FINANCIAL CRIMES ENFORCEMENT NETWORK

Financial Trend Analysis

Chinese Money Laundering Networks: 2020 - 2024 Threat Pattern & Trend Information

August 2025

Chinese Money Laundering Networks: 2020 - 2024 Threat Pattern & Trend Information

This Financial Trend Analysis (FTA) focuses on patterns and trends identified in Bank Secrecy Act (BSA) data linked to suspected Chinese money laundering networks (CMLNs). This report is issued pursuant to Section 6206 of the Anti-Money Laundering Act of 2020, which requires the Financial Crimes Enforcement Network (FinCEN) to periodically publish BSA-derived threat pattern and trend information.[1] The information in this report is relevant to the public, including a wide range of consumers, businesses, and industries, and it highlights the value of BSA data filed by regulated financial institutions.

Executive Summary: FinCEN analyzed 137,153 BSA reports (the dataset), totaling approximately $312 billion in suspicious activity, filed between 1 January 2020 and 31 December 2024 (the review period), associated with suspected Chinese money laundering network (CMLN) activity.[2] FinCEN's analysis of the dataset revealed certain trends in CMLN activity—including the potential role of U.S.- and foreign-based Chinese passport holders—and sheds light on how CMLNs launder illicit proceeds from criminal activities, including drug trafficking, and how CMLNs launder money on a global scale.

- *Banks Filed the Majority of Potentially CMLN-Related BSA Reports in the Dataset:* Depository institutions filed 85 percent of reports in the dataset, which predominantly identified subjects potentially engaged in money laundering activity. Money services businesses (MSBs) filed the second-highest number of BSA reports in the dataset, accounting for nine percent.
- *CMLNs Reportedly Rely on U.S.-Based Chinese Nationals to Deposit Cash—Often Unknown Sources of Funds—into the U.S. Financial System:* CMLNs facilitate money laundering for criminal organizations by using U.S.-based accounts—including both personal and business accounts—often initiated through large cash deposits, which are inconsistent with a customer's account profile, and sometimes conducted by non-authorized account users. CMLNs also use foreign-based accounts to move and launder illicit funds through the U.S. financial system.
- *CMLNs' Access to USD Potentially Facilitates Trade-Based Money Laundering Schemes:* CMLNs are extremely agile and support various types of money laundering based on the needs of their customers. CMLNs service Chinese nationals seeking U.S. dollars (USD), facilitate trade-based money laundering (TBML), and enable other types of money laundering schemes. Financial institutions filed 512 reports within the dataset that reference the term TBML, totaling

1. The Anti-Money Laundering Act of 2020 was enacted as Division F, §§ 6001-6511, of the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, Pub. L. 116-283 (2021).
2. These reports may refer to financial activity that occurred prior to the review period. BSA filers often reported suspicious financial activity that may have occurred over a multi-year period that began before 2020. This included instances in which filers identified derogatory information, such as arrests and indictments, involving their customers.

approximately $9.7 billion in reported suspicious activity. FinCEN analysis also identified multiple indicators of TBML-related activity in BSA reports in the dataset even where those reports did not expressly reference the term TBML.

- *CMLNs Potentially Working with U.S.-Based Daigou Buyers to Launder Illicit Proceeds:* U.S.-based CMLNs recruit individuals known as *daigou* buyers (meaning "buying on behalf of") to purchase high-value electronics and luxury goods for export to the People's Republic of China (PRC) and other countries. The term "*daigou*" was reported in a small number of BSA reports in the dataset associated with approximately $9.6 million in suspicious activity. The need for large amounts of USD to facilitate *daigou*-related purchases likely brings *daigou* networks into contact with CMLNs, which have access to bulk U.S. currency available for sale.
- *Potential Human Trafficking- and Smuggling-Related Activity Involving U.S.-Based Chinese Passport Holders:* Financial institutions filed 1,675 BSA reports in the dataset indicating suspicious activity potentially involving human trafficking or human smuggling.
- *CMLNs Potentially Using Adult Daycare Centers Located in New York to Further Laundering Activities; Also Linked to Healthcare Fraud, Elder Abuse, and Illicit Gaming Activity:* Financial institutions filed 43 BSA reports in the dataset involving approximately $766 million in suspicious activity, on 83 adult and senior day care centers, all of which listed addresses in New York. FinCEN also identified 108 BSA reports in the dataset involving deposited funds potentially associated with healthcare fraud, elder abuse, and suspicious gaming activity.
- *CMLNs Potentially Facilitating Real Estate Purchases Funded by Illicit Proceeds from a Variety of Financial Crimes:* Financial institutions filed 17,389 BSA reports in the dataset associated with more than $53.7 billion in suspicious activity involving the real estate sector. CMLNs potentially play a key role in laundering illicit funds through U.S. real estate by using complex, layered transactions; involving third parties; and ultimately, integrating illicit proceeds into the real estate sector to launder ill-gotten gains. CMLNs potentially target high-value markets and leverage Chinese investors who have strong interest in U.S. real estate.
- *CMLNs May Use Chinese Students to Engage in a Variety of Suspicious Financial Activities and Schemes:* Financial institutions filed 20,282 BSA reports in the dataset involving approximately $13.8 billion in suspicious activity and referenced individuals purporting to be Chinese students. Chinese students may be vulnerable to recruitment and exploitation by U.S.-based CMLNs, which need access to, and control of, many bank accounts to place illicit proceeds into the U.S. financial system, according to FinCEN analysis.

Scope and Methodology: For purposes of this report, FinCEN analyzed BSA reports pertaining to subjects with Chinese passports and containing keywords potentially indicative of CMLN activity. FinCEN used a combination of automated and manual review of the BSA reports to remove false positives. The final dataset comprises 137,153 BSA reports totaling approximately $312 billion in potential CMLN-related suspicious activity filed over a five-year period. FinCEN identified these BSA reports based on a report's filing date, rather than the date of the suspicious activity; therefore, these reports may also refer to incidents that occurred prior to the five-year review period.

In this report, FinCEN highlights prevalent trends and typologies used by CMLNs reflected in the dataset. FinCEN has based its analysis on the information provided in these BSA reports, as well as certain portions of transactional data underlying these BSA reports. FinCEN's analysis is also informed by its ongoing work to support law enforcement.

A Note About BSA Data

BSA reporting reflects only suspicious activity that has been identified and reported, and therefore should not be considered a complete representation of the scope of any particular type of suspicious activity. BSA reporting may include additional transactions and information beyond a specific transaction that may be reportable as suspicious and, accordingly, the total reportable suspicious activity amount in any report may be overly inclusive. For example, BSA reporting may reflect both completed and attempted transactions, both inbound and outbound transactions, and transfers between accounts. The reported suspicious activity in any individual BSA filing may include both legal and illicit activities associated with a particular subject. BSA reporting may also describe continuing suspicious activity or amend earlier reporting, or reports that cover expanded networks involved in potential illicit activity, and therefore may reflect cumulative transactions from a single filer involving the same subject.

