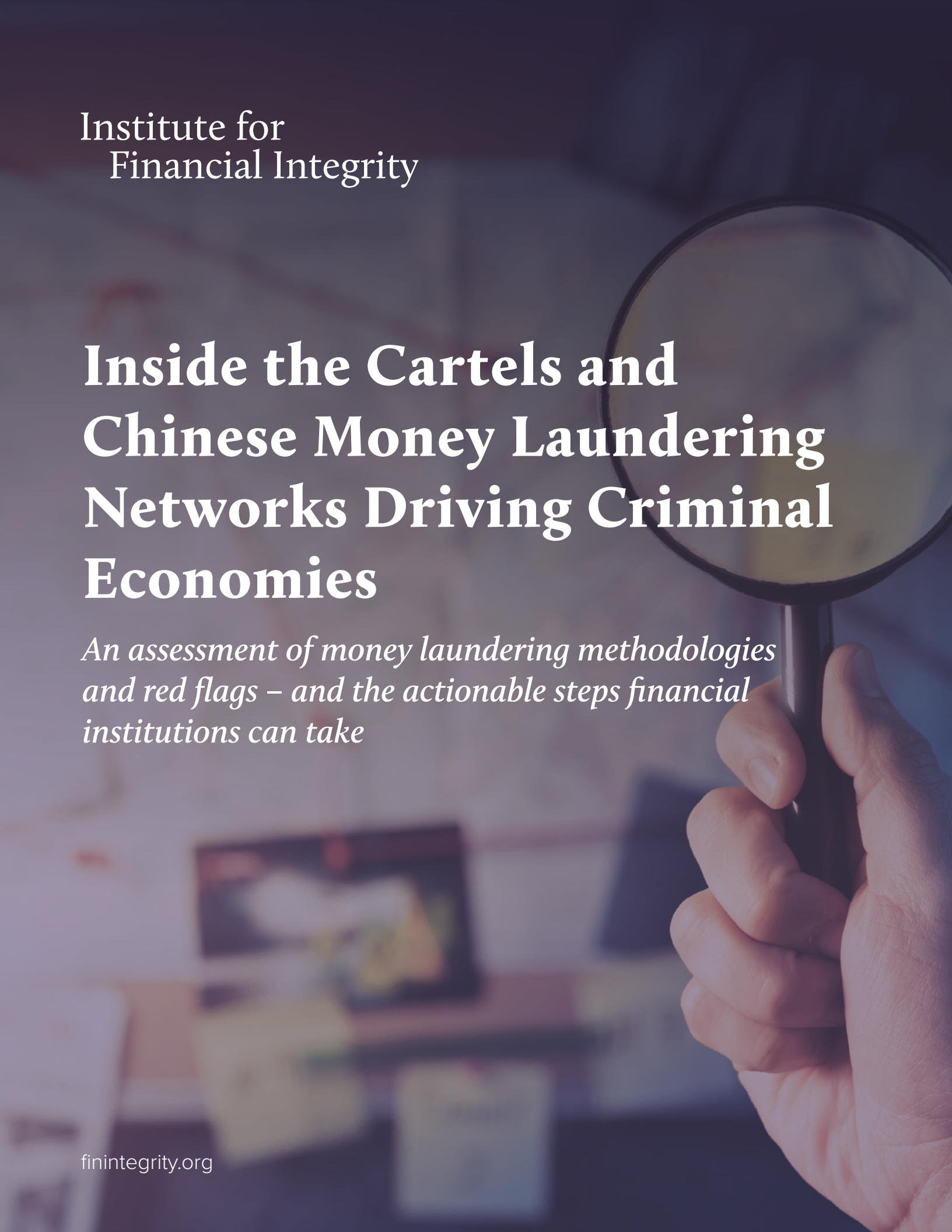
Institute for
Financial Integrity

Inside the Cartels and Chinese Money Laundering Networks Driving Criminal Economies

An assessment of money laundering methodologies and red flags – and the actionable steps financial institutions can take

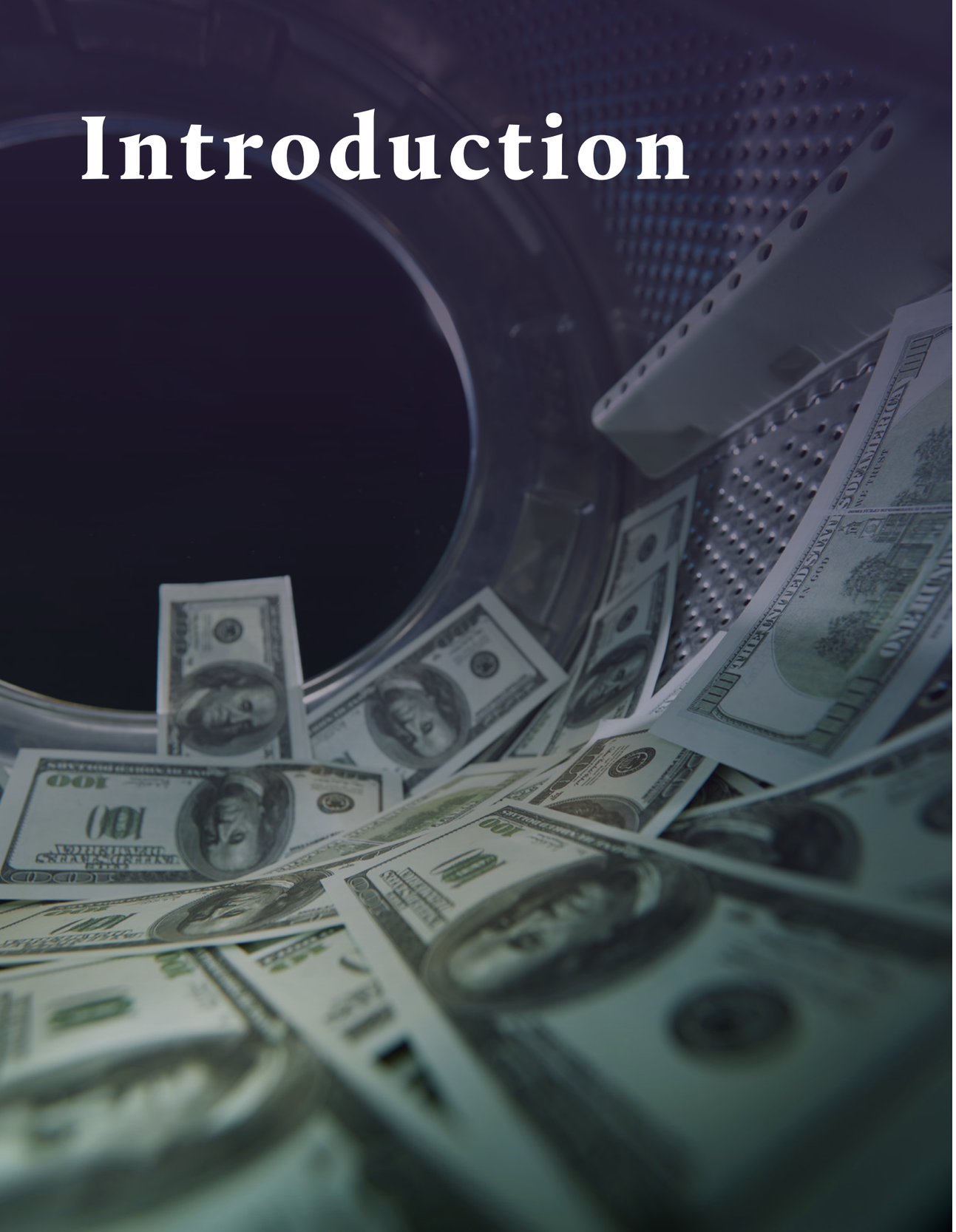


finintegrity.org

Table of Contents

Inside the Cartels and Chinese Money Laundering Networks Driving Criminal Economies

Chinese capital flight amplifies financial crime globally by driving demand for USD and other currencies outside China. It provides a "market opportunity" for Chinese Money Laundering Networks to profit by servicing cartel requirements to launder billions of dollars in illicit proceeds from narcotics trafficking, human exploitation, environmental destruction, economic harm, and other destructive enterprises.



Introduction

Globally, $800 billion-$2 trillion is laundered each year, representing 2-5% of GDP, based on estimates from the United Nations Office on Drugs and Crime (UNODC). The criminality that generates these revenues, and the subsequent laundering process, drive violence and harm across the communities in which organized criminal groups operate: locations where illicit proceeds are generated, transit routes, markets, and those where laundering occurs. More than 80% of the world's population live in countries with high crime, according to a 2023 report from the Global Initiative Against Transnational Organized Crime.

In the United States, in February 2025 the U.S. State Department designated six Mexican cartels as Foreign Terrorist Organizations and Specially Designated Global Terrorists. This signaled the U.S. Government's committed intention to counter cartels and their support networks, and indicated that financial institutions must ensure they are taking action against cartel financing. Section 1 of this report describes the designated cartels, their operational areas, sources of funding, and money laundering methods.

In the continued professionalization of laundering, Chinese Money Laundering Networks (CMLNs) are taking an increasingly significant role in laundering cartel proceeds. Driven by capital flight from China, which is estimated at $516 billion per year, CMLNs match demand from Chinese nationals for USD and other currencies with the immense supply of cartel cash that needs to be laundered. Offering competitive pricing, fast execution, and sometimes guarantees of delivery, CMLNs parallel legitimate financial institutions in global scale, reach, and range of services.

Cartels have expanded from their well-established sources of revenues from narcotics trafficking, and now generate illicit funds from diverse activities including human trafficking and smuggling, wildlife trafficking and illegal fishing, illegal mining and mineral smuggling, fuel theft and oil smuggling, service fees and corruption at ports, extortion and "taxation" of local economies, weapons trafficking and arms procurement, fraud, and more. Section 2 outlines these methods and key global and national data on their scale.

The methods used to launder these funds are equally diverse. Traditional methods such as casinos, trade-based money laundering, real estate and other high-value assets, gold and precious stones, shell and front companies, complicit professionals, and bulk cash continue to be used. However, new methods are increasingly used too.

- CMLNs use “mirror transfers” to move value without cross-border wires, reducing the risk of detection, and requiring financial institutions to adapt their methods to identify the touchpoints that remain to the financial system.
- More crypto is seized than cash by the Drug Enforcement Administration (DEA), and crypto is integrated throughout the illicit product lifecycle.
- Daigou, or “buying on behalf of”, uses purchases of luxury and high-value goods to move value, financed by cartel proceeds and enabled by CMLNs.
- To resource their laundering operations, CMLNs often target Chinese students to become money mules, using cultural obligations and gambling debts from illegal casinos to induce involvement in criminal activity.

These typologies are integrated and combined to provide flexible, adaptive money laundering that can move funds at speed and scale. Section 3 outlines these money laundering methodologies and describes the emergence of CMLNs, followed by Sections 4 - 8 which provide detailed analyses of specific methods including real-life case studies and red flags.

Illicit proceeds are used to finance cartels’ criminal enterprises, acquire assets such as real estate to generate further revenues and facilitate laundering, finance lifestyles of cartel members, and gain influence within political and economic structures. Section 9 outlines the uses of illicit funds and how they further criminal activity.

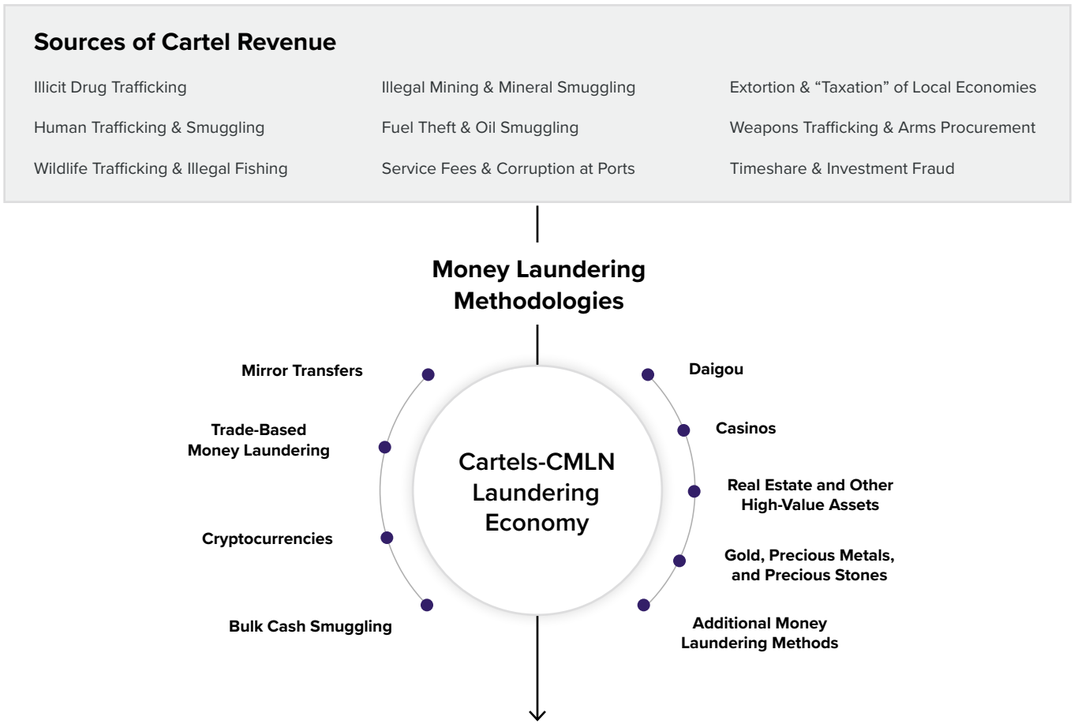
Financial institutions have a critical responsibility and the capability to take action in response. However, this can only be achieved with a comprehensive, effective, and coherent counter-illicit finance program.

