, from October 2019 to October 2023, members and operatives of the Sinaloa Cartel imported large quantities of narcotics, including fentanyl, cocaine, and methamphetamine, into the United States, generating huge sums of drug cash proceeds in USD. In January 2021, Martinez-Reyes allegedly traveled to Mexico to meet with Sinaloa Cartel members to strike a deal with money remitters with links to Chinese underground banking to launder drug trafficking proceeds in the United States. After the deal was struck, the Sinaloa Cartel—through their connections and associates—distributed cocaine, methamphetamine, and other narcotics, generating U.S. dollars as drug proceeds. Martinez-Reyes and other conspirators allegedly then delivered the currency—frequently in amounts of hundreds of thousands of USD in cash—to other members of the Chinese underground money exchange and remitting organizations to be laundered for a fee. The remitting organizations possessed large amounts of USD and could help wealthy Chinese nationals evade the PRC's currency controls. The money remitters allegedly disposed of the drug proceeds by either delivering United States currency directly to their money exchange customers or by purchasing real or personal property, including luxury goods and cars to be shipped to China. Additionally, the remitters also moved illicit drug proceeds through cryptocurrency transactions. They also allegedly used a variety of traditional methods to place the funds into the traditional banking system such as purchasing cashier's checks, or "structuring," that is, depositing small amounts at a time into bank accounts opened for this purpose to avoid banks from reporting large cash deposits to the U.S. government.[42]

Red Flags Related to CMLNs Laundering Cartel Proceeds

FinCEN has identified red flags to help financial institutions detect, prevent, and report suspicious activity connected to CMLNs laundering illicit proceeds. As no single red flag is determinative of illicit or suspicious activity, financial institutions should consider the surrounding facts and circumstances, such as a customer's historical financial activity, whether the transactions are in line with prevailing business practices, and whether the customer exhibits multiple red flags, before determining if a behavior or transaction is suspicious or otherwise indicative of a connection to a CMLN.

42. DOJ, "Federal Indictment Alleges Alliance Between Sinaloa Cartel and Money Launderers Linked to Chinese Underground Banking" (June 18, 2024); First Superseding Indictment, Dkt. No. 217, *United States v. Martinez-Reyes*, 2:23-cr-258 (C.D. Cal. Apr. 4, 2024). Proceedings in the case remain ongoing.

Red Flags Potentially Indicative of CMLN-Affiliated Money Mules

1. A customer, especially a customer who presented a Chinese passport as identification during the onboarding process, regularly receives funds that are not commensurate with the reported occupation or income, and the source of the funds cannot be attributed to payroll or other legitimate sources of income (*i.e.*, unexplained wealth).[43]
2. During the onboarding process, a customer presents a Chinese passport and a visa that contain the same photograph despite being allegedly issued years apart.[44]
3. A customer, especially a Chinese national, creates an account at a financial institution and reports their occupation as a student during the onboarding process. This customer then regularly deposits cash into their account or receives wire transfers notated as "tuition" or "living expenses" that are not commensurate with the reported information. After receiving the funds, the customer may subsequently initiate wire transfers or P2P transactions to unknown individuals who are unrelated to the purpose of the wire transfers or may make credit or debit card payments.
4. A customer, especially a Chinese national, reports their occupation during customer onboarding as a student, retiree, housewife, or other low-income occupation but has unexplained wealth.
5. A customer, especially a Chinese national with unexplained wealth, initiates a wire transfer related to a real estate purchase or purchases cashier's checks made payable to a real estate company. The customer may be accompanied by a real estate agent at the time of purchasing the cashier's checks.
6. A customer, especially a Chinese national, regularly deposits large volumes of cash or cashier's checks, or receives multiple wire, ACH, or P2P transfers for no business or apparent lawful purpose. The customer then subsequently uses the funds to purchase a cashier's check or disperses the funds to other individuals using P2P and wire transfers, often to other high-risk jurisdictions.
7. A customer's account, especially a Chinese national, receives numerous transfers or deposits, and has a significant number of withdrawals or transfers, none of which appear to be related to routine payroll, living expenses, or customer's stated expected activity.
8. A customer, especially a Chinese national, has large amounts of cash funding cashier's checks, which are then deposited at another financial institution.
9. A customer, especially a Chinese national, is reluctant or refuses to provide information regarding the source of funds deposited or transferred into their account or acts evasive when questioned about the purpose of a transaction or may explain it as repayment of a loan.

43. *See* Counterfeit Chinese Passports, *supra* note 10.
44. *Id.*

10 A customer that is a U.S.-based escrow company receives funds from an unaffiliated, foreign-based shell company or entity in a disparate line of business that are used to purchase real estate in the United States.