The Role of CMLNs in Facilitating Money Laundering

CMLNs have seized on the globalization of financial and trade markets involving the PRC to establish and operate businesses worldwide that allow them to launder large amounts of illicit proceeds through global commerce, according to FinCEN's analysis of BSA reports and law enforcement information. CMLNs bypass the PRC's capital flight restrictions and aid criminals in laundering their illicit proceeds using a multitude of techniques. International cartels have relied heavily on CMLNs in recent years to launder USD drug-trafficking proceeds through myriad methods, including both illegal and legal businesses that rely on complex schemes to disguise the source(s) of funds.[3]

CMLNs facilitate money laundering using bulk USD received from drug trafficking networks in the United States and returning the profits to cartels in Mexico. Over the past five years, FinCEN has seen an increase in complex money laundering schemes controlled by CMLNs that also launder illicit proceeds from otherwise unrelated criminal networks involved in a range of illicit activities, including fraud schemes; human trafficking and smuggling; marijuana grow house operations; and tax evasion, by facilitating the exchange of cash proceeds. CMLNs have gained prominence among global money laundering groups due to their reliability, low fees, organizational structure, worldwide presence, and access to the U.S. financial system. CMLNs often rely on Chinese passport holders residing in the United States that allow illicit funds to enter and circulate within the U.S. financial system, ultimately moving into the legitimate economy.

Banks Filed the Majority of Potentially CMLN-Related BSA Reports in the Dataset

Financial institutions filed 137,153 BSA reports potentially relating to CMLN activity in the dataset. A total of 1,038 financial institutions filed the BSA reports in the dataset, with filers consisting of depository institutions, MSBs, casinos, as well as insurance, securities/futures, and loan/finance companies.[4] Additionally, three of the filers are categorized within the dataset as "other," which includes online retailers and a compliance service provider.

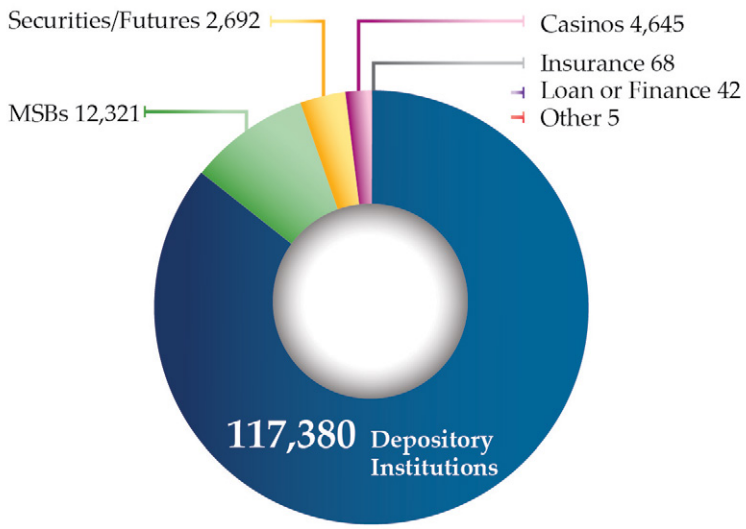
- Depository institutions filed 117,380 BSA reports—or 85 percent of the dataset.[5] In total, 489 unique depository institutions filed BSA reports in the dataset, and three of the depository institutions reported over 10,000 BSA reports each. The depository institutions reported

3. Please refer to FinCEN's Advisory on the Cartels' use of CMLNs to launder illicit proceeds for more information. Financial institutions should file SARs related to this activity using the keyword: **CMLN-2025-A003**. *See generally* "FinCEN Advisory on the Use of Chinese Money Laundering Networks by Mexico-Based Transnational Criminal Organizations to Launder Illicit Proceeds," FinCEN Advisory #FIN-2025-A003, 28 August 2025, https://www.fincen.gov/sites/default/files/advisory/2025-08-28/FinCEN-Advisory-CMLN-508.pdf.
4. FinCEN analysis identified likely false positives of CMLN-related activity within BSA reporting filed by a U.S.-based MSB; therefore, the CMLN-related dataset excludes this reporting.
5. For this Financial Trend Analysis report, depository institutions include banks and credit unions.

potentially suspicious activity linked to U.S.-based Chinese students, real estate transactions, suspicious wire and peer-to-peer (P2P) transfers, suspected human trafficking and human smuggling activity, evasion of capital flight restrictions, and other financial schemes.

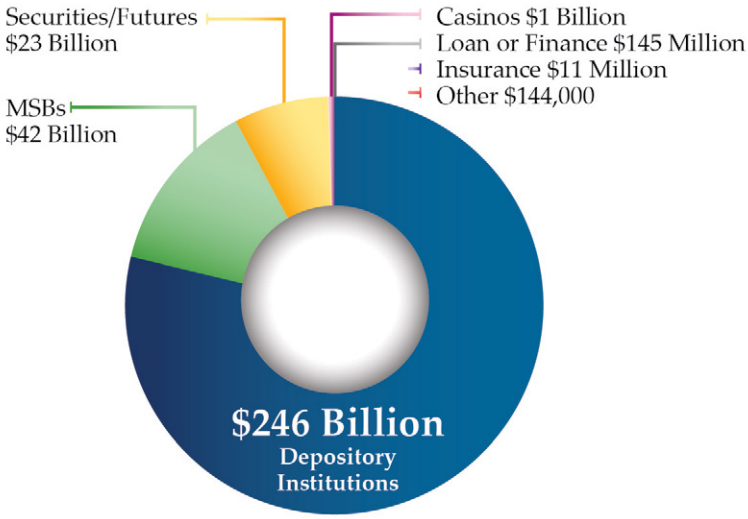
- MSBs filed the second highest number of BSA reports in the dataset, accounting for nine percent—or 12,321 BSA reports. In total, 222 unique MSBs filed BSA reports in the dataset. The MSBs most frequently reported potentially suspicious transactions involving excessive purchases of money orders, structured outgoing money transfers to evade PRC currency restrictions, and the rapid movement of incoming and outgoing money transfers over a short time frame.
- Casinos, securities/futures firms, insurance companies, loan/finance companies, and other filers accounted for the remaining BSA reports—totaling 7,452 BSA reports or five percent—within the dataset. These filers consisted of 327 unique financial institutions, frequently flagging potentially suspicious transactions related to casino gaming incidents, suspicious investment activity, suspicious life insurance policy payments, and loan and mortgage payments funded with unsourced cash.

Figure 1. Total Number of Potentially CMLN-Related BSA Reports by Filer Type (2020-2024)



The dataset of BSA reports accounted for approximately $312 billion in total suspicious activity, averaging approximately $2.3 million per filing, and a median amount of approximately $86,000 per filing. Depository institution filings comprised the vast majority of the suspicious activity amount—approximately $246 billion—with MSBs making up the second highest dollar amount with over $42 billion in reported suspicious activity during the review period. Casinos, insurance companies, securities/futures firms, loan/finance companies, and others reported approximately $24 billion in reported suspicious funds combined.