- The institutional risk assessment must be adapted and maintained to specifically address cartel and CMLN risks, adapted for that specific business’ exposure based on their geographies, clients, and products.
- The institution must ensure its processes and systems are adapted to the emerging methodologies used by cartels and CMLNs, such as mirror transfers and daigou.
- Training must be customized based on the roles of staff to enhance engagement and retention.
- The institution must monitor alerts and advisories – and take action on them.
- Finally, partnership between the public and private sector is critical to a joint and effective response, both bilaterally and as part of more formal partnerships.

Section 10 sets out the actions for financial institutions at the strategic level, complementing the detailed red flags from earlier sections.

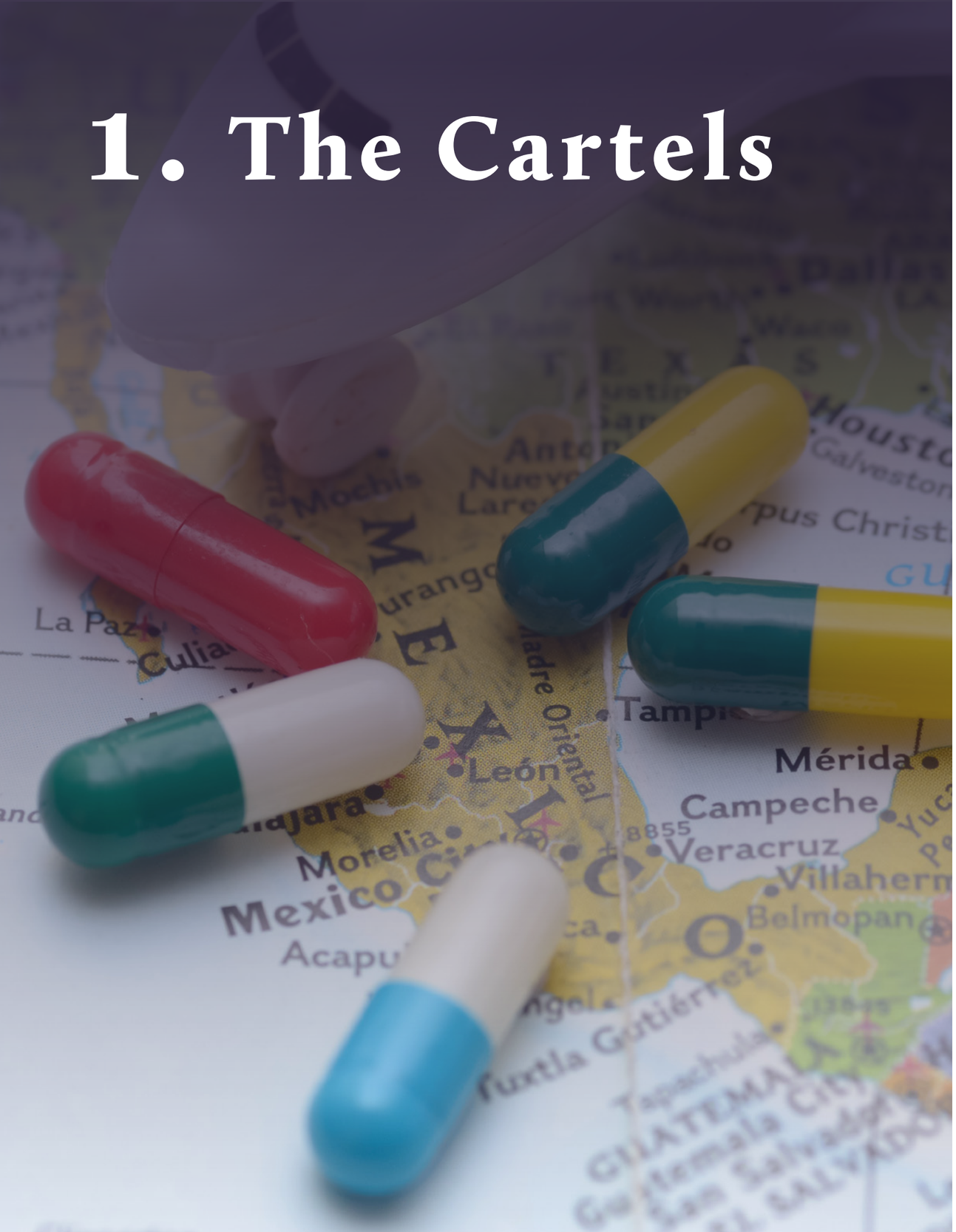
Cartels, CMLNs, and their illicit financing represent not only a threat to the integrity of the financial system, but also drive a cycle of violence, harm, and corruption in communities globally. Financial institutions are expertly well-positioned to disrupt this cycle, and this report provides actionable resources for them to use.

Figure 1: Cartel and CMLN Revenue Sources, Laundering Methodologies, And Uses Of Illicit Funds



Source: Analysis by the Institute for Financial Integrity using open sources

1. The Cartels



An estimated $800 billion-$2 trillion is laundered globally each year, representing 2-5% of global GDP, according to estimates from the United Nations Office on Drugs and Crime (UNODC). In the United States, the FBI assesses that more than $300 billion is laundered each year. The scale of criminal financial activity is immense.

In February 2025, the U.S. State Department designated six Mexican drug cartels as Foreign Terrorist Organizations (FTOs) pursuant to section 219 of the Immigration and Nationality Act, and as Specially Designated Global Terrorists (SDGTs) pursual to Executive Order 13224:

1. Sinaloa Cartel
2. Jalisco New Generation Cartel
3. Northeast Cartel
4. Gulf Cartel
5. New Michoacan Family
6. United Cartels

While many cartels and their supporters were already designated, designation as FTOs/SDGTs increases the risks and consequences of dealing with these groups. For example, designation as an FTO means that U.S. persons that knowingly provide “material support” can be charged under criminal law, and designation as a SDGT means that Treasury can impose secondary sanctions on financial institutions that knowingly engage in significant transactions with the designated cartels.

Since the FTO/SDGT designations, the Treasury Department has rolled out more than 10 tranches of designations of over 100 targets associated with these cartels.

The Treasury Department, State Department, Drug Enforcement Administration (DEA), Homeland Security Investigations (HSI), Federal Bureau of Investigations (FBI), Customs and Border Protection (CBP), Department of Justice, and others have coordinated a “whole-of-government” effort to use all available tools to counter cartels and their support networks.

The cartels operate not just in Mexico and the United States: their supply chains, markets, and money laundering operations destabilize countries globally.

The following table summarizes key operational data for the cartels designed by the U.S. government as FTOs/SDTGs in 2025. It outlines their geographic reach, sources of funding, and money laundering methods.

Figure 2: Cartel Operations

Foreign Terrorist Organization	Operational Areas in Mexico	Operational Areas outside Mexico	Sources of Funding	Money Laundering Methods
Sinaloa Cartel	Sinaloa Sonora Chihuahua Durango Others Port of Mazatlan	Almost all 50 U.S. states, most notably: Arizona California Florida Georgia Illinois Texas At least 40 countries worldwide	Drug trafficking Human smuggling Wildlife trafficking Fuel theft / oil smuggling Extortion Weapons trafficking Prostitution	Chinese money laundering networks Trade-based money laundering Cryptocurrencies Bulk cash smuggling Shell and front companies, such as restaurants, real estate, and agriculture Structuring
Jalsico Cartel	Jalisco Colima Guerrero Michoacán Guanajuato Others Ports of Manzanillo, Lázaro Cárdenas, and Veracruz	Almost all 50 U.S. states, most notably: California Colorado Florida Georgia Illinois Missouri Texas At least 40 countries worldwide	Drug trafficking Human smuggling Fuel theft / oil smuggling Services fees at ports Extortion of farmers Weapons trafficking Real estate schemes	Chinese money laundering networks Trade-based money laundering Cryptocurrencies Bulk cash smuggling Real estate investments Shell and front companies Money services businesses Structuring
Gulf Cartel	Tamaulipas Nuevo Leon Coahuila Veracruz Mexico City Others Port of Altamira	16 states, including: California Nebraska New York Oklahoma Pennsylvania Texas Virginia Upper Midwest Southeastern U.S.	Drug trafficking Human smuggling Illegal fishing Fuel theft / oil smuggling Extortion Weapons trafficking Kidnapping Counterfeit products	Trade-based money laundering Bulk cash smuggling Shell and front companies Money services businesses Structuring Properties and vehicles Gas stations
Northeast Cartel	Tamaulipas Nuevo Leon Zacatecas Mexico City Others	Texas Georgia Oklahoma Upper Midwest	Drug trafficking Human smuggling Fuel theft / oil smuggling Extortion Kidnapping Vehicle theft Prostitution Armed robbery	Trade-based money laundering Shell and front companies Cash-intensive businesses Horse-racing business
New Michoacán Family	Michoacán Guerrero Port of Lázaro Cárdenas (contested with Jalisco Cartel)	~1/3 of U.S. states, including: Georgia New Mexico North Carolina Texas	Drug trafficking Human smuggling Illegal mining Extortion Weapons trafficking Kidnapping	Trade-based money laundering, including through used clothing stores Bulk cash smuggling Shell and front companies Money services businesses Black-market peso exchange
United Cartel	Michoacán, especially Tepalcatepec	~1/3 of U.S. states, including: California Colorado Georgia Illinois Missouri Texas Distribution network spans to Europe, Australia, and other regions	Drug trafficking Extortion, including of lime and avocado farmers Illicit economies across Michoacán's Tierra Caliente region	Unknown

Source: Analysis by the Institute for Financial Integrity using open sources

The Big Two: Sinaloa and Jalisco Cartels

According to the DEA, the two most important FTOs are the Sinaloa and Jalisco New Generation Cartels: they are at the heart of the fentanyl crisis and have a presence across the United States. In Mexico, they are based out of the states from which they derive their names (Sinaloa and Jalisco), but they exercise control and influence beyond those areas, including at multiple maritime ports, to help facilitate their shipments and raise revenue. In addition, the "big two" cartels operate extensive global supply chains, from precursor chemicals to production facilities, and direct complex networks that include international shippers, cross-border transporters, corrupt officials, tunnel builders, shell companies, and money launderers.

- The Sinaloa Cartel is one of the most powerful drug cartels and one of the largest producers and traffickers of fentanyl and other illicit drugs to the United States. It controls and operates extensive transnational networks to facilitate the procurement and shipment of precursor chemicals from China and India to synthesize synthetic drugs in Mexico-based clandestine laboratories. The organization is divided into two main factions: "Los Chapitos," led by the sons of Sinaloa Cartel co-founder "El Chapo," and "Los Mayos," led by the sons of Sinaloa Cartel co-founder "El Mayo"
- The Jalisco New Generation Cartel (a.k.a. Cartel Jalisco Nueva Generacion, or CJNG) is one of Mexico's most powerful, influential, and violent criminal organizations and a key supplier of illicit fentanyl to the United States. The organization operates under a franchise business model overseen by Ruben "El Mencho" Oseguera-Cervantes, and maintains a financial arm known as "Los Cuinis" that leads its diverse network of money laundering operations.

The Northeasterners: Gulf and Northeast cartels

The Gulf Cartel and Northeast Cartel are both based in the Mexican state of Tamaulipas, which is in the northeastern corner of Mexico bordering Texas.

- The Gulf Cartel (a.k.a. Cartel del Golfo, or CDG) is one of Mexico's oldest and most notorious criminal groups. It has moved arms, drugs, and migrants into the United States for many years, and was responsible for the kidnapping and murder of American citizens in March 2023. In recent years CDG has lost territory and influence and has splintered into several rival factions. The names of the different factions include Scorpions, Metros, Cyclones, Rojos, and Panthers.
- The Northeast Cartel (a.k.a. Cartel del Noreste, or CDN), formerly known as the Zetas, originated as an enforcement arm of the Gulf Cartel formed by deserters from the Mexican Army's elite special forces in 1997 and became one of Mexico's most powerful and feared groups circa 2007-2012. Infighting and the loss of key leaders led to the Zetas' decline, and CDN emerged as the most dominant splinter faction.

The Michoacanos: New Family Michoacana and United Cartels

The New Family Michoacana and United Cartels are based in the Mexican state of Michoacán and have been locked in an ongoing battle with the Jalisco Cartel to control drug trafficking routes running through the state and their share in local illicit economies, including drug production and the extortion of avocado producers.