Red Flags Potentially Indicative of CMLN-Affiliated TBML Schemes

11 A business[45] owned by a Chinese national regularly receives deposits from online marketplaces, but rarely, or never, engages in transactions that indicate the purchase of goods to maintain inventory.

12 A business owned by a Chinese national regularly receives wire transfers indicating the export of goods to foreign countries including Mexico, China, Hong Kong, and the United Arab Emirates, but rarely, or never, engages in transactions that indicate the purchase of goods to maintain inventory.

13 A small U.S.-based business in the electronics or real estate industry receives wires from Mexico, China, Hong Kong, and the United Arab Emirates and has no known nexus to these countries.

14 A customer, especially a Chinese national, regularly receives P2P or wire transfers from unknown individuals and subsequently uses those funds to make a substantial credit card payment. If questioned about the source of the funds, the customer may state that the transfers are from U.S.-based family members of Chinese citizens who are sending the customer funds to purchase goods.

15 A customer, especially a Chinese national, regularly uses a credit card to purchase large volumes of electronics or other luxury goods.

16 A business that sells electronics or other luxury goods has income that is not commensurate with the size and scale of the business.

17 A business that sells electronics or other luxury goods makes payments for multiple credit cards associated with various individuals, who are seemingly unrelated to the business.

18 Hong Kong registered trading companies with shell-like characteristics send funds to Chinese nationals residing in the United States, real estate escrow or title insurance companies, and other international destinations with no apparent business or economic purpose.

45. According to BSA reporting, businesses are commonly reported to be in shipping, transportation, freight, logistics, industrial supplies, food, and technology sectors.

Reminder of Relevant BSA Obligations and Tools for U.S. Financial Institutions

Suspicious Activity Reporting

A financial institution is required to file a suspicious activity report (SAR) if it knows, suspects, or has reason to suspect a transaction conducted or attempted by, at, or through the financial institution involves funds derived from illegal activity; is intended or conducted to disguise funds derived from illegal activity; is designed to evade regulations promulgated under the BSA; lacks a business or apparent lawful purpose; or involves the use of the financial institution to facilitate criminal activity.[46] All statutorily defined financial institutions may voluntarily report suspicious transactions under the existing suspicious activity reporting safe harbor.[47]

When a financial institution files a SAR, it is required to maintain a copy of the SAR and the original or business record equivalent of any supporting documentation for a period of five years from the date of filing the SAR.[48] Financial institutions must provide any requested documentation supporting the filing of a SAR upon request by FinCEN or an appropriate law enforcement or supervisory agency.[49] When requested to provide supporting documentation, financial institutions should take special care to verify that a requestor of information is, in fact, a representative of FinCEN or an appropriate law enforcement or supervisory agency. A financial institution should incorporate procedures for such verification into its BSA compliance or AML program. These procedures may include, for example, independent employment verification with the requestor's field office or face-to-face review of the requestor's credentials.

SAR Filing Instructions

SARs, and compliance with other BSA requirements, are crucial to identifying and stopping CMLNs. FinCEN requests that financial institutions indicate a connection between the suspicious activity being reported and the activities highlighted in this Advisory by including the key term "**CMLN-2025-A003**" in SAR field 2 (Filing Institution Note to FinCEN), as well as in the narrative. Financial institutions may highlight additional Advisory, Alert, or Notice keywords in the narrative, if applicable.

Financial institutions should select SAR field 38(n) (Suspicious Use of Informal Value Transfer System); SAR field 38(s) (Unlicensed or Unregistered MSB); SAR field 36(l) (Trade Based Money Laundering/Black Market Peso Exchange), and any other applicable check box. Financial

46. 31 U.S.C. § 5318(g)(1); *see also* 31 CFR §§ 1020.320, 1021.320, 1022.320, 1023.320, 1024.320, 1025.320, 1026.320, 1029.320, 1030.320.
47. *See* 31 U.S.C. § 5318(g)(3). Financial institutions may report suspicious transactions regardless of amount involved and still take advantage of the safe harbor.
48. *See* 31 CFR §§ 1020.320(d), 1021.320(d), 1022.320(c), 1023.320(d), 1024.320(c), 1025.320(d), 1026.320(d), 1029.320(d), 1030.320(d).
49. *Id.*; *see also* FinCEN, FIN-2007-G003, "Suspicious Activity Report Supporting Documentation" (June 13, 2007).

institutions also should select all other relevant suspicious activity fields, such as those in SAR fields 36 (Money Laundering) and 38 (Other Suspicious Activities), if applicable.