Figure 2. Total Reported Suspicious Activity Amount of Potentially CMLN-Related BSA Reports by Filer Type (2020-2024)



CMLNs Reportedly Rely on U.S.-Based Chinese Nationals to Deposit Cash—Often Unknown Sources of Funds—into the U.S. Financial System

BSA reporting identified large cash deposits into bank accounts by U.S.-based Chinese nationals as the most common suspicious activity type in the dataset, based on the lack of a verifiable income source or because transactors were employed in low-wage sectors. Thirty-three percent—or 46,360 BSA reports—in the dataset reference cash deposit transactions totaling over $33 billion in reported suspicious activity. Large cash deposits with unidentified sources of funds—or that are not aligned with the expected income of the known occupation—were considered suspicious and potentially indicative of illegal activity, such as money laundering.[6]

Filers also reported large, suspicious cash deposits used to purchase cashier's checks for real-estate-related transactions that are often linked to money laundering schemes, including those involving CMLNs.[7] These transactions may involve large cash deposits, or structured deposits designed to avoid regulatory reporting thresholds, which are commonly used to conceal the origins of illicit funds.[8] BSA reporting also identified the following transaction patterns:

- Large cash deposits into a U.S. bank account used to fund same-day wire transfers to accounts at a different U.S. bank, which are controlled by a Chinese national living in the PRC.
- Large cash deposits into an account at a U.S. bank, only to be transferred to another account within the same bank, which is controlled by the same account signer, on the same day. Banks also noted that this was suspicious because the second account had an additional account signer.

6. *See* "Federal Financial Institutions Examination Council (FFIEC) BSA/AML Manual, Appendix F – Money Laundering and Terrorist Financing Red Flags," *FFIEC*, 27 February 2015, https://bsaaml.ffiec.gov/docs/manual/10_Appendices/07.pdf.
7. *See* "Chinese Money Laundering Organizations: Cleaning Cartel Cash," U.S. Senate Caucus on International Narcotics Control, 30 April 2024, https://www.drugcaucus.senate.gov/media-center/files/2024-04-30-mayoral-testimony/.
8. *See* "2024 National Strategy for Combating Terrorist and Other Illicit Financing," U.S. Department of the Treasury, May 2024, https://home.treasury.gov/system/files/136/2024-Illicit-Finance-Strategy.pdf.

- Large cash deposits into an account where funds were used to purchase a cashier's check made payable to the account signer and deposited at a different bank on the same day.

PRC Currency Restrictions Fuel Use of U.S.-Based CMLNs to Access USD

The PRC maintains strict currency controls, also known as capital flight restrictions, which limit the amount of money Chinese citizens can transfer abroad each year to 50,000 USD for investment and financial purposes.[9] [10] [11] Many Chinese citizens have turned to alternative methods, like the Chinese underground banking system (CUBS), to bypass these restrictions. The CUBS consists of various individuals and businesses from different industries who collaborate through "mirror transfers" to move money across borders, as part of informal value transfer system schemes.[12] The CUBS, in turn, depends on CMLNs to secure foreign currency. While the funds held by Chinese citizens are often considered legitimate, the PRC continues to crack down on corruption. Individuals seeking to avoid tax obligations in China have also fueled the use of CUBS to provide an anonymous transfer method, enhancing reliance on CMLNs. CMLNs use these funds to facilitate CUBS payments related to illicit transactions. CMLNs generate profits by laundering funds from unrelated criminal activities in the United States and reselling that USD to Chinese nationals seeking to circumvent the PRC's strict currency controls. The relationship between CUBS and CMLNs often results in legitimate funds becoming intertwined with illicit proceeds.

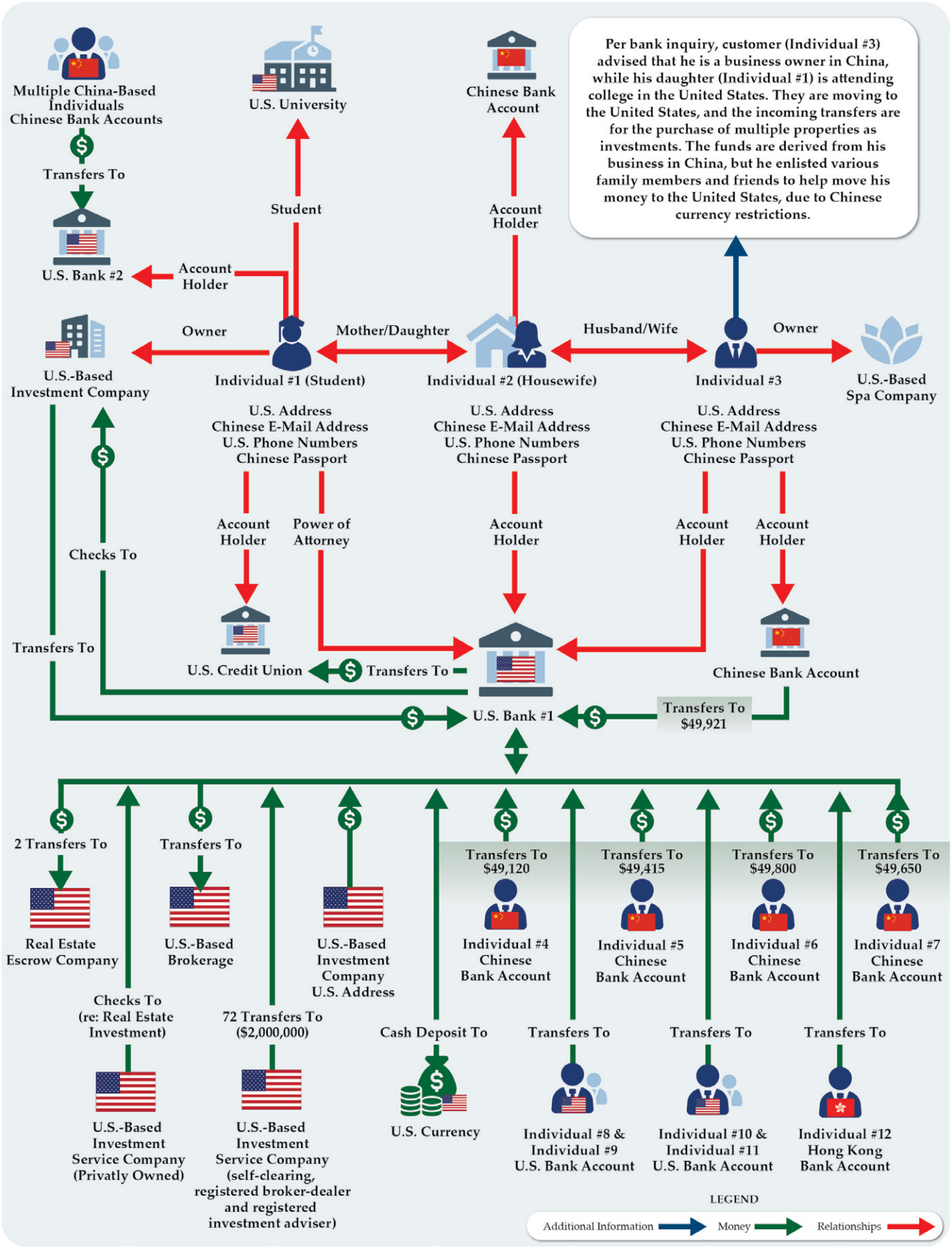
BSA Reports Highlight Common Indicators of Chinese Capital Flight

FinCEN analysis revealed 741 BSA reports in the dataset that identified "*capital flight*" or "*Chinese currency restriction*," indicating transactional activity consistent with currency control evasion.

Filers cited difficulty determining the true source of the incoming wire transfers from the PRC or noted that the transfers appeared to be conducted in a manner to avoid the PRC's currency restrictions. BSA reports indicated that funds received from international transfers that originated from the PRC were used in a suspicious manner, or that the funds were not used as intended. BSA reports described multiple incoming international transfers that originated from the PRC over short periods of time, followed by rapid withdrawal of funds in one outgoing transaction, often involving the purchase of real estate.