- The New Family Michoacana Cartel (a.k.a. La Nueva Familia Michoacana, or LNFM) has splintered into several factions since the 2000's, some of which have joined forces under the United Cartels banner. In addition to trafficking fentanyl and other drugs to the United States, the group has engaged in acts of terror and violence in Mexico through kidnappings, killings, and extortion.
- The United Cartel (a.k.a. Carteles Unidos, or CU) is a coalition of criminal networks and civilian defense groups that joined forces to resist the Jalisco Cartel's expansion into Michoacán and keep control of the state's drug trade. It is led by "El Abuelo" (Juan Jose Farias Alvarez), the leader of Cartel del Abuelo.

2. Cartel Revenue Sources

Cartels generate revenues from the exploitation of people, wildlife, the environment, trade, and commerce. They drive a cycle of violence and destruction in communities in which they operate, with subsidiaries and supply chains (not just markets) that span the world. In many countries, cartels have pervasive and extensive reach: criminal organizations are the 4th largest employer in Mexico, according to the Atlantic Council. In the West Balkans, South American cartels have strategically inserted themselves at key points in the drug trafficking supply chain, developing a reputation as a reliable transactional partner, rather than attempting to control the entire supply, according to the Global Initiative against Transnational Organized Crime Organized Crime Index 2025.

This section describes some of the key sources of cartel revenues.

Illicit Drug Trafficking

Globally, 316 million people worldwide used drugs in 2023, an increase over the previous year that outpaced population growth, according to the United Nations Office on Drugs and Crime, providing a market for cartel activity – and a significant human cost.

Synthetic opioids, primarily fentanyl, are responsible for the deaths of more than 52,000 Americans each year, with drug overdoses being the leading cause of death for those aged 18-44 years old. The U.S. Department of Homeland Security's Homeland Security Threat Assessment 2025 reported that the Sinaloa Cartel and Jalisco New Generation Cartel are the primary smugglers of fentanyl, methamphetamine, cocaine, and heroin into the United States. While seizures of cocaine and methamphetamine are higher than those of fentanyl, fentanyl is a key concern due to its potency, lethality, and availability.

There are also implications for financial integrity. In 2024, U.S. financial institutions reporting to FinCEN identified approximately $1.4 billion in suspicious transactions potentially linked to fentanyl-related activities, including precursor chemical procurement, fentanyl trafficking, and associated money laundering.

Global:
316 Million
people worldwide who used drugs in 2023

United States:
$1.4 billion
suspicious transactions potentially linked to fentanyl in 2024

United States:
52,000
deaths from synthetic opioids per year

Human Trafficking and Smuggling

Human trafficking and smuggling are distinct but closely related. Human smuggling involves transporting individuals illegally across an international border and is voluntarily undertaken by the individual being smuggled. Human trafficking involves exploiting men, women, and children for the purposes of forced labor or sexual exploitation – using force, fraud, or coercion – and does not necessarily involve movement or transport. However, smuggled individuals are also vulnerable to trafficking. For example, smugglers may extort migrants for additional fees, coerce them into exploitative labor to pay off debts for transport, or use threats relating to their unlawful immigration status to further exploitation.

As an indicator of global scale, human trafficking in the private economy generates US$236 billion in illegal profits per year, according to the United Nations International Labor Organization. Cartels are estimated to have generated $13 billion from human smuggling in 2021. Fees per migrant to cross the U.S.-Mexico border average $8,000-$12,000 for land crossings and $12,000-$20,000 for water crossings, though they may be as low as $400-$500 for border crossings in large groups of 200-300 people.

Global:
$236 billion
illegal profits from human trafficking

Cartels:
$13 billion
revenues from human smuggling in 2021

$400-$20,000
fees per migrant for crossing the Mexican-United States Border

Wildlife Trafficking and Illegal Fishing

Trafficking in wildlife is estimated to be the 4th-largest organized crime globally, after drug trafficking, human trafficking, and counterfeiting. “Wildlife” includes all wild animals and plants including birds, fish, timber, and forest products, in violation of international and national laws. It has significant implications for biodiversity and the environment, as well as bringing criminality and violence into communities.

There is significant demand from China for illegal wildlife originating in Mexico including jaguars, reptiles, sea cucumbers, jellyfish, and sharks, for use in “traditional medicine,” for consumption, or to be sold as pets.

Mexico, along with Brazil and Colombia, has the highest instances of wildlife trafficking in Latin America and the Caribbean. Cartels have intervened in these supply networks, adapting narcotics smuggling routes to wildlife too. Wildlife trafficking is highly profitable and lower risk than other types of trafficking, such as narcotics. For example, the bladder of the totoaba fish can be sold for $60,000 on the black market, and Mexican authorities seized more than seven metric tons from 2012-2016, with an estimated value of $420 million.

“FinCEN is calling attention to this threat [illegal wildlife trade] because of: (1) its strong association with corruption and transnational criminal organizations (TCOs)… [and] wildlife trafficking’s contribution to biodiversity loss, damage to fragile ecosystems, and the increased likelihood of spreading of zoonotic diseases… FinCEN assesses TCOs have an increasing role in facilitating the movement of both wildlife and related money laundering because of the increase in the movement of bulk wildlife product using established trade routes consistent with the experience, organization, and sophistication of TCOs. Also, given the profit motivations of TCOs, wildlife trafficking is appealing as it is a low-risk and high-reward crime…” – FinCEN Threat Analysis (2021)

Global:
4th
largest organized crime is the illegal wildlife trade

Cartels:
$1.4 billion
drives demand for illegal wildlife products from countries including Mexico

Illegal Mining and Mineral Smuggling

Illegal mining refers to the extraction of metals, stones, and other materials without the required permits, licenses, land rights, or environmental safeguards. Extractives include gold, silver, iron, coal, diamonds, emeralds, and rare earths. Illegal mining is often associated with organized crime, corruption, fraud, and human trafficking.

Illegal mining is estimated at $12-48 billion globally, according to the United Nations Environment Program and Interpol. It results in deforestation, loss of biodiversity, environmental damage, and harm to human health through the use of toxic materials such as mercury.

In Peru, the illegal gold economy is seven times larger than cocaine trade, and in Querétaro in Mexico, cartels such as the Jalisco New Generation exercise a high degree of control over illegal gold mines.

Gold mining is not just a source of revenue: it also provides cartels with a method to launder illicit proceeds by converting them into another form of value. According to a FinCEN advisory citing the FBI, transnational criminal organizations are exporting illegally extracted gold to the United States to launder billions of illicit proceeds from criminal operations in Latin America.

Global:
$12-14 billion
revenue from illegal mining

Cartels:
x7
illegal gold vs coccaine, in some countries like in Latin America

Fuel Theft and Oil Smuggling

Fuel theft and crude oil smuggling are the most significant non-drug illicit revenue source for cartels, according to an analysis from FinCEN.

Despite being one of the top 15 countries in the world for oil production, Mexico does not have the capacity to refine the crude oil produced by Petróleos Mexicanos (Pemex), Mexico's state-owned energy company, to fully meet the country's needs. Instead, unrefined and partially refined crude oil is exported to the United States and other countries for refining, then the gasoline, diesel, and other fuel is exported back to Mexico.

Cartels exploit both the export and re-import. They illegally acquire crude oil by bribing Pemex employees and government officials, as well as illegally tapping oil pipelines and stealing from refineries. The illicitly obtained crude oil is smuggled across the U.S. border and sold at a discount.

They also smuggle refined products back into Mexico, undercutting the legitimate fuel market. Illegal fuel imports are valued at more than $20 billion per year. The sophistication and scale of cartel oil smuggling continue to increase. For example, in 2025, a tanker docked at the Port of Ensenada on Mexico's Pacific coast. It carried almost 120,000 barrels of diesel which was unloaded directly from the ship to fuel trucks using hoses, a highly risky operation compared with using specialist infrastructure. The activity was assessed as being a "dark fleet" ship operated by cartels to smuggle oil.

Cartels:

2nd

most significant revenue source for cartels, after drug trafficking

Mexico:

$20 billion

illegal fuel imports per year

Service Fees and Corruption at Ports

Where ports are located within cartel-controlled territory, the cartel can extract bribes and "service fees" for customs, logistics, and other port services. Control of ports also facilitates illegal imports and exports such as narcotics, precursors, and fuel. For example, cartel CJNG controls the Mexican state of Colima, which includes the port of Manzanillo. Control of this port enables the cartel to coordinate CJNG's fentanyl precursor procurement and other drug trafficking operations.

Extortion and "Taxation" of Local Economies

Criminal organizations in Mexico extort businesses as well as individuals, demanding "protection payments" or "taxes" in territory within their control. An estimated 4.7 million extortion attempts occurred in Mexico in 2022, and an estimated 97% were not reported to law enforcement, according to the Atlantic Council. For example, cartels have targeted avocado farmers and packing-houses, resulting in losses of hundreds of millions of dollars, equivalent to 10% of each year's national avocado exports.

Weapons Trafficking and Arms Procurement

The Mexican government estimated that 200,000 firearms were smuggled from the United States into Mexico in 2021. These are often acquired by "straw purchasers" or assembled from kits or parts, since traffickers may not be able to pass the background checks necessary to directly buy weapons. An ongoing investigation by the DEA into the Sinaloa cartel has resulted in the seizure of more than 21,000 rounds of ammunition as of January 2025, along with 2,000 kilograms of cocaine and fentanyl, and more than $16 million in cash.

While weapons may generate revenues for cartels, they also have more direct uses: for cartel violence against Mexico's security forces and local communities; in extortion, kidnapping, and murder; and in conflicts between cartels.

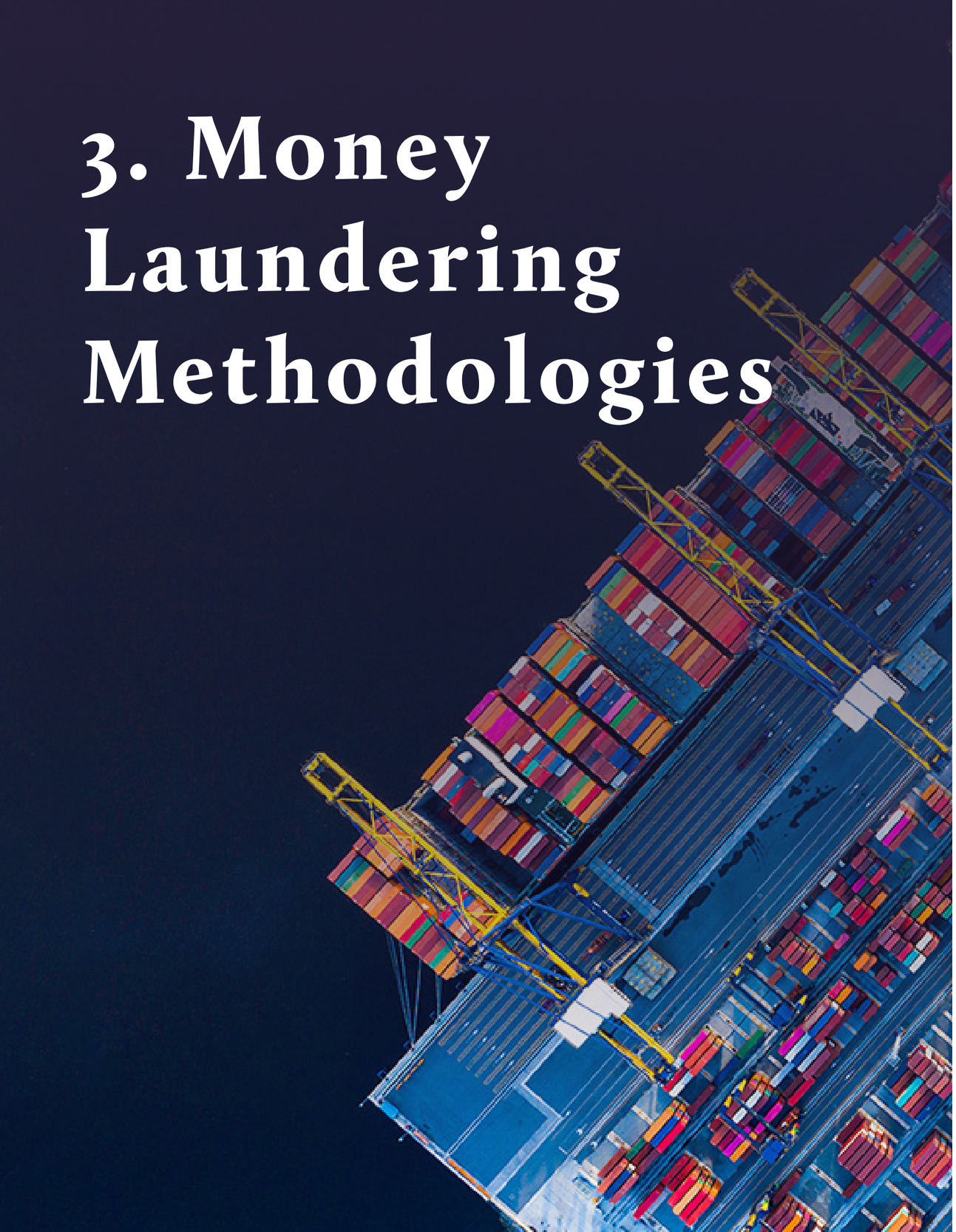
"In the case of arms trafficking, the relationship between violence and organized crime is even more direct. Firearms are not only traded commodities but also essential enablers of crime, conflict and insecurity. Illicitly sourced weapons are crucial tools for organized crime groups, enabling them to intimidate, coerce victims and engage in other crimes." – Global Initiative against Transnational Organized Crime Global Organized Crime Index (2025)

Timeshare and Investment Fraud

To diversify their revenue streams, cartels such as the Jalisco New Generation Cartel (CJNG) are targeting U.S. owners of timeshares in Mexico. The schemes operate from cartel-controlled call centers and engage in lengthy scams purporting to purchase timeshares above market price or rent them out at above market rates. The FBI estimated that more than 6,000 U.S. victims reported losing a total of nearly $300 million between 2019 and 2023 to timeshare fraud schemes in Mexico.