Financial institutions should include all available information relating to the account and locations involved in the reported activity, identifying information related to other entities and persons involved in the activity and the status of their accounts with the institution. Financial institutions also should provide all available information regarding other domestic and foreign financial institutions involved in the activity; where appropriate, financial institutions should consider filing a SAR jointly on shared suspicious activity.[50]

Financial institutions are required to file complete and accurate reports that incorporate all relevant information available. In situations involving violations requiring immediate attention, such as ongoing money laundering schemes, a financial institution should also immediately notify, by telephone, an appropriate law enforcement authority, in addition to filing a timely SAR.[51] Immediate notification to law enforcement is especially important in situations involving suspected terrorist activity, as terrorists and terrorist organizations often rely on the international financial system to acquire funding to sustain and finance their operations and engage in acts of terrorism. Additionally, FinCEN emphasizes that any financial institution and any director, officer, employee, or agent of such institution who makes, or requires another to make any voluntary disclosure of any possible violation of law or regulation to a government agency under the BSA or its implementing regulations is protected from liability for any such disclosure.[52]

Financial institutions wanting to report suspicious transactions that may potentially relate to terrorist activity should call the Financial Institutions Toll-Free Hotline at (866) 556-3974 (7 days a week, 24 hours a day).[53]

Other Relevant BSA Reporting Requirements

Financial institutions and other entities or persons may also have other relevant BSA reporting requirements to provide information in connection with the subject of this Advisory. These include obligations related to the Currency Transaction Report (CTR),[54] Report of Cash Payments Over $10,000 Received in a Trade or Business (Form 8300),[55] Report of Foreign

50. *See* 31 CFR §§ 1020.320(e)(1)(ii)(A)(2))(i), 1021.320(e)(1)(ii)(A)(2)), 1022.320(d)(1)(ii)(A)(2), 1023.320(e)(1)(ii)(A)(2)(i), 1024.320(d)(1)(ii)(A)(2), 1025.320(e)(1)(ii)(A)(2), 1026.320(e)(1)(ii)(A)(2)(i), 1029.320(d)(1)(ii)(A)(2), 1030.320(d)(1)(ii)(A)(2).
51. *See, e.g.*, 31 CFR §§ 1020.320(b)(3), 1022.320(b)(3), 1023.320(b)(3).
52. 31 U.S.C. § 5318(g)(3); *see, e.g.*, 31 CFR 1020.320(f).
53. The purpose of the hotline is to expedite the delivery of this information to law enforcement. Financial institutions should immediately report any imminent threat to local-area law enforcement officials.
54. A report of each deposit, withdrawal, exchange of currency, or other payment or transfer, by, through, or to a financial institution that involves a transaction in currency of more than $10,000. Multiple transactions may be aggregated when determining whether the reporting threshold has been met. *See* 31 CFR §§ 1010.310-313, 1020.310-313, 1021.310-313, 1022.310-313, 1023.310-313, 1024.310-313, and 1026.310-313.
55. A report filed by a trade or business that receives currency in excess of $10,000 in one transaction or two or more related transactions. The transactions are required to be reported on a joint FinCEN/Internal Revenue Service form when not otherwise required to be reported on a CTR. *See* 31 CFR §§ 1010.330-331. A Form 8300 also may be filed voluntarily for any suspicious transaction, even if the total amount does not exceed $10,000.

Bank and Financial Accounts (FBAR),[56] Report of International Transportation of Currency or Monetary Instruments (CMIR),[57] Registration of Money Services Business (RMSB),[58] and Designation of Exempt Person (DOEP).[59]

Due Diligence

Banks, brokers or dealers in securities, mutual funds, and futures commission merchants and introducing brokers in commodities (FCM/IBs) are required to have appropriate risk-based procedures for conducting ongoing customer due diligence that include, but are not limited to: (i) understanding the nature and purpose of customer relationships for the purpose of developing a customer risk profile; and (ii) conducting ongoing monitoring to identify and report suspicious transactions and, on a risk basis, to maintain and update customer information.[60] Covered financial institutions are required to identify and verify the identity of beneficial owners of legal entity customers, subject to certain exclusions and exemptions.[61] Among other things, this facilitates the identification of legal entities that may be owned or controlled by foreign politically exposed persons (PEPs).