9. *See* "International Narcotics Control Strategy Report Volume II, Money Laundering and Financial Crimes," U.S. Department of State, Bureau of International Narcotics and Law Enforcement Affairs, March 2016, https://2009-2017.state.gov/documents/organization/253983.pdf.
10. *See* U.S. Department of State, "2024 Investment Climate Statements: PRC," 2024, https://www.state.gov/reports/2024-investment-climate-statements/china/.
11. *See* "China: the evolution of foreign exchange controls and the consequences of capital flows," *Bank for International Settlements*, https://www.bis.org/publ/bppdf/bispap44h.pdf, accessed 10 June 2025.
12. "Mirror transfers" is a term used by U.S. law enforcement to describe a money laundering typology involving foreign currency exchange. The process typically happens within black market peso exchange schemes and usually involves a network that conducts two equal, but separate, transactions involving at least two parties who often are unaware of each other. *See* "Chinese Money Laundering Organizations: Cleaning Cartel Cash," U.S. Senate Caucus on International Narcotics Control, 30 April 2024, https://www.drugcaucus.senate.gov/media-center/files/2024-04-30-mayoral-testimony/.

Figure 3. Likely Capital Flight Example Involving Chinese Student and the Purchase of Real Estate



CMLNs' Access to USD Potentially Facilitates Trade-Based Money Laundering Schemes

Financial institutions filed 512 BSA reports in the dataset, totaling approximately $9.7 billion in reported suspicious activity, that reference TBML activity. BSA reports in the dataset identified TBML schemes, which are often categorized by financial institutions as "high-risk" typologies, that are directed by CMLNs. TBML is a method used by CMLNs that often includes the movement of illicit proceeds through a series of transactions involving the acquisition, shipment, and/or resale of goods. TBML involving cell phones and electronics is a widely used methodology by CMLNs to launder funds and profit on the resale of high-demand goods outside the United States.[13] CMLNs often use U.S.-based money mules to place large volumes of cash into the U.S. financial system that are then used to further TBML schemes. CMLNs are often compensated by other criminal organizations, like Mexico-based cartels, for arranging, organizing, and executing these transactions. BSA reports in the dataset highlighted the following transaction patterns linked to suspected TBML:

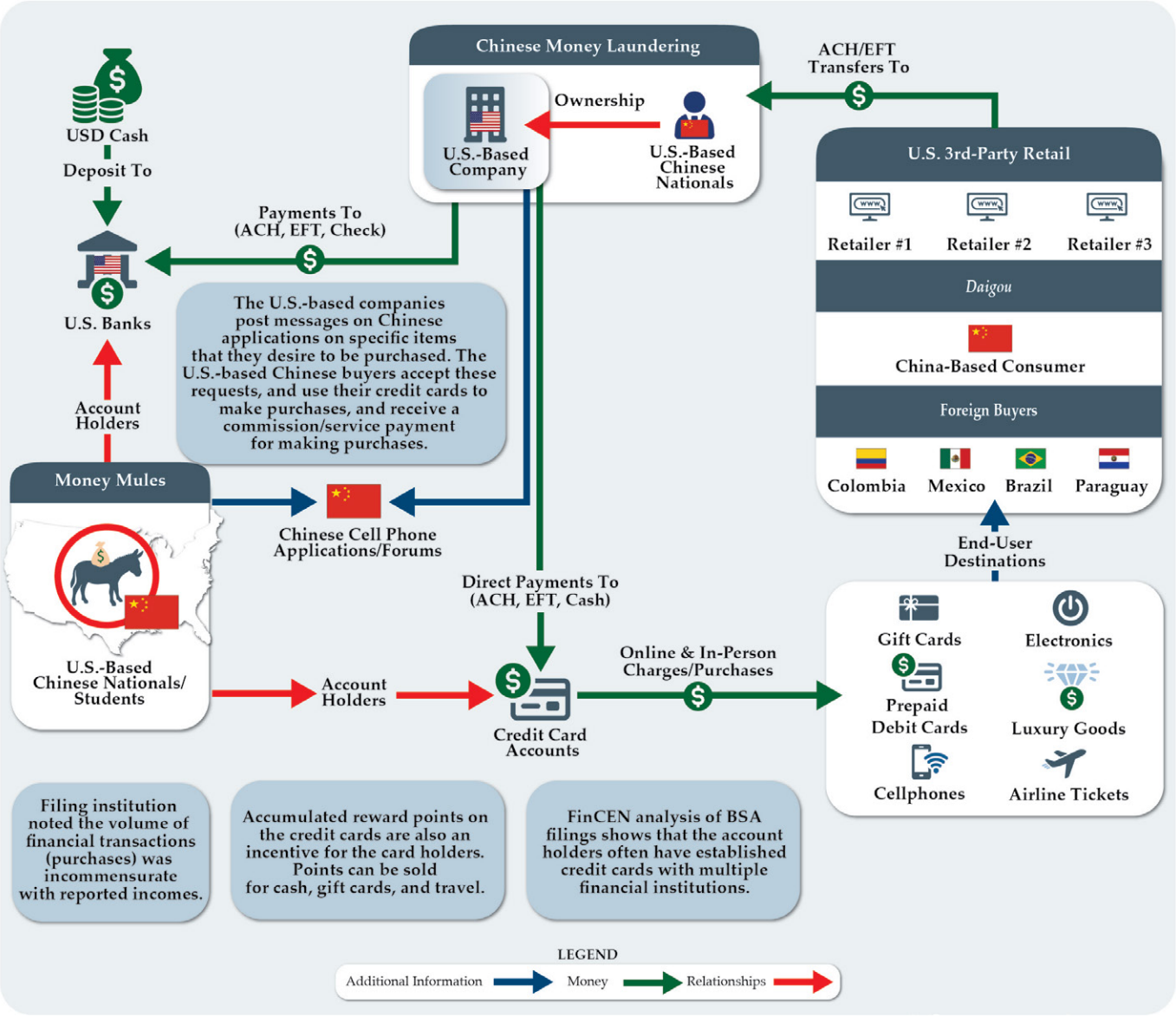
- Financial institutions reported suspicious activity consisting of unusual deposits into the same customers' accounts from various unrelated individuals and businesses that did not appear to be related to the customers' business or occupation type; excessive structured cash deposits; incoming wires from individuals and businesses; electronic deposits from investment vehicles and virtual currency addresses; and P2P credits from individuals for which the relationship and purpose was unknown.
- BSA reports highlighted the purchase of high-value luxury goods, such as watches, designer bags, and cell phones, which are commonly used because of their resale value and portability.[14] The reported transactions often involved various layering mechanisms and movements of funds without any reference to the origins of the goods or anticipated purposes of the transactions. Banks reported that accounts held by their customers were being funded by check deposits and transfers from accounts that the same customer controls at other banks.
- BSA reporting identified that individual account holders are using deposited funds to pay down balances for credit cards that are being used to purchase items, such as cell phones, in an excessive and repetitive manner. Filers reported large volumes of credit card purchases and unknown sources of deposited funds to facilitate payments. Filers also noted that deposited funds are often from companies identified as being sellers on third-party websites that are posting the same types of items for sale.