These are some of the key sources of cartel proceeds, and they generate billions in revenue each year. These illicit proceeds must then be laundered. The next section examines laundering methods used by cartels, including the significant role of Chinese Money Laundering Networks.

3. Money Laundering Methodologies



Cartels source their illicit proceeds from multiple types of criminality including trafficking, smuggling, corruption, and fraud. They then seek to launder the funds. Multiple laundering methods are used. Sometimes, the source and money laundering method may be combined. For example, illicit gold provides a source of revenue, and the gold can also be used to launder the proceeds of multiple crimes.

Professional money launderers are increasingly used. Professional money launderers are individuals, organizations, or networks who launder criminal proceeds for a fee or commission. The U.S. Department of Treasury identified in 2024 that drug traffickers are using professional money launderers, in particular Chinese Money Laundering Networks (CMLNs), and that CMLNs have “come to dominate money laundering services” for some drug trafficking organizations.

This section outlines some of the key laundering methods relevant to cartels.

Mirror Transfers

Mirror transfers are an informal value transfer system that moves value across borders without cross-border wire transfers. Each currency stays in its own country, for example the USD stay in the United States and Chinese RMB stay in China. This minimizes detection by financial institutions – though touchpoints remain such as money mules depositing cash into bank accounts, business accounts being used to purchase precursor chemicals, and transactions that indicate funneling and laundering. Mirror transfers and financial system touchpoints are described in detail in Section 4 Focus: Mirror Transfers.

Trade-Based Money Laundering

Trade-based money laundering (TBML) uses trade or commercial financing to disguise the origin and movement of value across international borders, as well as to generate further illicit proceeds. Examples of TBML include overvaluation, undervaluation, double or multiple invoicing, and false description of goods. Further details of these methods and the associated red flags are available from the Financial Action Task Force (FATF) and U.S. Homeland Security Investigations.

Cryptocurrencies (Digital Assets)

Cryptocurrencies – also called digital assets, virtual assets, or cryptoassets – are integrated throughout the "product lifecycle" of illicit activities like fentanyl trafficking, as well as into multiple other predicate offenses and laundering methodologies. The use of cryptocurrencies to acquire materials and launder cartel proceeds is described in detail in Section 5 Focus: Cryptocurrencies (Digital Assets), using fentanyl as the example.

Bulk Cash Smuggling

Cartels smuggle bulk cash generated from illicit activity in the United States back to cartels in Mexico by physically transporting it in vehicles, cargo, or on persons. They may also subsequently use Mexico-based businesses to repatriate the previously-smuggled cash back into the United States using domestic armored car services and air transport. Further detail on these methods and the associated red flags is available from FinCEN.

Casinos

Casinos have been historically used to launder the proceeds of organized crime – and continue to be – often with the involvement of CMLNs. The "Vancouver method," a type of mirror transfer, was used to launder millions of dollars in cash through casinos in Canada, according to the Cullen Commission report (2022), and this and similar methods continue to be identified in multiple countries. Casino-based laundering and red flags are described in detail in Section 6 Focus: Casinos.

Daigou ("Buying on Behalf of")

Daigou, or "buying on behalf of," is a method used by CMLNs to move value through the purchase of luxury or high-value goods in the United States, shipping them to China, and selling them at a profit. Daigou operations are often organized and funded by criminal networks as part of the laundering process. Daigou methodologies and red flags are described in Section 7 Focus: Daigou and Luxury-Goods Laundering.

Real Estate and Other High-Value Assets

Real estate is attractive to money launderers because it often involves high-value assets which appreciate in value, and large sums that can be laundered in a single transaction. Purchases can also be made in the name of shell or front companies, which limit transparency. Further detail on laundering through real estate is available in FinCEN Advisory FIN-2017-A003. CMLNs may also use real estate to enable capital flight and launder illicit proceeds, as detailed in FinCEN Advisory FIN-2025-A003 and the accompanying Financial Trends Analysis. Similar techniques can be used to acquire and launder funds through luxury vehicles, yachts, art, and jewelry.

Gold, Precious Metals, and Precious Stones

Precious metals, including gold, and precious stones, can be used for money laundering because of their high value, high value to low size, stable pricing, anonymity, and convertibility. For example, gold can be purchased with illicit proceeds then exported, refined, and sold for cash. Alternatively, in an intersection with TBML, some cartels imported bars of gold mixed with lead, declaring them as fine gold in invoices, enabling the cartel to disguise its profits and movements. Further detail on laundering using precious metals and stones is available in the U.S. Department of the Treasury National Money Laundering Risk Assessment 2024.

Additional Money Laundering Methods

Money laundering methods which may be integrated with all of the above include complicit professionals (such as attorneys, accountants, and corporate service providers), use of shell and front companies, money mules, and many others.

The next sections of this report focus on several of these money laundering methods. They describe the laundering methodology, provide real-life examples, and articulate the red flags specific to each type of laundering. These can be used by financial institutions to adapt their counter-illicit finance programs – policies, processes, systems, controls, and training – to ensure they effectively identify and respond to cartel and CMLN risks.

Money Laundering Methodologies

Chinese Money Laundering Networks: How Capital Flight From China Drives Cartel Laundering

Distribution and sale of narcotics in the United States, along with other illicit activity, generates significant volumes of cash for cartels, which they seek to launder and repatriate to the cartel in countries such as Mexico. Recently, Chinese Money Laundering Networks (CMLNs) have emerged as the leading “service provider” to launder these illicit funds.

CMLNs service a growing demand from Chinese nationals to access currency outside China, which is otherwise restricted by a $50,000 limit imposed by the Chinese government on movement of capital. The drivers for capital flight include restrictions on private enterprise, political uncertainty and concerns over military build-up with the potential for conflict in the future, investment, and the need to fund tuition and living expenses of relatives living outside China. The result is billions of dollars circumventing capital controls: capital flight from China was estimated at $516 billion in 2024.

CMLNs meet this immense demand by identifying suppliers of currency in the United States, Europe, the United Kingdom, and other countries. In the United States, the high volumes of cash generated by narcotics trafficking and other cartel activities provide a key supply of USD.

Cartels need to dispose of U.S. dollars and Chinese nationals want to acquire them.

The result of this supply-and-demand is a close association between CMLNs and cartels, with CMLNs providing extensive, adaptive, and efficient professional money laundering services. In the United States, financial institutions reported $312 billion in suspicious transactions associated with Chinese Money Laundering Networks between 2020-2024.

While we may refer to Mexican cartels or Chinese Money Laundering Networks, this does not reflect on the law-abiding citizens of those countries. Cartels and CMLNs are criminal networks gaining benefits for themselves to the detriment of their own communities, and the other countries in which they operate, undermining human security and financial integrity.

4. Focus: Mirror Transfers and Financial System Touchpoints

"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.

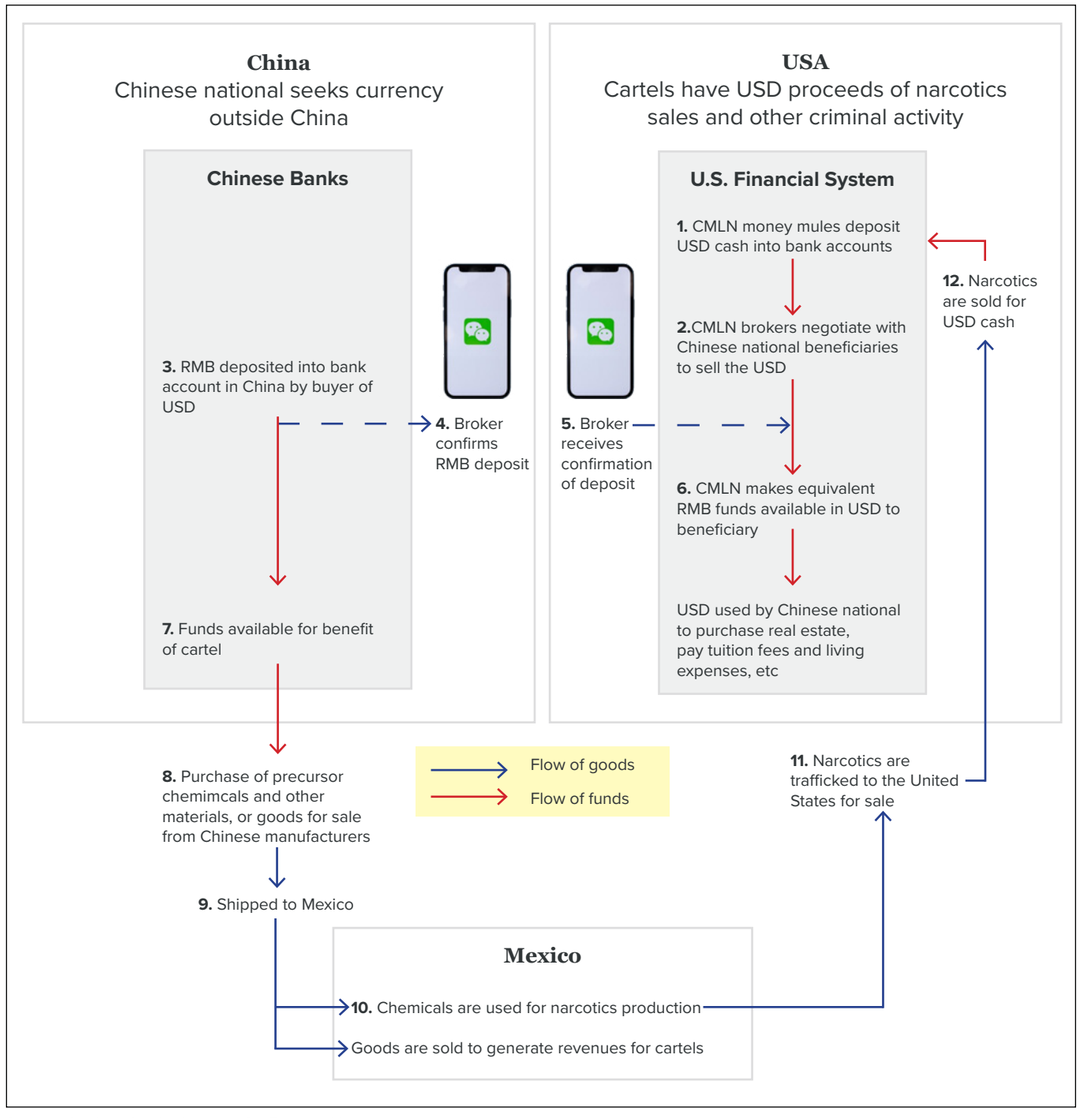
This demand for USD has led CMLNs to partner with illicit actors, such as the Cartels, who have access to large sums of USD that they need to launder. CMLNs assume much of the risk of transporting and laundering large volumes of cash inside the United States, while providing near-instant transfers of value back to their clients by engaging in informal value transfer systems (IVTS) or trade-based money laundering (TBML) schemes.

In the United States, CMLNs functionally operate as unregistered money services businesses (MSBs) and serve as money brokers in the global Chinese underground banking system (CUBS), which provides Chinese citizens the ability to move funds out of China despite the PRC's currency control laws."

– FinCEN Advisory FIN-2025-A003

Cartels and Chinese Money Laundering Networks (CMLNs) use "mirror transfers" – a form of informal value transfer – to move illicit proceeds across borders without using traditional wire transfers, reducing the possibility of detection by financial institutions.

Figure 3: Mirror Transfers Step-By-Step



Source: Analysis by the Institute for Financial Integrity using open sources

The key steps in the mirror transfer methodology are described below.

1. Cartel cash enters the U.S. financial system: Cartels generate large amounts of U.S. dollar proceeds from narcotics sales and other criminal activity. Money mules working for CMLNs deposit this cash into U.S. bank accounts, often in small amounts to minimize detection.

2. CMLN brokers sell the dollars: CMLN brokers in the U.S. connect with Chinese nationals who want access to U.S. dollars (for example, to pay for tuition, cover living expenses in the U.S., or buy real estate). The brokers offer to sell them these cartel-originated dollars.

3. RMB are deposited in China: The Chinese national or their representative deposits the equivalent amount in Chinese yuan (RMB) into a bank account in China specified by the broker.

4–5. Confirmation of deposit via encrypted apps: Using apps like WeChat, the broker confirms the RMB deposit has been made. This communication happens outside the financial system, making it difficult for investigations to link the two sides of the transaction – the mirror transfers – together.

6. USD delivered to beneficiary: Once the RMB deposit is confirmed, the broker provides the agreed amount in U.S. dollars to the beneficiary in the United States nominated by the Chinese national. The dollars can now be used for investments or expenses.