Senior foreign political figures and due diligence obligations for private banking accounts

In addition to these due diligence obligations, under section 312 of the USA PATRIOT Act (31 U.S.C. § 5318(i)) and its implementing regulations, covered financial institutions must implement due diligence programs for private banking accounts held for non-U.S. persons that are designed to detect and report any known or suspected money laundering or suspicious activity conducted through or involving such accounts.[62] Covered financial institutions must establish risk-based controls and procedures for ascertaining the identities of nominal and beneficial owners of such accounts and ascertaining whether any of these owners are senior foreign political figures, and for conducting enhanced scrutiny on accounts held by senior foreign political figures that is reasonably designed to detect and report transactions that may involve the proceeds of foreign corruption.[63]

56. A report filed by a U.S. person that has a financial interest in, or signature or other authority over, foreign financial accounts with an aggregate value exceeding $10,000 at any time during the calendar year. *See* 31 CFR § 1010.350; FinCEN Form 114.
57. A form filed to report the transportation of more than $10,000 in currency or other monetary instruments into or out of the United States. *See* 31 CFR § 1010.340.
58. A form filed to register a money services business (MSB with FinCEN, or to renew such a registration. *See* 31 CFR § 1022.380.
59. A report filed by banks to exempt certain customers from currency transaction reporting requirements. *See* 31 CFR § 1010.311.
60. *See* 31 CFR §§ 1020.210(a)(2)(v), 1023.210(b)(5), 1024.210(b)(6), 1026.210(b)(5).
61. *See* 31 CFR §§ 1010.230, 1010.650(e)(1) (defining "covered financial institution").
62. *See* 31 CFR § 1010.620. The definition of "covered financial institution" is found in 31 CFR § 1010.605(e)(1). The definition of "private banking account" is found in 31 CFR § 1010.605(m). The definition of "non-U.S. person" is found in 31 CFR § 1010.605(h).
63. *See* 31 CFR § 1010.620(c).

AML/CFT program and correspondent account due diligence requirements

Financial institutions are reminded of AML/CFT program requirements,[64] and covered financial institutions are reminded of correspondent account due diligence requirements under Section 312 of the USA PATRIOT Act (31 U.S.C. § 5318(i)) and implementing regulations.[65] As described in FinCEN Interpretive Release 2004-1, the AML/CFT program of an MSB must include risk-based policies, procedures, and controls designed to identify and minimize risks associated with foreign agents and counterparties.[66]

Information Sharing

Information sharing among financial institutions is critical to identifying, reporting, and preventing CMLN-related and other illicit financial activity. Financial institutions and associations of financial institutions sharing information under the safe harbor authorized by section 314(b) of the USA PATRIOT Act are reminded that they may share information with one another regarding individuals, entities, organizations, and countries suspected of possible terrorist financing or money laundering.[67] In accordance with the requirements of section 314(b) and its implementing regulations, FinCEN strongly encourages such voluntary information sharing as it relates to money laundering or possible terrorist financing in connection with Foreign Terrorist Organizations (FTOs)[68] and Specially Designated Global Terrorists (SDGTs).[69]

The Financial Crimes Enforcement Network's Advisory Program communicates priority money laundering, terrorist financing, and other illicit finance threats and vulnerabilities to the U.S. financial system. Financial institutions may use this information to support effective, risk-based, and reasonably designed anti-money laundering and countering the financing of terrorism (AML/CFT) programs and suspicious activity monitoring systems to help generate highly useful information for law enforcement and national security agencies.

64. *See* 31 CFR §§ 1010.210, 1020.210, 1021.210, 1022.210, 1023.210, 1024.210, 1025.210, 1026.210, 1027.210, 1028.210, 1029.210, 1030.210.
65. *See* 31 CFR § 1010.610.
66. *See* FinCEN, Anti-Money Laundering Program Requirements for Money Services Businesses with Respect to Foreign Agents or Foreign Counterparties, Interpretive Release 2004-1, 69 Fed. Reg. 74,439 (Dec. 14, 2004); *see also* FinCEN, "Guidance on Existing AML Program Rule Compliance Obligations for MSB Principals with Respect to Agent Monitoring" (Mar. 11, 2016).
67. *See* 31 CFR § 1010.540; *see also* FinCEN, "Section 314(b) Fact Sheet" (Dec. 2020).
68. *See* U.S. Department of State, "Foreign Terrorist Organizations."
69. Executive Office of the President, "Executive Order 13224" (Sept. 23, 2001).

For Further Information

FinCEN's website at www.fincen.gov contains information on how to register for FinCEN Updates. Questions or comments regarding the contents of this Advisory should be addressed to the FinCEN Regulatory Support Section at www.fincen.gov/contact.

The mission of the Financial Crimes Enforcement Network is to safeguard the financial system from illicit use, counter money laundering and the financing of terrorism, and promote national security through strategic use of financial authorities and the collection, analysis, and dissemination of financial intelligence.