One BSA filer identified a suspected CMLN that included U.S.-based electronics companies and thousands of Chinese nationals who purchased bulk electronics and gift cards in a massive TBML scheme. The filer reported that the CMLN used credit cards involving over seven million charges

13. *Ibid.*
14. *See* "2024 National Money Laundering Risk Assessment," U.S. Department of the Treasury, February 2024, https://home.treasury.gov/system/files/136/2024-National-Money-Laundering-Risk-Assessment.pdf.

exceeding $6 billion USD between 2019 and 2024. The credit card holders and electronics company representatives communicated over online forums and message boards to discuss the quantities of electronics needed, as well as gift cards, shipping addresses, and other pertinent information for the scheme. Once the items were purchased and shipped, the companies made payments in the form of cash, checks, and transfers to the credit card account holders' bank accounts, or directly to the credit card company, to include a service fee for the purchaser.

Figure 4. Use of Credit Cards in CMLN-Directed TBML Scheme



CMLNs Potentially Working with U.S.-Based Daigou Buyers to Launder Illicit Proceeds

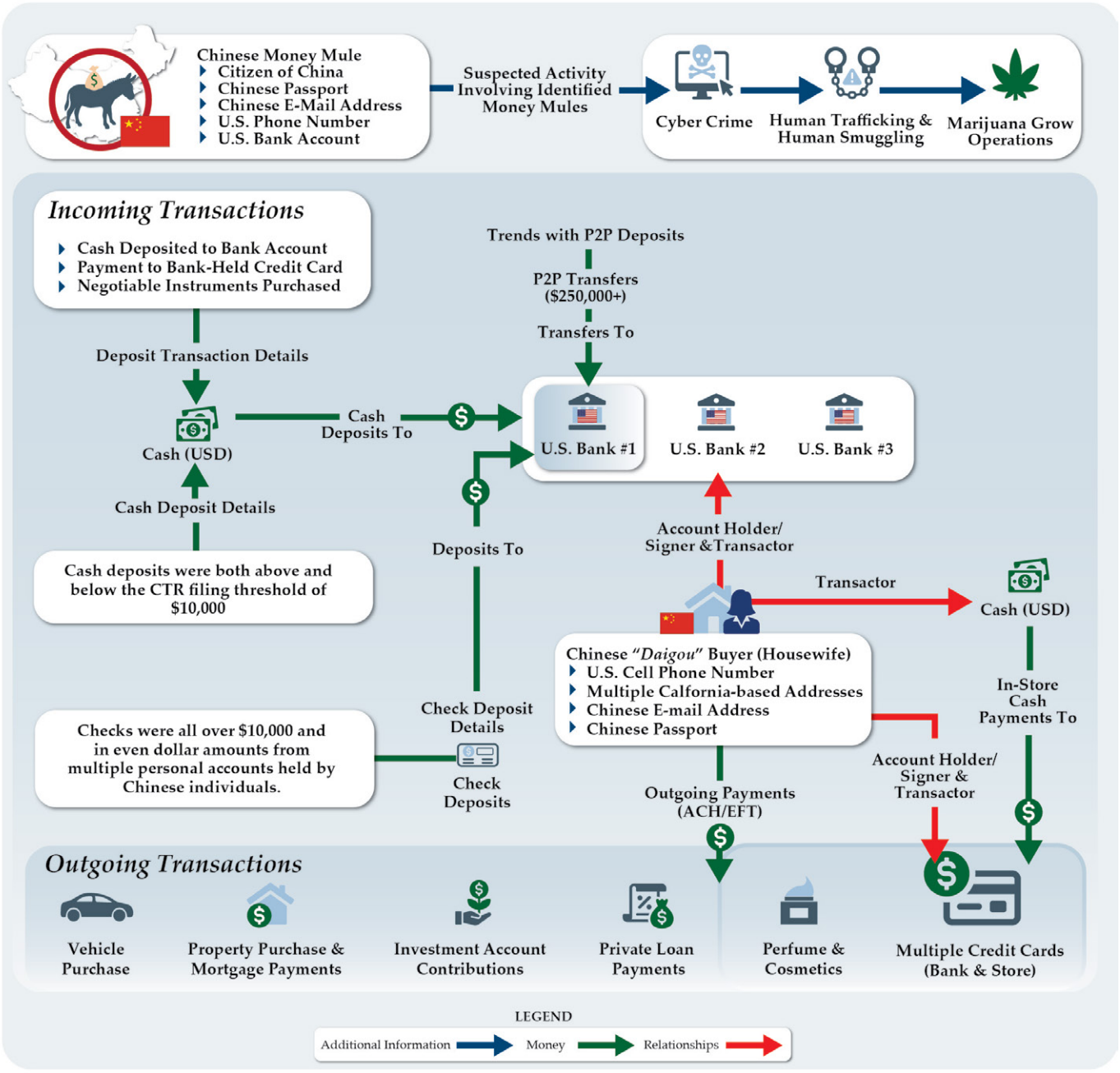
U.S.-based CMLNs likely recruit individuals in the United States to purchase high-value electronics and luxury goods for export to the PRC and other regions, as part of money laundering schemes. CMLNs appear to recruit both witting and unwitting Chinese national students in the United States to serve as buyers, partly due to their familiarity with *daigou* and their need for USD while studying and residing in the United States. The term *daigou* means "buying on behalf of," and it refers to an informal arrangement where buyers, mainly using messaging platforms popular in the PRC, connect PRC-based consumers with products from abroad.[15] These goods are sold for profit, with proceeds then used to replenish overseas bank accounts that support CUBS activities. Additionally, U.S.-based daigou networks require large amounts of U.S. currency to facilitate ongoing purchases, which brings them into contact with CMLNs, who have access to bulk U.S. currency available for sale.

Chinese nationals involved in *daigou* have been observed using credit cards to purchase luxury items and obtaining cash from CMLNs to make payments towards account balances. Filers also identified payments involving P2P and automated clearing house (ACH) transactions between parties within an unknown relationship. *Daigou* buyers also benefit from using credit cards to accumulate reward points, which can be used for travel or exchanged for USD payment. These buyers often maintain vast networks of customers and promote offerings through social media or gray-market Chinese language e-commerce platforms, which can have upwards of 150 million active users.[16] The growth of digital technology and communication has made *daigou* transactions more efficient, with many being handled through CUBS, allowing the practice to operate outside official PRC currency channels.

FinCEN analysis of the dataset identified the term "*daigou*" in a small number of BSA reports totaling approximately $9.6 million in reported suspicious activity.[17] Additionally, the term "credit card" was identified in 16,799 BSA reports totaling a reported suspicious activity amount of approximately $19 billion. In the reports, filers observed high volumes of items purchased and a high frequency of purchases that far exceeded typical personal use. In some cases, the filer's customer stated that they were buying items for friends and family in the PRC because the items were much cheaper in the United States.

15. *See* "Chinese Daigou shoppers represent a new type of entrepreneur," *Queensland University of Technology*, 15 June 2023, https://phys.org/news/2023-06-chinese-daigou-shoppers-entrepreneur.html.
16. *See* "Focus: 'Daigou' goes corporate as retailers seek new ways to reach Chinese shoppers," *Reuters*, 21 December 2023, https://www.reuters.com/business/retail-consumer/daigou-goes-corporate-retailers-seek-new-ways-reach-chinese-shoppers-2023-12-21/.
17. In addition to the 18 BSA reports that reference *daigou*, FinCEN also identified several key terms that are often associated with *daigou* activity within a larger subset of the total dataset.