7. Cartels gain access to funds in China: Meanwhile, the cartel, through its relationships with the broker, now has funds in China. The currency was not transferred, but the value was moved.

8. RMB are used to purchase chemicals and goods: The cartel can use these funds to purchase fentanyl precursors, lab equipment, or other goods from Chinese suppliers.

9. Goods are shipped to Mexico: The materials are exported from China to Mexico as commercial goods. The link to the cartel proceeds in the United States is further obscured.

10. Drugs are produced and sold: The chemicals are used to produce fentanyl or other narcotics in Mexico. Imported goods unrelated to fentanyl production are also sold to generate revenue as part of traditional TBML schemes.

11. Drugs are trafficked into the United States: The drugs are smuggled into the United States and sold, restarting the cycle. No cross-border wire transfers occurred – only informal settlements and movement of goods – making detection extremely difficult.

This description is just one example of how mirror transfers can work and there are many variations. Significantly, by using this method each currency stays within its own country: USD stay in the United States, RMB in China, and pesos in Mexico. Mirror transfers enable laundering of cartel proceeds, fund further illicit activity, and meet demand from wealthy Chinese nationals for offshore currency – while reducing the risk of detection by minimizing use of the financial system and avoiding cross-border wire transfers. It is a highly efficient, lower visibility method of laundering money across borders.

CMLNs and mirror transfers offer significant advantages compared with other money laundering methods.

Figure 4: Cartels and CMLNs – a Side-by-Side Comparison

Cartels	CMLN Mirror Transfers
Fees charged 5%-10%	Fees for cartels: 0%-2% Fast, often with guaranteed delivery Uses mirror transfers to avoid cross-border wires (minimizes detection)
Trade-Based Money Laundering	**Bulk Cash Smuggling**
Slow and inefficient - may take weeks for laundered cash to reach cartels	Higher costs (e.g. for bribe to border officials)

Source: Analysis by the Institute for Financial Integrity using open sources

While mirror transfers avoid cross-border wire transfers, there are still touchpoints to the formal financial system. Financial institutions must adapt their counter-illicit finance programs to ensure they are responsive to how these methodologies may present and the red flags that can still be detected. These actions will vary depending on the financial institution: red flags that can be detected by a retail bank will be different from those potentially visible to a correspondent bank. Four case studies illustrate these differences and provide actionable red flags for financial institutions to build into their controls.

Focus: Mirror Transfers and Financial System Touchpoints

CMLNs charge significantly lower fees, a difference of up to 10% compared with cartel launderers. A legitimate business would consider it a success to increase their profitability by 10% by changing one supplier.

But in the context of cartels and CMLNs, this represents more money, available more quickly, to further illicit activity and the harms they cause.

Case Study 1: Individual Accounts – Money Mules

Context: Individuals may be used by CMLNs as "money mules," meaning they are used to open bank accounts, deposit cash resulting from narcotics sales and other illicit activity, and engage in transactions to launder those funds.

Case: In September 2023, a Chinese national claiming to be a cook at a Chinese restaurant opened a checking account at a U.S. financial institution using a fraudulent Chinese passport. Between September and October 2023, the account holder purchased more than $4 million in cashier's checks made payable to various individuals and limited liability companies, including real estate companies located in major U.S. metropolitan cities. These negotiable instruments were funded either directly with cash or from recent cash deposits that had been made into the account. The funds were ultimately used to purchase real estate in the United States.

Red flags: The red flags for money mule activity that can be identified by financial institutions from this and similar cases include:

- Counterfeit passports, visa stamps, or entry stamps are often used.
- The same photos are used for a passport and visa even though the issue dates are purportedly years apart.
- Sequential passport numbers are identified for apparently unaffiliated account holders.
- Multiple accounts are opened at the same institution using the same passport number but different identities.
- Accounts are opened with different identities and passport numbers but the same address, phone number, or email address.
- There are "translators" (who are actually representatives of a CMLN) present when an account holder makes cash deposits.
- The individuals state their occupation to be hospitality or food services workers, students, laborers, or delivery drivers but their account activity is inconsistent with that expected for that occupation, such as small dollar cash deposits (e.g. $100) followed by large dollar cash deposits.
- An account holder is unable to explain the source of cash deposits.
- Deposited funds are almost immediately withdrawn to purchase round-dollar cashier's checks payable to third parties not associated with the account.
- Checks are negotiated and used to pay for luxury goods, jewelry, or electronics.

Focus: Mirror Transfers and Financial System Touchpoints

Case Study 2: Transactional Activity – Structuring

Context: "Structuring" is used in an attempt to avoid the mandatory requirement to file reports and therefore to attempt to minimize detection. For example, in the United States a Currency Transaction Report (CTR) must be filed for cash transactions over $10,000, so deposits of illicit cash may be divided into multiple transactions of less than $10,000 or may be deposited at automated teller machines (ATMs) at different locations or operated by different banks.

Case: Operation Fortune Runner, which was part of a U.S. Organized Crime Drug Enforcement Task Forces operation, identified that more than $50 million in drug proceeds were laundered by the Sinaloa cartel conspiring with CMLNs. The methods used included making multiple structured cash deposits into ATMs, a few hundred dollars at a time, often with only minutes between each transaction. These included:

- Luis Belandria-Contreras made 24 cash deposits over a 1 hour 19 minute period, each of a few hundred dollars, into various ATMs in Long Beach and Downey, California. The total amount deposited was $15,960.
- Guillermo Zambrano made 15 cash deposits over a 13 minute period, into a single ATM. The total amount deposited was $19,900.

Red flags: The red flags for structuring that can be identified by financial institutions from this and similar cases include:

- Multiple cash transactions are made, each below $10,000, within a short time period, potentially at different ATM or branch locations or into different accounts.
- The account holder is unable to explain the source of the large cash deposits.
- Post-deposit activity on the account indicates funneling or other indicators of money laundering.
- Accounts are opened with different identities and passport numbers but the same address, phone number, or email address.

Case Study 3: Corporate Accounts – Laundering and Funneling

Context: Corporate and business accounts are often used to launder proceeds of criminal activity or to purchase precursor chemicals and items used to manufacture narcotics. These companies are often shell or front companies, meaning corporate entities with no significant assets or operations, or those that appear legitimate but are used to conceal illicit activity.

Case: In 2024, Luis Reinaldo Ramirez was sentenced by a U.S. federal court to 10 years in prison for laundering $16.5 million in narcotics proceeds for the Sinaloa Cartel. He paid for and facilitated the travel of bulk cash couriers to collect cash throughout the United States, including in Chicago, Omaha, Boston, New York City, Baltimore, Charlotte, and Philadelphia. The cash was deposited into shell company bank accounts opened at four different banks. It was subsequently funneled and transferred to Mexico or used in trade-based money laundering schemes. In this case, the shell companies were LLCs incorporated in Wyoming. The account for one of the shell companies, HFMV LLC, at one U.S. bank was funded by $1,813,862 in cash deposits and subsequently debited by $1,575,803 in wire transfers to Mexico-based individuals and entities. The HFMV LLC account at another U.S. bank was funded by cash deposits of $200,000 and subsequently debited by $199,862 in wire transfers to Mexico-based individuals and entities.

Red flags: The red flags for laundering and funneling through corporate accounts that can be identified by financial institutions from this and similar cases include:

- Transactional activity indicates that the account is being used for funneling, such as similar value withdrawals and deposits, especially where the deposits are large volumes of cash.
- Transactional activity does not correspond with expected business activity, such as higher transaction volumes than would be expected for a new/small business or the absence of legitimate business activity on the account.
- Businesses that do not show legitimate business activity, for example the absence of a website or physical office premises.
- Contact information, such as telephone numbers, email addresses, or addresses, is shared between multiple apparently unrelated companies, especially those in industries/geographies associated with cartel and CMLN activity.
- Counterparties to transactions are located in geographies with a higher risk of cartel activity.
- Entities have complex corporate ownership structures, which may indicate attempts to obscure the identity or the owner.
- The business is incorporated in a “secrecy jurisdiction.”

Focus: Mirror Transfers and Financial System Touchpoints

Case Study 4: Corporate Accounts – Precursor Chemical Acquisition

Context: China continues to be the primary source country for fentanyl precursor chemicals and related equipment such as pill presses. Individuals, shell and front companies may be used during the acquisition of materials for narcotics manufacture.

Cases: A financial institution identified a Mexico-based company purporting to operate a chemical importation business. The company had been established only one year before and was transacting solely with a China-based chemical distributor. Another institution identified a Mexico-based company which previously sent payments directly to China, which were assessed as being for acquisition of precursor chemicals. Subsequently, the payments were changed to a U.S.-based company owned by a Chinese national, which was assessed as being a potential intermediary.

Red Flags: The red flags for acquisition of precursors that can be identified by financial institutions from this and similar cases include:

- Clients operate in high-risk industries and geographies, such as chemical and pharmaceutical companies in China, Hong Kong, or Mexico.
- Entities in unrelated industries in Mexico transact with Chinese chemical or pharmaceutical companies, or vice versa.
- Business characteristics indicate the use of shell or front companies, such the absence of expected business activity (described previously under Corporate Accounts).
- Client contact information matches contact information on chemical company websites or e-commerce platforms.
- “Chemical Abstract Service Numbers” (chemical identifiers) are used in open-source advertisements associated with a client, or the numbers are listed in payment instructions or invoices provided by clients. For example, precursor 1-Boc-4-piperidone has identifier 79099-07-3 and 1-Benzyl-4-piperidone has identifier 3612-20-2.
- There are periods of account dormancy between 1 to 2 month periods of unusual chemical-related payments.

These cases demonstrate how CMLNs and cartels cooperate to provide highly effective methods of laundering the proceeds of narcotics trafficking and other criminality, using both informal value transfers and the financial system. There are other laundering methods that operate in parallel with the financial system too, such as cryptocurrencies.

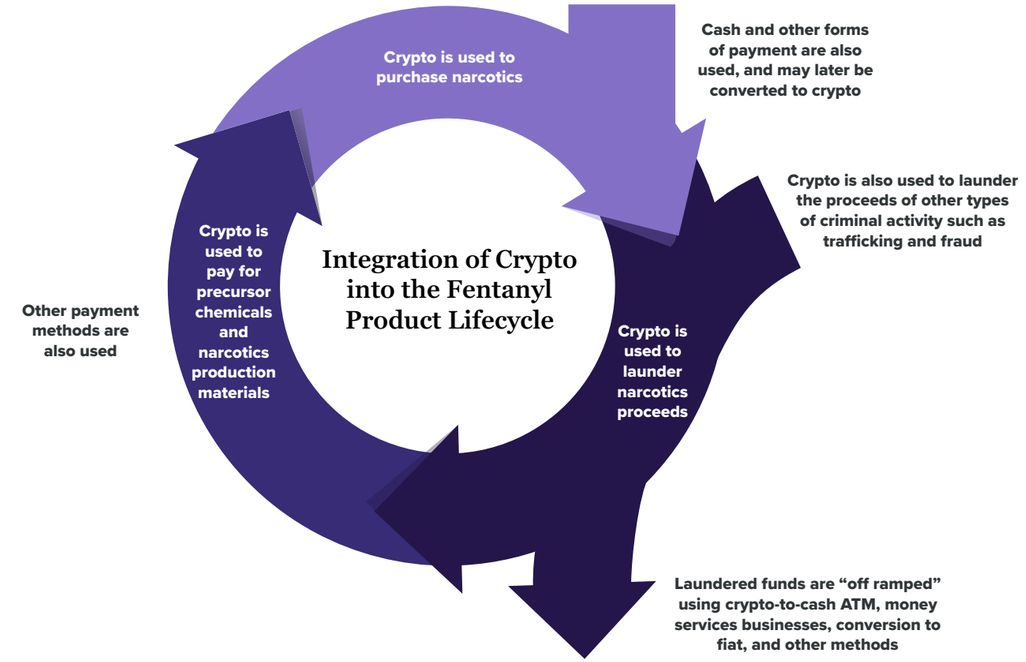
5. Focus: Cryptocurrencies (Digital Assets)

Crypto is increasingly dominant when it comes to laundering cartel proceeds. In the United States, $2.5 billion in crypto was seized by the DEA compared with $2.2 billion in U.S. currency from 2020-2024 as cartels – and the Chinese Money Laundering Networks (CMLNs) who are key enablers of their criminality – continue to adapt their methodologies.

This section focuses on narcotics as an example of how cartels have integrated digital assets into their operations throughout the narcotics "product lifecycle."

- Crypto is one accepted method of payment for precursor chemicals, narcotics production materials, and goods to be sold in trade-based money laundering schemes.
- After narcotics are manufactured and distributed, cash payments for drugs like fentanyl are converted into crypto during the laundering of these proceeds. Sometimes, payments for narcotics are made directly in crypto on darknet marketplaces. Crypto is also used to move ("layer") the proceeds from multiple types of criminal activity, comingled with narcotics proceeds.
- Crypto can be cashed out using crypto ATMs, money service businesses (MSBs), trade-based money laundering, or fiat currency.

Figure 5: The Integration of Crypto into the Fentanyl Product Lifecycle



Source: Analysis by the Institute for Financial Integrity using open sources

Payment for Precursors

China is the primary country of origin for the precursor chemicals used to manufacture narcotics for distribution in the United States, according to the DEA. Crypto is widely accepted as a form of payment: 97% of more than 120 Chinese precursor manufacturers accepted payment in digital assets, according to an assessment using blockchain analytics.

The use of crypto to pay for precursor chemicals is increasing: payments in crypto to Chinese precursor manufacturers increased more than 600% from 2022 to 2023, reaching more than $26 million, and more than doubled in the first four months of the following year.

The digital assets used for payment are primarily Bitcoin (60%), stablecoin Tether (USDT) on the Tron blockchain (30%), and USDT on the Ethereum blockchain (6%).

Precursors are shipped to countries such as Mexico to manufacture narcotics, which are then transported to markets such as the United States for distribution and sale.

Payment and Laundering Narcotics Proceeds

Payments for narcotics like fentanyl are often made in cash. Payments may also be made directly in crypto, for example when narcotics are purchased on a darknet marketplace.

Multiple methods are used to launder the proceeds from narcotics sales, including use of the traditional financial system, “mirror trades” enabled by CMLNs (section 4 of this report), TBML, and other methods. Increasingly, crypto is used for laundering too.

Cash proceeds are converted to crypto as part of the laundering process, either directly using cash-to-crypto ATMs, or the cash may be deposited into bank accounts by money mules and later converted to digital assets. The assets are primarily Bitcoin and stablecoin USDT, although others may also be used such as USD Coin (USDC), Ripple (XRP), and Ether (ETH). Stablecoins are digital assets that are “pegged” to a fiat currency, usually USD, and they therefore offer lower volatility compared with Bitcoin. The crypto can then be rapidly moved, including across borders, to cartel-controlled wallets. Often, the proceeds of narcotics trafficking are co-mingled and laundered with the proceeds of other criminality such as fraud, as described in the folllowing case studies.

To complete the narcotics trading cycle, the crypto may be used to acquire more precursor chemicals, or it may be cashed-out at crypto ATMs, through money services businesses (MSBs), or converted into fiat currency, often at a discount given its criminal origin.

Case Studies: Cartel Use of Crypto in Laundering

In September 2023, OFAC designated Mario Alberto Jiminez Castro, a member of the Los Chapitos faction of the Sinaloa Cartel. Jiminez Castro arranged for U.S.-based couriers to collect cash in the United States and deposit it into digital asset wallets for payment onwards to the cartel for reinvestment in fentanyl production. OFAC also designated a cryptocurrency address (wallet) which received $740,000 from March 2022 to February 2023. These designations marked the first time OFAC publicly identified that cartels use crypto to launder drug proceeds. Although crypto was not used to pay for the narcotics, it was used to launder the proceeds.

In January 2024, Martin Mizrahi was convicted of laundering more than $4 million in proceeds from illegal narcotics and fraud and $8 million in bank and credit card fraud. From February to June 2021, Mizrahi accepted bulk cash which was the proceeds of narcotics sales. He converted it into bitcoin and layered it through multiple crypto wallets specified by cartels. Indicative of the intersection between multiple types of criminality, Mizrahi was also convicted for laundering the proceeds of business email compromise fraud and other types of fraud, as well as narcotics proceeds.

To effectively identify risk indicators, financial institutions including crypto businesses must understand how crypto is used by cartels and money launderers, and the red flags applicable to their specific type of business.

Red Flags: Institutions should already have well-established counter-illicit finance programs including Know Your Client (KYC), transaction monitoring, data analytics to identify anomalous activity, and organizational and governance structures. Blockchain technology, which underpins many types of digital assets, provides additional tools to identify red flags that can indicate money laundering using digital assets. Red flags specific to the use of digital assets in the narcotics trade and laundering the proceeds include:

- Rapid movements in or out of a suspected account over short periods of time.
- Deposits into crypto accounts (purchases or transfers-in of crypto) that are quickly moved out leaving a zero or almost-zero balance.
- “Funneling” or “pooling”, especially if “gas fees” are funded as a single payment covering multiple deposits and withdrawals (see detail below).
- Swaps between different digital asset chains (for example, receiving tokens on the Tron blockchain and withdrawing tokens on the Ethereum blockchain).
- High volumes of transactions between accounts/wallets with red flags (for example, those where the wallet owner’s IP address indicates they access the account from a geographical area with a high risk of cartel activity).
- Transactions with wallets already identified by blockchain analytics tools as being associated with narcotics trafficking or other illicit activity.

Deep Dive: How Gas Fees Can Indicate Pooling of Illicit Proceeds

Blockchain analytics can be used to trace digital asset transactions. Like money laundering through the fiat financial system, crypto transactional activity may indicate "pooling" or "funneling", which is a red flag for money laundering. To identify pooling, blockchain analytics can be used to identify specific patterns associated with "gas fee" payments.

"Gas fees", meaning the processing fees for blockchain transactions, are also visible as a blockchain transaction. Where the gas fee for multiple deposits and withdrawals are financed as a single payment, often in Ether or Tron, it reveals an association between the transactions.

The example below shows how Jiminez Castro, described above, operated wallets to funnel value using stablecoin USDT. For example, 19.2K USDT is deposited in his wallet and later 19.2K in USDT is withdrawn. The same pattern applies to other deposits and withdrawals shown below. Each deposit/withdrawal pair is assessed as being a separate pick-up job (specifically, a collection of bulk cash proceeds from narcotics sales) and the amounts are matched before and after pooling in Jiminez Castro's wallet. The processing fees for the transactions are paid as a single combined payment, shown in orange and in the reverse direction. This indicates that all the transactions covered by the gas fee payment are related.

Source: Elliptic

Crypto Use in Human Trafficking and Smuggling

This section has focused on fentanyl. However, digital assets are used by organized crime groups and launderers in other illicit activities too. For example, digital assets may be used in human trafficking and people smuggling including:

- Crypto may be used to pay human traffickers and transporters on smuggling routes
- Ransom payments for kidnapped migrants may be demanded in digital assets
- Smugglers may demand payments in crypto before enabling them to cross borders

While cryptocurrencies represent the use of newer representations of value for laundering and funding illicit activity, traditional methods – like casinos – continue to be used too.

6. Focus: Casinos

Casinos and gaming platforms, both physical and online, constitute one of the world's fastest-growing entertainment sectors, but they also remain highly exposed to money laundering.

- The United Nations estimates that global gambling revenues will reach $205 billion by 2030, while industry projections suggest the figure could rise as high as $700 billion by 2028.
- In the United States, commercial gaming generated $72 billion in 2024, with an additional $41.9 billion from tribal gaming enterprises.
- In the United Kingdom, there are 2,343 gambling operators and 8,301 premises, including 144 casinos.
- Australia, 38% of the population gambles weekly, and in the state of New South Wales there is the equivalent of one gaming machine for every 88 people.
- Across Europe, gross gaming revenues reached €123.4 billion ($144 billion) in 2024 – a 5% year-on-year increase – with online gambling now representing 39% of total revenue.

These numbers indicate the financial scale and social reach of gambling and gaming, characteristics which can be exploited by transnational criminal networks, including cartels and CMLNs.

One of the highest profile recent cases of casinos being used to launder cartel proceeds was investigated by the Cullen Commission, with the methodology often referred to as the "Vancouver method" because it was used in casinos in British Colombia.

The Vancouver Model and Mirror Transfers

The Cullen Commission, which reported in 2022, identified that millions of dollars were laundered through casinos in British Columbia between 2008 and 2018, including the proceeds of drug cartels based in Mexico and South American countries. Indicative of the scale of laundering, in a single month, July 2015, more than $20 million in suspicious cash was reported by casinos to their regulators. This included more than $14 million that was accepted in $20 bills – this is not the total volume of cash handled, it is ***only*** the activity identified as meeting the suspicious reporting threshold.

The gamblers were often "high rollers" from Asian countries who required access to significant volumes of cash to fund betting on their visits to Canada, with bets of up to $100,000 on a single hand of baccarat. Many of these gamblers had significant wealth abroad, but with China imposing a limit of $50,000 per year on removal of capital, and the practical difficulties of gamblers from other Asian countries acquiring and bringing cash with them, casino patrons had difficulty accessing these funds in Canada.

In contrast, cartel networks selling narcotics and involved in other types of illicit activity had large volumes of cash in Canada and a need to launder it. Money laundering network operatives made this available as cash or chips in casinos, carparks, and nearby locations. Gamblers used it to gamble, genuinely putting it at risk and often losing it. The Commission identified that the "loans" were repaid in electronic funds transfers or using other methods, enabling launderers in Canada to convert bulky, illicit cash into more convenient and less suspicious forms of value.

Red Flags

The Cullen Commission identified multiple red flags indicative of the criminal origin of cash and/or laundering:

- "Cash facilitators" were identified in casinos passing cash and/or chips between players but rarely playing. Casino staff initially characterized them as "loan sharks."
- Cash was provided to gamblers in plastic bags, shoeboxes, and knapsacks, usually in $20 bills held together in bundles with elastic bands. The bundles were irregularly arranged such as some notes being face-up, others face-down, or in other varied orientations. In contrast, cash withdrawn from financial institutions is well arranged and in appropriate packaging.
- Bags of cash were brought into the casino, converted into chips, then exchanged back into cash without any play having occurred, or only minimal or low-value bets.

The use of the Vancouver method declined significantly in 2018 when source-of-funds recommendations were implemented in British Columbia. However, similar "mirror transfer" methods have been identified in casinos in Australia, Macau SAR, Cambodia, Laos, Myanmar, and the Philippines. Evolutions of mirror transfers beyond casinos also continue to be used by CMLNs, as described in Section 4 Focus: Mirror Transfers.

Casinos and online gambling and gaming also continue to be used to launder illicit proceeds in the United States, Australia, the United Kingdom, and many other countries.

For casinos and gaming operators, five key red flags that can identify potential laundering through gambling/gaming include:

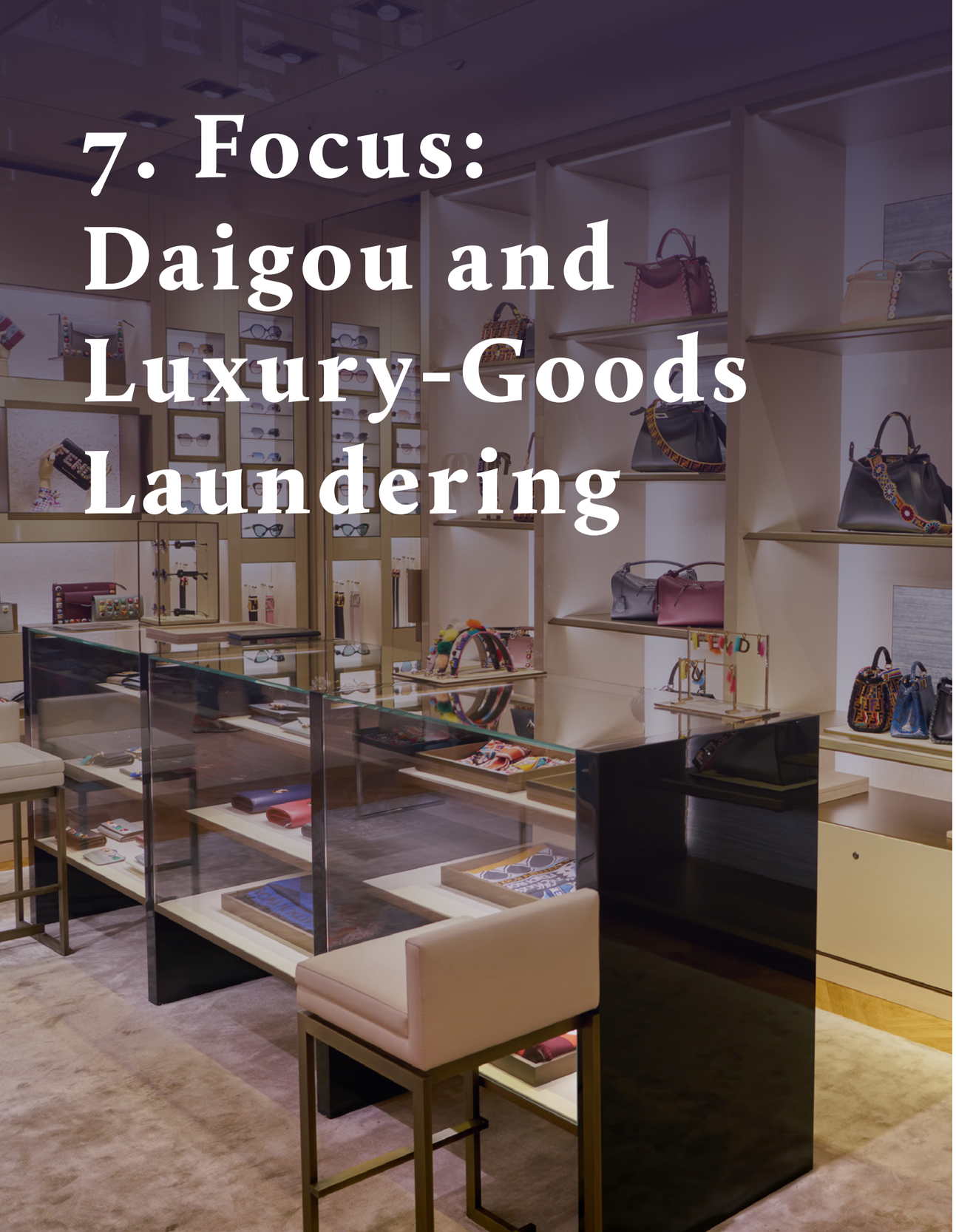
- Client transactional activity is inconsistent with the client profile (for example, large bets are placed by individuals expected to have lower income, such as students).
- A client gambles large amounts of money and appears to find losses acceptable. This may indicate that they are spending the proceeds of crime and see the losses as an acceptable "cost" of laundering.
- A client places bets that ensure minimal losses (for example, bets equal amounts on a player and the banker, or places the same bets on black and red in roulette), allowing money to be represented as winnings when it is paid out.
- There are indications of collusive play between participants, which may indicate bets are being used to transfer value between players while making it appear to be legitimate winnings (or losses).
- A client conducts transactions or bets just below the reporting threshold (for example, $10,000) or changes their bets to stay under the threshold.