Figure 5. Reported Incoming Financial Transactions for Identified U.S.-Based Daigou Shopper



Potential Human Trafficking- and Human Smuggling-Related Activity Linked to CMLNs Involving U.S.-Based Chinese Nationals

Financial institutions filed 1,675 BSA reports involving suspicious financial activity potentially related to human trafficking or human smuggling within the dataset.[18] The amount of reported suspicious activity totaled approximately $4.2 billion, with depository institutions reporting approximately 95 percent of these BSA reports. Financial institutions flagged FinCEN's Advisories issued in 2014 and 2020 regarding human trafficking- and human smuggling-related financial activities, as well as an Alert specific to human smuggling along the U.S. southwest border, in 1,166—or approximately 70 percent—of the human trafficking- or smuggling-related BSA reports (1,675) in the dataset.[19] [20] [21]

Financial institutions frequently reported suspicious P2P credit and debit activity, rapid incoming and outgoing wire transfers, and cash deposits followed by cashier's check or money order purchases. The activity often involved funds transfers to businesses frequently used by human traffickers for labor or sex trafficking, including massage businesses, spas, escort services, and restaurants or bars.[22] In one case, a Chinese national was indicted on human trafficking charges related to commercial sex operations at illicit massage parlors in Michigan. The individual was charged with money laundering, keeping a house of prostitution, and conducting a criminal enterprise, among others, facing up to 75 years in prison, if convicted.[23]

18. The U.S. Department of the Treasury's 2024 National Strategy for Combating Terrorist and Other Illicit Financing highlights human trafficking as a key illicit threat to the U.S. financial system. CMLNs often launder the proceeds derived from human trafficking activity through front companies, frequently with the goal of gaining access to USD to evade China's currency restrictions. Front companies commonly used for human trafficking activities include massage businesses, escort services, restaurants, and bars. These types of businesses are vulnerable to human trafficking due to their cash-intensive nature, as well as the opportunity for exploitation of one's services or labor. *See* "2024 National Strategy for Combating Terrorist and Other Illicit Financing," U.S. Department of the Treasury, May 2024, https://home.treasury.gov/system/files/136/2024-Illicit-Finance-Strategy.pdf. *See* "China in Our Backyard: How Chinese Money Laundering Organizations Enrich the Cartels," House Committee on Oversight and Accountability, Subcommittee on Health Care and Financial Services, 26 April 2023, https://oversight.house.gov/wp-content/uploads/2023/04/Hearing-on-Chinese-Money-Laundering-Mavrellis-Written-Testimony-4.26.2023-FINAL.pdf.
19. *See* "Guidance on Recognizing Activity that May be Associated with Human Smuggling and Human Trafficking – Financial Red Flags," FinCEN Advisory #FIN-2014-A008, 11 September 2014, https://www.fincen.gov/sites/default/files/advisory/FIN-2014-A008.pdf.
20. *See* "Supplemental Advisory on Identifying and Reporting Human Trafficking and Related Activity," FinCEN Advisory #FIN-2020-A008, 15 October 2024, https://www.fincen.gov/sites/default/files/advisory/2020-10-15/Advisory%20Human%20Trafficking%20508%20FINAL_0.pdf.
21. *See* "FinCEN Alert on Human Smuggling along the Southwest Border of the United States," FinCEN Alert #FIN-2023-Alert001, 13 January 2023, https://www.fincen.gov/sites/default/files/shared/FinCEN%20Alert%20Human%20Smuggling%20FINAL_508.pdf.
22. *See* "Supplemental Advisory on Identifying and Reporting Human Trafficking and Related Activity," FinCEN Advisory #FIN-2020-A008, 15 October 2024, https://www.fincen.gov/sites/default/files/advisory/2020-10-15/Advisory%20Human%20Trafficking%20508%20FINAL_0.pdf.
23. *See* "Chinese National to Stand Trial on Human Trafficking Charges," Michigan Department of Attorney General Press Release, 7 January 2025, https://www.michigan.gov/ag/news/press-releases/2025/01/07/chinese-national-to-stand-trial-on-human-trafficking-charges; *see also* Register of Actions, *State of Mich. v. Piao*, No. 25-88-01-FH (Third Judicial Circuit of Mich.), https://cmspublic.3rdcc.org/CaseDetail.aspx?CaseID=4129932.

- One filer reported numerous incoming checks and P2P transfers to an alleged booking website for massage companies referencing "advertisements"; however, a majority of the clients sending the funds were also listed on adult advertising sites. The financial institution also reported that the adult advertisements on the sites included keywords like "girl" or "young," which may indicate massage services provided by a minor. The massage businesses are owned by Chinese nationals or individuals who may be permanent U.S. residents or U.S. citizens.

CMLNs Potentially Using Adult Daycare Centers Located in New York to Further Laundering Activities; Also Linked to Suspected Healthcare Fraud, Elder Abuse, and Illicit Gaming Activity

Financial institutions filed 43 BSA reports in the dataset involving approximately $766 million in suspicious activity on 83 New York-based adult and senior day care centers ("senior facilities"), which identified the owner and/or account signer as using a Chinese passport. Senior facilities offer protective care and supervision for dependent adults, ranging from medical services to social and recreational activities.[24]

- Filing institutions reported suspicious activity involving senior facilities in New York for allegedly defrauding Medicaid, Medicare, or private insurance companies by billing for services that were not provided. CMLNs often moved fraudulent proceeds through accounts held by individuals, unrelated businesses, and overseas companies to facilitate other criminal activity and TBML schemes. The senior facilities potentially exploit the Medicaid-eligible elderly population by offering cash, gift cards, or other financial incentives to enroll in their services.