For financial institutions, five key red flags that can identify potential laundering through gambling/gaming include:

- The client's account is funded by casino checks, however the check memo indicates the funds are not the result of casino winnings.
- The client's account activity appears to be circular (for example, deposits of casino checks followed by bank drafts used at casinos, followed by deposits from casino checks, especially if the memo indicates they are not the result of casino winnings).
- The client's account appears to be used exclusively for casino gaming (for example, the activity is casino check deposits, bank draft issuances to casinos, or cash withdrawals at casinos, rather than everyday banking such as payroll and bill payments).
- The client's account shows high volumes of gaming activity and transactions involving high value goods such as real estate or luxury vehicles.
- Credit card activity is primarily casino-related and paid off in cash.

For a comprehensive analysis of money laundering through the gambling and gaming sector, refer to the Institute for Financial Integrity's report High Stakes: Casinos, Crime, and Cartels which examines case studies in five countries including casino junkets, online gaming, sports betting, and casinos; red flags for land-based casinos, online gambling/gaming, and financial institutions; and compliance best practices for operators and financial institutions.

In addition to the well-established and large-scale laundering operations through mirror transfers, the financial system, crypto, and casinos, CMLNs use less well-known methods to launder cartel proceeds too. One of these is "daigou," or "buying on behalf of," which uses purchases of luxury and high-value items to move value while minimizing detection.



7. Focus: Daigou and Luxury-Goods Laundering

Daigou, which approximately translates as “buying on behalf of,” uses straw buyers to acquire goods in western countries, which are exported to China and sold at a profit. While daigou itself is not illegal, daigou operations are often financed by Chinese Money Laundering Networks (CMLNs), which receive and launder proceeds from cartels and other criminal activities. Daigou may also involve tax and tariff evasion, and can obscure the identity of the client and source of funds.

Scale of Daigou

Only a small proportion of suspicious activity reports from U.S. financial institutions specifically reference “daigou,” approximately $9.6 million from a total of $312 billion in suspicious activity associated with CMLNs overall, according to a 2025 FinCEN Financial Trend Analysis. However, a significantly higher proportion of reports involve unusual credit card activity ($19 billion), some of which may also represent unidentified daigou.

Daigou operations have been identified by law enforcement and Financial Intelligence Units in other countries too. An advisory on daigou published by the United Kingdom National Crime Agency identified one CMLN as controlling approximately 600 accounts at a single financial institution, and the same CMLN was known to control accounts at multiple other financial institutions too. Daigou networks have also been identified operating in Canada.

Drivers of “Surrogate Shopping”

In China, luxury goods are often subject to significant tariffs and can be expensive compared with the same item purchased overseas. Counterfeiting is also prevalent and may result in health risks or even death. In 2004, fake infant formula originated in the Anhui province in China caused the deaths of 13 babies, followed in subsequent years by further infant deaths caused by contamination. The result is demand for authentic western products and/or luxury items at lower prices than official outlets (where taxes and duties have been paid), with discounts of around 40% for some products.

With movement of capital out of China restricted to approximately $50,000 per person per year, daigou buyers in western countries face liquidity issues with financing their purchases, as well as moving the proceeds of sales outside China. They may therefore engage with CMLNs as financial service providers, or alternatively CMLNs may directly manage and operate daigou networks.

Daigou Methodology

One methodology for daigou operations is:

1. Goods are advertised on marketplaces in China such as TaoBao (comparable with eBay) or on social media.

2. The daigou (buyer) receives funding from the CMLN to make their purchases. This may be cash, electronic funds transfers, peer-to-peer payments, or checks.

3. Daigou buyers use cash or credit cards to purchase items in the United States or other western countries. Often, these are high-value electronics or luxury goods, purchased according to instructions from CMLNs. Items may also include cosmetics or health products.

4. Where credit cards are used, the cash and/or bank funds are used to pay off the account balances. Credit card reward points may also be used for travel or exchanged for USD payments.

5. The buyer ships the items to China or to a daigou operator in the buyer country (for example the United States) who receives items from multiple daigou then coordinates the exports to China.

6. The items are sold for a profit by avoiding the applicable import taxes or duties. The daigou receives the proceeds in China.

Daigou and Mirror Transfers

Daigou may also use CMLNs to move value using mirror transfers, circumventing Chinese capital restrictions. For example, the United Kingdom National Crime Agency has identified this methodology. Daigou in the United Kingdom receive funds into a UK bank account, which are provided by CMLNs and originate from criminal activity. In China, daigou pay the equivalent value to the CMLN in China from the proceeds of sales of luxury or other items. The effect is for the daigou to move the value of their profits from China to the United Kingdom using a mirror transfer.

There are many variations on daigou operations, with the methodologies above representing just some examples.

Red Flags – Individual Accounts

CMLNs often target Chinese diaspora to operate as money mules, buyers, or brokers. Some may be recruited by being told they are providing money transmission services for other students or unbanked Chinese workers, whereas other mules are aware their account will be used for illicit activity.

Red flags most relevant to daigou activity include:

- The customer shows indications of irregularities in documents which may indicate they are fraudulent, for example a Chinese passport and visa contain the same photograph despite purportedly being issued years apart.
- Activity that is not commensurate with the customer profile. For example, a student receives wire transfers described as “tuition” or “living expenses” that do not correspond with the timing of these costs during the academic year, or where the amounts do not correspond with the expenses described.
- There are discrepancies between declared income/earnings and account activity.
- A customer, especially a Chinese national, regularly uses a credit card to purchase large volumes of electronics or other luxury goods.

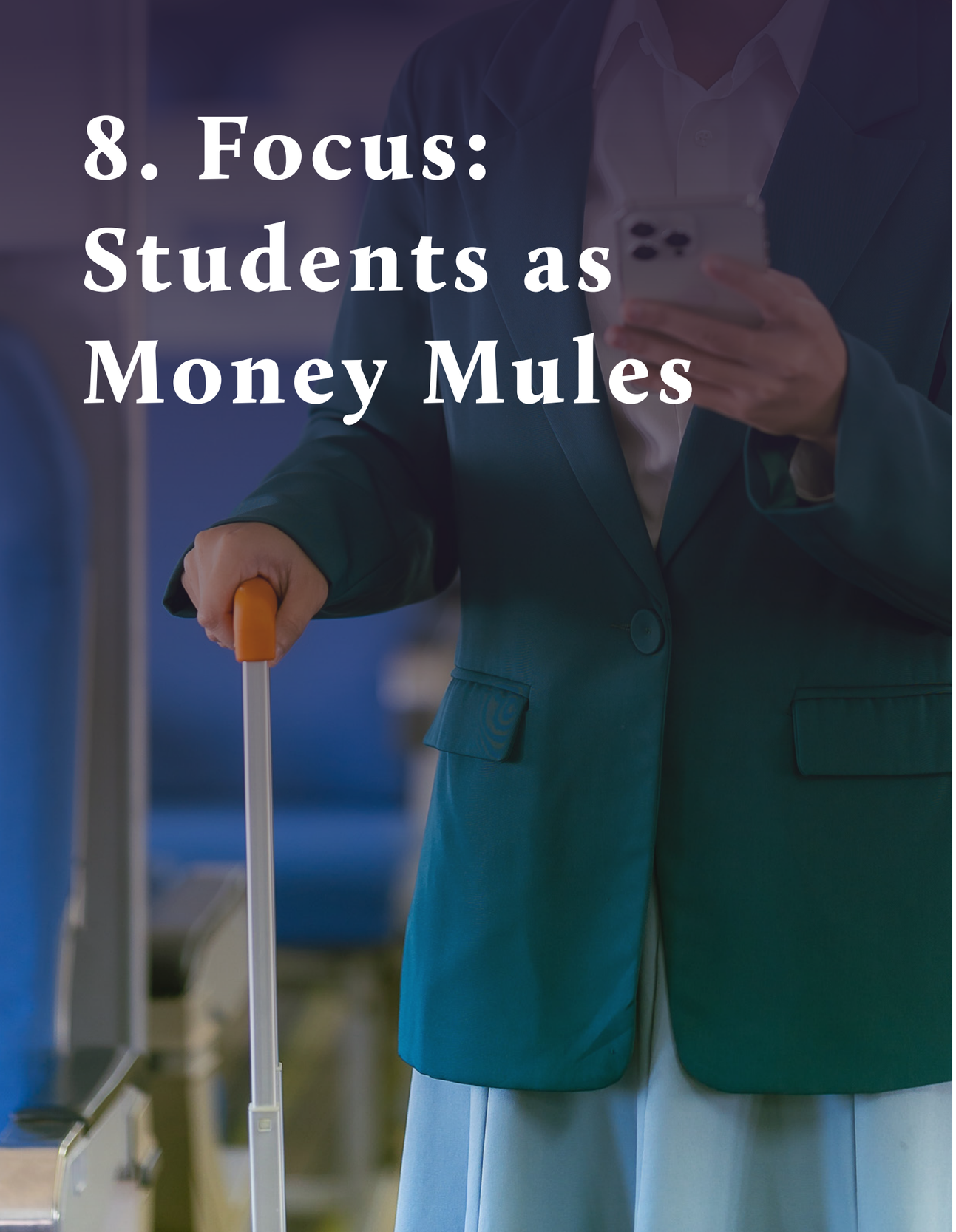
Additional red flags for money mules are described in Section 4 Focus: Mirror Transfers.

Red Flags – Corporate Accounts

Business bank accounts may also be used to facilitate daigou activity. Red flags include:

- Individuals associated with a business account, such as directors or authorized signatories, show indications of irregularities in their identity documents or client profile (refer above to red flags for individual accounts).
- A business operating in the electronics or luxury goods sector shows revenues that are not proportionate to the business’ size or scale.
- A business operating in the electronic or luxury goods sector makes payments for multiple credit cards for individuals unrelated to the business.
- Companies registered in Hong Kong send funds to Chinese nationals residing in the United States, where the company has characteristics of a shell company.

As referenced throughout this report, many of the money laundering methods used by CMLNs rely on money mules from the Chinese community. The next section assesses in more detail how CMLNs target Chinese students and the reasons they become involved in criminality.



8. Focus: Students as Money Mules

As CMLNs represent an increasing proportion of cartel laundering, CMLNs need increasing numbers of money mules to launder proceeds. CMLNs target Chinese students, using cultural obligation, debt bondage from rigged games at illegal casinos, and financial payments to induce students to participate.

A 2025 FinCEN Advisory highlights the scale of CMLN operations targeting students. From 2020-2024, more than 20,000 suspicious activity reports referencing individuals purporting to be Chinese students were filed by U.S. financial institutions. These reports represented approximately $13.8 billion in suspicious activity and were filed from multiple financial sectors including banks, MSBs, and casinos.

"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..." – **FinCEN Financial Trend Analysis August 2025**

Chinese Money Laundering Networks: Recruitment and Control of Students

The methods used by CMLNs to recruit and control students have similarities across jurisdictions. In the United States, FinCEN assessed that the reasons Chinese students could become involved included financial returns and obligations towards the Chinese community.

"CMLNs appear to have increasingly recruited Chinese students studying at U.S. universities, and some of these students may have continued to participate in CMLN operations after graduating... 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)." – FinCEN Advisory

Similar patterns are seen in other countries. In the United Kingdom, Chinese students are recruited as money mules by being told they are providing transmission services for other students or unbanked Chinese citizens in the UK, accordingly to the United Kingdom National Crime Agency.

Chinese students may be coerced into being money mules, for example through "debt bondage" from gambling losses at illegal casinos (as described in the real-life example below). However, in many situations students are simply asked to undertake illicit activity, against a backdrop of cultural expectations and obligations.

A 2023 survey of Chinese students in the United Kingdom undertaken by the United Kingdom Home Office Modern Slavery and Organised Crime Team identified that where students were targeted by Chinese criminal networks, many felt obligated to comply if they were simply asked. The preliminary findings* include:

- The survey focused on two specified activities: laundering money through the student's personal bank account and accepting packages of illicit substances.
- 12.5% of Chinese students in the United Kingdom had been asked or coerced by a person of their own ethnicity to undertake these activities. 1 out of 4 had been coerced; the remaining 3 were simply asked.
- 32.9% responded that they would feel compelled or highly compelled to assist if asked by a person of their own ethnicity.