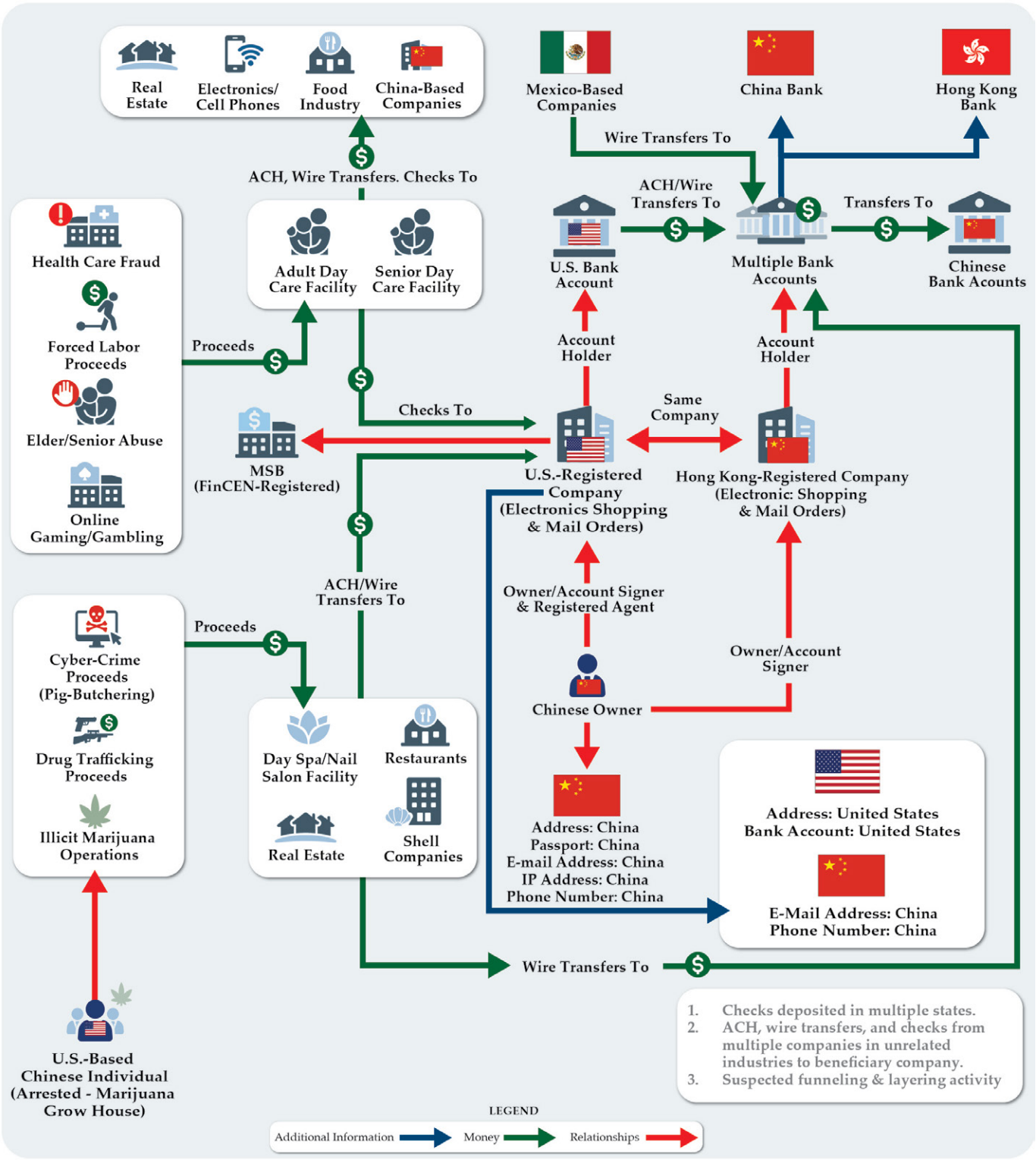
FinCEN identified multiple BSA reports in the dataset involving companies receiving funds from the adult daycare companies that identified the owner and account signer of the company as Chinese national students. In one example, 34 BSA reports were filed on one Chinese student and his established company that in aggregate were associated with more than $168 million in activity over the review period. The reported activity included large cash deposits, purchases of cashier's checks payable to unknown third parties, and suspicious incoming checks and transfers from unrelated businesses. FinCEN also identified 101 BSA reports listing the student as the transactor, exceeding $5.5 million in cash deposited over a two-year period.

FinCEN also identified 108 BSA reports in the dataset involving deposited funds potentially associated with healthcare fraud, elder abuse, and suspicious gaming activity. The filers reported the activity as indicative of money laundering because the businesses were moving funds at an excessive and unnecessary rate, while noting that the funds were not linked to typical operational expenses. The volume of certain types of outgoing transactions was deemed suspicious and inconsistent with business-related expenses. Identified transactions consisted of cash withdrawals, P2P transactions, wire transfers, checks, ACH, cashier's checks, and teller transfers, and involved the following examples of suspicious activity:

24. *See* "Testimony of the New York State Adult Day Services Association (NYSADSA) to the Joint Budget Committee on Health," New York State Senate, 8 February 2022, https://www.nysenate.gov/sites/default/files/nys_adult_day_services_assoc.pdf.

- Outgoing large even-dollar payments were sent to companies with addresses in Hong Kong or the PRC but utilizing a U.S. bank account to receive the funds. The filers reported that these companies' business profiles were unrelated to the healthcare industry.
- Outgoing checks and payments to companies in the construction, home improvement, real estate-related industry.
- Outgoing payments to suspected shell companies, where the funds were sent to companies associated with cell phones, electronics, precious metals, and logistics.

Figure 6. Flow of Funds Involving Potentially CMLN-Linked Adult Daycare Facilities



CMLNs Potentially Facilitating Real Estate Purchases Funded by Illicit Proceeds from a Variety of Financial Crimes

Financial institutions filed 17,389 BSA reports associated with more than $53.7 billion in reported activity that identified transactions involving the real estate sector, accounting for approximately 13 percent of the BSA reports in the dataset. Chinese nationals residing in the PRC generally are not permitted to purchase real property in the United States, as indicated on a PRC government website.[25] According to a Homeland Security Investigations (HSI) Bulletin, Chinese citizens seeking to evade these restrictions and purchase or invest in property in the United States may use alternate mechanisms to transfer funds from the PRC to the United States—such as CUBSs—through a U.S.-based CMLN broker, who can facilitate the often-large payments involved in real estate transactions.[26] BSA reports identified Chinese nationals making large cash deposits used to purchase cashier's checks that were made payable to third parties, and further deposited into another account, often at a different financial institution. Cashier's checks purchased with large cash deposits and consolidated to purchase larger cashier's checks and used to purchase real estate were common in the dataset of BSA reports. Additionally, the pooling of funds for the purchase of real estate is consistent with red flags associated with money laundering through real estate acquisitions.[27]

- BSA reports identified the suspected involvement of CMLNs to move cash through various intermediaries, converting the cash into cashier's checks, and then using those checks to purchase real estate, often for individuals in the PRC attempting to move wealth outside of the PRC.