** The preliminary findings from the study are used here with permission of the author, David Wilson from the UK Home Office Modern Slavery and Organised Crime Team.*

As well as being recruited as mules to launder funds through financial institutions, CMLNs recruit students to act as buyers in daigou schemes, to launder money through casinos and gaming, real estate, healthcare, and other industries, and combinations of these.

Real-Life Investigation: Illegal Casinos and Debt Bondage

An investigation by the West Midlands Police in the United Kingdom identified that overseas students were being targeted by criminal networks in illegal casinos using "rigged" games. For example, in one investigation the cards at the poker table were marked, then the play was monitored by a covert infrared camera. The information was relayed to another player, who used it to cheat the other players out of cash. The West Midlands Police identified that the criminal networks gained influence over students through their gambling debts, using this to coerce them into criminality.

Figure 6: Awareness-Raising on Illegal Gambling

Source: United Kingdom CrimeStoppers

Red Flags for Financial Institutions

While it may be difficult for financial institutions to identify the predicate offenses from cartel activity (such as narcotics trafficking or human trafficking), they are well-positioned to identify laundering of the proceeds. Red flags that may indicate money mule activity, particularly by students, include:

- There are irregularities in documents which may indicate fraud, for example a Chinese passport and visa contain the same photograph despite purportedly being issued years apart.
- The person shown in the identity document has a similar appearance to the bank account or credit card applicant, but is not the same person.
- Multiple accounts are opened at the same institution using the same passport number but different identities.
- Multiple accounts are opened with different identities and passport numbers but the same address, phone number, or email address.
- Accounts are funded via third party wires or cash deposits rather than income from employment.
- There is little or no normal daily spending on the account.
- The account receives wire transfers described as “tuition” or “living expenses,” but they do not correspond with the timing of these costs during the academic year, or the amounts do not correspond with the expenses described.

Red flags that may indicate debt bondage, for example as a result of gambling debts, include:

- A customer is escorted and monitored while at the bank, for example by a person describing themselves as a “translator” or a “friend” who appears to be directing or controlling the customer, or is keeping the customer’s identity documents.
- An existing customer wants to open another account but the information they provide doesn’t match their existing account details.
- The same home address or phone number are shared by multiple customers.

Further resources to identify and take action against exploitation

Further resources on how financial institutions and their staff can identify exploitation and the actions to take are available from non-profits Polaris (United States) and Unseen (United Kingdom).

9. Use of Illicit Funds

The objectives of criminal networks include generating revenue to further illicit enterprises, acquiring assets that can generate “legitimate” income, financing the lifestyles of those involved in criminal networks, and gaining influence. Often, but not always, this means that the illicit funds must be laundered so that their illicit origins are obscured.

Criminal Network Operations

Criminal networks require funds to operate and extend their illicit activities, as well as to counter competitors. Examples include:

- Purchasing weapons
- Acquiring narcotics precursors and materials
- Paying commissions or fees to money mules, criminal network members, or professional money launderers
- Renting premises or paying for transport to use in human trafficking or smuggling
- Paying bribes to corrupt officials

Acquiring Assets

Where a criminal network can acquire assets that generate “legitimate” income, it avoids the need to launder those proceeds. For example, if laundered funds are used to acquire real estate which is subsequently rented out, the rental income appears legitimate. Assets such as real estate are also a store of value and often appreciate in value.

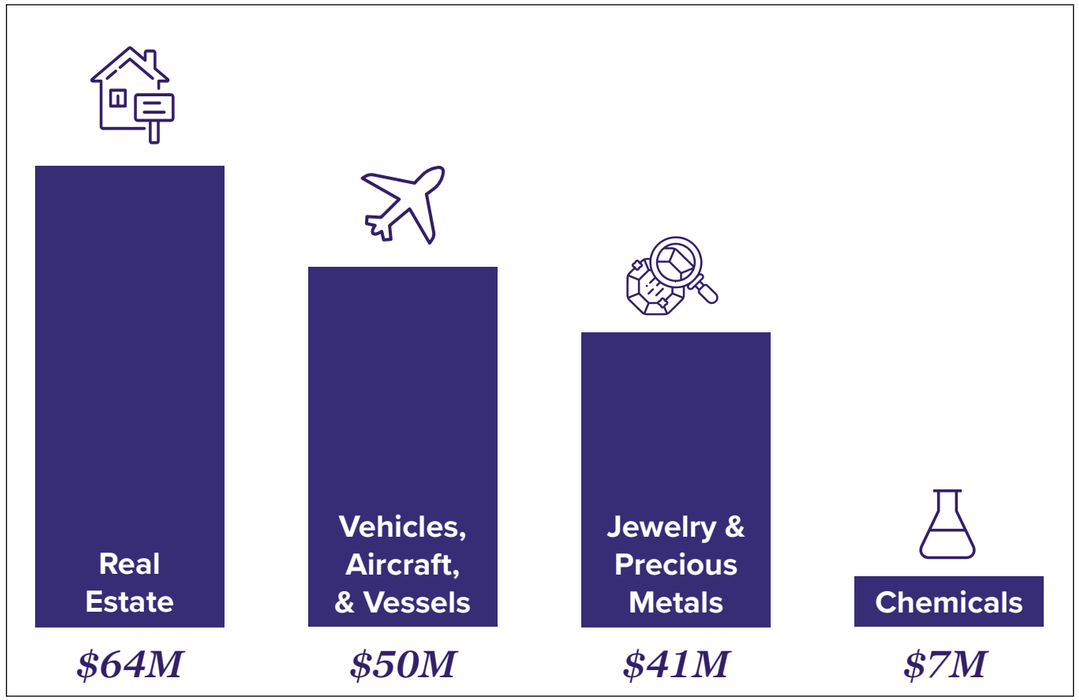
Assets can also be used to launder other illicit proceeds. For example, if proceeds are used to acquire and operate a business, illicit cash can be co-mingled with legitimate business income to provide a laundering channel.

Trade-related and logistics businesses can also be used to further trade-based money laundering through falsified invoices or customs declarations, over-invoicing, or under-invoicing.

Financing Lifestyles and Gaining Influence

Cartel members and CMLNs, particularly higher-ranking members, fund lifestyle costs from illicit proceeds. This includes property, vehicles, artwork, jewelry, luxury goods, and travel. These are not only for personal benefit: they can also provide access to government officials and business leaders, signal the success of the criminal network to enhance recruitment and control, and entrench criminal actors within legitimate political and economic structures. Cartels may also establish “soft power” in communities by funding community projects or local businesses, or by making political donations.

Figure 7: How Narcotics Proceeds are Used – DEA seizures in 2024 provide an example on the use of narcotics proceeds, as well as their size.



Source: DEA National Drug Threat Assessment 2025

Along with public sector partners, financial institutions have a critical responsibility to disrupt these illicit financial flows and deny cartels, CMLNs, and other illicit actors access to financial resources and rewards of their criminality.

10. Actions for Financial Institutions

Financial institutions fulfil a critical role in countering the threat posed by cartels and CMLNs. By detecting, disrupting, and reporting suspicious activity, they form a key line of defense against criminal finance. In previous sections, this report detailed methodologies, case studies, and detailed red flags associated with specific cartel and CMLN activity. This section describes the enterprise-level actions required by financial institutions.

1. Update the institutional risk assessment
2. Ensure processes and systems are updated and operating effectively
3. Deliver customized staff training based on role
4. Monitor alerts and advisories for updates, then action them
5. Engage in public-private intelligence sharing

Update and Maintain the Institutional Risk Assessment

The first step for a financial institution is to undertake (and maintain) its institutional risk assessment to ensure it addresses how risks and red flags may present for that specific type of institution. Some examples of these differences and their implications for the institutional risk assessment include:

- **Retail bank:** A retail bank may have visibility of large or structured cash deposits being made at its branches, as well as the larger financial flows as the laundered proceeds are funneled together and moved via wire transfers. Its controls could focus on client relationships such as client due diligence, understanding the expected activity of that client, and using data analytics to identify outlier activity.
- **Money Services Business (MSB):** MSBs are a transaction-driven rather than account-focused businesses, and their services may be used to fund payments made for precursor chemicals. The focus of their controls may be on geographic locations and transactional patterns.
- **Crypto business:** Crypto businesses need to understand the digital assets and transaction types that correspond with cartel activity. For example, where digital assets are used, retail payments often use bitcoin whereas cartels laundering and moving larger volumes of funds increasingly often use stablecoins like USDT.

In addition, as with all illicit finance risk assessments, considerations include how the financial institution is exposed to cartel and related money laundering risks through:

- **Geography/jurisdiction:** The markets in which the financial institution and its clients operate and how these are exposed to cartel and money laundering risks
- **Sectors:** The sectors in which the financial institutions' clients and their counterparties operate
- **Products/services and channels:** The products and services the financial institution offers – such as retail banking including cash deposits, crypto products, or remittances – and the delivery channels – such as online or in branches

The risk assessment must then inform the financial institution's counter-illicit finance processes and systems.

Ensure Processes and Systems are Updated and Operating Effectively

Cartel risks and money laundering are not new, so a financial institution's processes and systems should already include controls such as client due diligence, screening against lists of designated entities and individuals, transaction monitoring to identify risk indicators, and investigations of unusual activity.

Many of the methods used by cartels are shared with other types of illicit activity and should already be built into preventative and detective controls. For example, cartels use front and shell companies to launder the proceeds as well as obscure the source and destination of shipments of precursor chemicals. Front and shell companies are also used in sanctions evasion, export control evasion, and many types of money laundering, and should be a well-established risk indicator.

Processes and systems must be regularly updated to ensure they remain current on evolving threats and risks. This can be achieved by regularly testing automated systems to ensure they are operating effectively, and providing training to staff to ensure their knowledge and skills are current. For example, traditionally cross-border payments have been considered a key indicator of money laundering, as illicit networks attempt to move and launder proceeds. As cartels and CMLNs increasingly use "mirror transfers," cross-border payments are not necessarily required to move value, and financial institutions must adapt their automated controls and investigative methodologies to address this change in criminal methodology.

Deliver Customized Staff Training Based on Role

Training for staff should be customized to how cartel and CMLN activity could present based on their role, and should link back to risk indicators and methodologies. Training should use up-to-date, relevant examples to enhance engagement and knowledge retention, and should be delivered through regular refreshers as well as annual baseline training.

Some examples of customized training relevant to cartel risks are:

- **Relationship managers and tellers** in retail branches are best positioned to identify money mules depositing cash and structuring payments. They will need to understand the profile and characteristics of individuals used as money mules by CMLNs, such as students, hospital workers, laborers, or delivery drivers, where the cash volumes cannot be explained by their income.
- **Compliance teams** designing and configuring automated monitoring controls should understand how "chemical abstract service numbers," which uniquely identify chemical substances including fentanyl precursors, may be used in payment instructions so they can use these as alert criteria.
- **Due diligence and investigative teams** should understand how some trafficking networks photoshop corporate names and logos onto images of the same building, in an attempt to make them appear to be legitimate and well-established suppliers.

Monitor Alerts and Advisories for Updates, Then Action Them

Advisories and alerts are regularly issued by government Financial Intelligence Units and other sources. Additional resources include analysis and summaries by educational institutions, policy advisors and thinktanks, among others.

Financial institutions should establish processes to identify updates, review them, and apply them within their organization. For example, when an alert with red flags is published, the institution should evaluate which ones are relevant to its business, and how they will be applied within its controls. Some red flags may be suitable to be implemented as automated controls, whereas others may not be sufficiently distinctive and are instead of value as context during an investigation.

Institutions would be well advised to consider using advanced data analytics to look beyond red flags to identify new and as-yet-unidentified risk indicators. Data analytics tools can compare groups of clients by entity type, sector, and geography, to identify outliers which can then be investigated to identify whether the unusual patterns are the result of illicit activity.

Engage in Public-Private Partnerships and Information Sharing

In addition to fulfilling their regulatory responsibilities to file suspicious activity reports / suspicious transaction reports, institutions should contribute to public-private partnerships and intelligence sharing. These can be bilateral relationships or formally established partnerships.

For example, in June 2025, as part of its public-private information sharing "Exchange" program, FinCEN launched a new series called "Combating and Obstructing Money Movements Associated with Narcotics and Drug Trafficking Organizations" (COMMAND). COMMAND brings together relevant stakeholders, including law enforcement agencies and financial institutions, to exchange information on emerging trends and typologies associated with cartel and fentanyl-related money laundering. FinCEN has also encouraged the expansion of information sharing among financial institutions through registration and participation in its 314(b) Information Sharing Program to help identify, report, and prevent cartel money laundering activities.

Conclusion

Conclusion

Cartels, Chinese Money Laundering Networks, and their destructive effects extend beyond any one region or country. They drive violence, death, and damage to legitimate economies and communities globally, whether in the countries where cartels generate illicit proceeds, the markets where they sell prodocuts like narcotics, or the industries and institutions used to launder the proceeds. Cartel and CMLNs' extensive, complex, and adaptable networks present formidable challenges across the financial sector.

All financial institutions are vulnerable and must prioritize effective action against cartels, CMLNs, and the threats they present to financial integrity and collective security.

Institute for
Financial Integrity

Join us in Protecting the Integrity of the Financial System