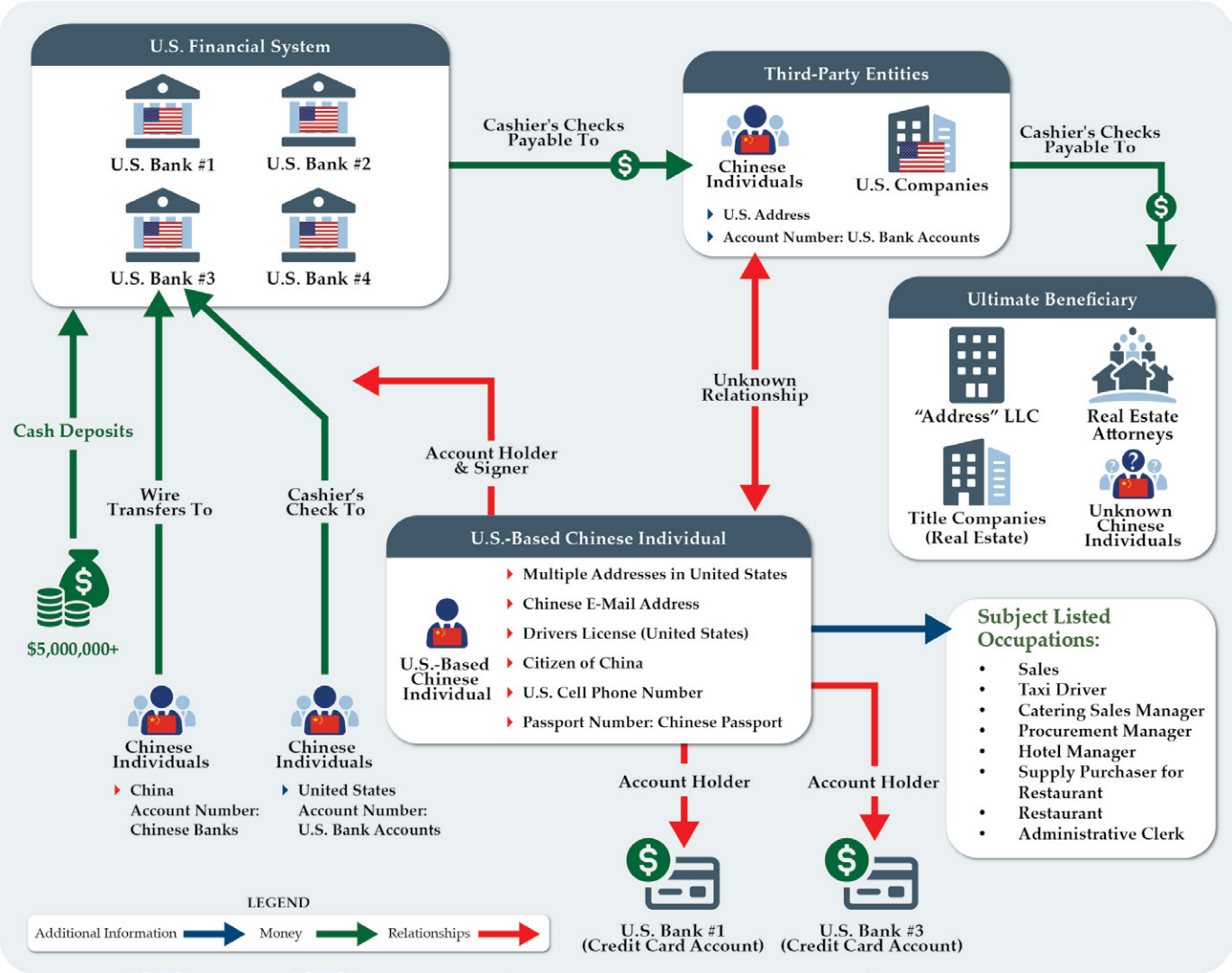
BSA reports in the dataset also frequently identified suspicious incoming wire transfers used to purchase real estate, which were possibly indicative of evading the PRC's currency restrictions, to U.S.-based accounts held by individuals or companies, owned by Chinese nationals. The BSA reports identified that the wire deposits were received from individuals in the PRC who were reported as family members. In other BSA reports, the financial institutions could not determine the relationship with the account holder.

- Financial institutions reported that they requested additional information for these transfers, but customers were often unable to provide any supporting documentation that would sufficiently verify the source of the funds and the relationship to the originator. When subjects did provide explanations, the most frequently cited reasons were to purchase real estate and tuition payments.

25. *See* https://www.safe.gov.cn.
26. *See* "Chinese Money Laundering Organizations (CMLOs) – Use of Counterfeit Chinese Passports," U.S. Department of Homeland Security Investigations Cornerstone Issue #48, 2 January 2024, https://content.govdelivery.com/accounts/USDHSICE/bulletins/37fff16.
27. *See* "Advisory to Financial Institutions and Real Estate Firms and Professionals," FinCEN Advisory #FIN-2017-A003, 22 August 2017, https://www.fincen.gov/sites/default/files/advisory/2017-08-22/Risk%20in%20Real%20Estate%20Advisory_FINAL%20508%20Tuesday%20%28002%29.pdf.

FinCEN analysis identified U.S.-based Chinese nationals engaging with suspected CMLNs, laundering illicit proceeds through the purchase of real estate from various business sectors involved with property ownership, to include construction, remodeling, real estate agents or brokers, and property management companies. BSA reports identified suspicious activity in the accounts of these companies, which appeared to be affiliated with CMLNs engaged in suspected criminal activity including marijuana distribution, health care fraud, laundering of drug trafficking proceeds for Mexican cartels, and distribution of counterfeit vaping products.

Figure 7. Real Estate Purchases Involving CMLN "Money Mules"



CMLNs May Use Chinese Students to Engage in a Variety of Suspicious Financial Activities and Schemes

Financial institutions filed approximately 20,282 BSA reports—or 14 percent of the total dataset—that referenced individuals purporting to be Chinese students during the review period. These 20,282 BSA reports accounted for approximately $13.8 billion in reported suspicious activity, with an average amount of approximately $680,000 per filing, and a median amount of approximately $87,000 per filing. Depository institutions filed the majority of the suspicious activity amount, totaling approximately $11.8 billion; securities and futures firms reporting the second highest dollar amount, totaling approximately $1.6 billion in reported suspicious activity. Casinos, MSBs, insurance companies, and loan/finance companies reported approximately $254 million in suspicious activity combined.

Chinese students may be vulnerable to recruitment and exploitation as money mules by U.S.-based CMLNs, which need access to, and control of, many bank accounts to facilitate frequent cash deposits to place illicit proceeds into the U.S. financial system, according to FinCEN analysis of the dataset. U.S.-based Chinese students potentially "lend" their accounts to CMLNs, typically in exchange for a fee, which varies based on the amount of money the CMLNs transact through the student's account, according to FinCEN analysis of the dataset and law enforcement information. The fees likely incentivize students to open accounts at multiple depository institutions, and other forms of accounts such as credit cards, according to FinCEN analysis of the dataset and law enforcement information.

FinCEN analysis of the dataset highlighted numerous suspicious financial transaction patterns conducted by U.S.-based Chinese students, former and current, over an extended period. Filers were primarily depository institutions, MSBs, and casinos, which frequently reported suspicious, unsourced, and excessive P2P transfers, large cash-in transactions at casinos, significant casino gaming activity with no reported employment, luxury purchases with unsourced funds, and the possible laundering of illicit narcotics proceeds.

- Financial institutions filed 87 BSA reports on one individual, exceeding $22 million in suspicious transactions, with filing dates ranging from 2010 to 2024. Casinos reported 85 of these BSA reports, which cited unusual gaming practices and suspicious chip walking activity.[28] The BSA reports do not mention the subject as a student, but filers reported the individual in a BSA report as early as 2007, where "student" was the listed occupation.
- Twelve financial institutions filed 34 BSA reports on an individual totaling over $81 million in suspicious activity between 2015 and 2024. The subject is listed as a student in 15 of the BSA reports, with four different California-based colleges listed as the place of study. Filers reported

28. Chip walking occurs when a casino patron leaves with gaming chips in his or her possession without redeeming the chips for cash or using them for chip buy-ins at other gaming tables. See "Anti-Money Laundering Program Effectiveness, Docket Number FINCEN-2020-0011, Regulatory Identification Number 1506-AB44," *American Gaming Association*, 16 November 2020, https://www.americangaming.org/wp-content/uploads/2021/08/AGA-Comment-to-ANPRM-re-AML-Program-Effectiveness-FINAL.pdf.

potential money mule activity, incoming high-dollar wire transfers from the PRC, high-end luxury purchases with unsourced funds, and financial transactions consistent with mass marketing scam activity.

The information in this report is based on CMLN-related information obtained from analysis of BSA data, and open-source publications, as well as insights from law enforcement and other partners. FinCEN welcomes feedback on this report, particularly from financial institutions. Please submit feedback to the FinCEN Regulatory Support Section at www.fincen.gov/contact.

Appendix:

Appendix A: TBML Scheme Involving CMLN Acquisition of Cell Phones for Export