Department of the Treasury

2026 National Money Laundering Risk Assessment

March 2026

Department of the Treasury

2026 National Money Laundering Risk Assessment

CONTENTS

EXECUTIVE SUMMARY

The United States first published the National Money Laundering Risk Assessment (NMLRA) over 10 years ago. This fifth iteration of the NMLRA finds that the top money laundering threats have remained consistent—fraud, drug trafficking, cybercrime, human trafficking, human smuggling, and corruption generate the largest volumes of illicit proceeds for money laundering activity in the United States. Illicit trade, such as tariff evasion or trafficking in stolen, illicit, or regulated goods, also generates billions of dollars each year. These threats are further enabled by professional money launderers, such as Chinese money laundering networks (CMLNs), that make crime more lucrative by providing expertise and economies of scale.

Technological advancements in finance and communication have amplified the threats posed by all these predicate crimes and threat actors. The rapid growth of emerging technologies, which is improving consumer access and experiences, also creates opportunities that illicit actors can exploit to obscure the origin of illicit funds more quickly and on a global scale. Illicit actors increasingly rely on social media to place malicious advertisements and recruit victims, encrypted messaging applications to communicate with victims and co-conspirators, digital assets to receive and launder funds, and, more recently, artificial intelligence (AI) tools to create fraudulent communications, identities, and websites.

Money launderers seek to exploit every facet of the U.S. financial system to obscure the nature and origin of their illicit proceeds. Whether it is through banks or casinos, cash or digital assets, the main objective is to disguise dirty money within the trillions of dollars of legitimate transactions that occur through the United States each year. In some cases, they misuse legal entities or rely on financial gatekeepers to foil financial institutions seeking to identify underlying actors and report suspicious activity to law enforcement. The U.S. public and private sectors must continue to evolve our capabilities to combat the threat posed by illicit finance while protecting and fostering legitimate finance without undue burden.

Illicit actors engaged in the predicate crimes for money laundering do not care about the well-being of their victims. They target the United States because of the openness of the U.S. economy, the size and sophistication of the U.S. financial system, and the relative wealth of U.S. citizens and companies. They purposefully operate outside of the laws and regulations that apply to all individuals and businesses to profit at the direct expense of others. But measuring the losses of these crimes in dollars and cents only goes so far. Illicit financial activity also crowds out legitimate actors, erodes trust in the free market, and weakens the national security of the United States.

Foreign scammers are stealing billions of dollars in hard-earned savings and siphoning taxpayer funds intended to help the neediest Americans to fund luxurious lifestyles. Narco-terrorists are flooding American cities with deadly drugs and reinvesting the illicit profits in their criminal conglomerates that traffic human beings and terrorize communities. The U.S. government is addressing these threats head on by surging resources through efforts such as Operation Take Back America and Homeland Security Task Forces. As the threat landscape evolves, the United States will continue working to bring threat actors around the world to justice while strengthening the U.S. financial system against their attacks.

INTRODUCTION

The 2026 National Money Laundering Risk Assessment (NMLRA) examines the current money laundering environment and identifies the ways in which criminals and other actors seek to launder funds. It aims to inform the understanding of illicit finance risk by public and private sector actors, strengthen the risk mitigation strategies of financial institutions, and enhance policy deliberations by the U.S. government. Illicit actors will always seek to develop and adopt new ways to launder illicit proceeds, necessitating the continuous identification of money laundering trends to develop tactical, regulatory, and policy solutions to stop illicit activity.

Over the past five years, the median loss from sentenced money laundering cases has increased by over 150 percent from $208,000 to $526,000. In 2019, just 17 percent of these cases involved loss amounts over $1.5 million, and in 2024 that proportion has nearly doubled to 32 percent of cases.[1] This trend comports with the increased targeting of U.S. citizens, businesses, and government programs by narco-terrorists and transnational criminal organizations (TCOs) engaging in fraud, human trafficking and smuggling, and corruption, as well as the exploitation of emerging technologies, such as encrypted communications and artificial intelligence (AI), that allow illicit actors to increase the size, scope, and speed of their schemes. These top money laundering threats present a national security threat to the United States and its financial system.

This report was prepared pursuant to Sections 261 and 262 of the Countering America's Adversaries Through Sanctions Act (PL 115-44) as amended by Section 6506 of the FY22 National Defense Authorization Act (NDAA) (P.L. 117-81). The 2026 NMLRA primarily relies on open-source reporting from the Department of Justice (DOJ), the use of publicly available court documents, and consultations with law enforcement agencies (LEAs) and regulated entities. The NMLRA also uses information from Bank Secrecy Act (BSA) reporting, such as strategic analysis on suspicious activity reports (SARs) conducted by the Financial Crimes Enforcement Network (FinCEN), as well as various types of enforcement actions taken by U.S. regulatory agencies. The assessment period covers January 1, 2024 to December 31, 2025.

The findings of the 2026 NMLRA, taken in tandem with the findings of the proliferation finance risk assessment and the terrorist financing risk assessment, will inform the forthcoming 2026 National Illicit Finance Strategy, which will lay out the roadmap to address the threats and vulnerabilities to the U.S. financial system, and ultimately strengthen the integrity of the U.S. financial system.

1 U.S. Sentencing Commission (USSC), "QuickFacts Money Laundering Fiscal Year 2024," https://www.ussc.gov/sites/default/files/pdf/research-and-publications/quick-facts/Money_Laundering_FY24.pdf; USSC, "QuickFacts Money Laundering Fiscal Year 2019," https://www.ussc.gov/sites/default/files/pdf/research-and-publications/quick-facts/Money_Laundering_FY19.pdf.

THREATS

Money laundering threats are the predicate crimes that generate illicit proceeds for laundering in, from, or through the United States. Threat actors include those who perpetrate predicate crimes or facilitate the money laundering process. This assessment primarily evaluates how money laundering threats impact the United States, including the volume of illicit proceeds generated, the scope of the illicit activity, and the economic activity lost due to illicit actors crowding out legitimate business. It also considers the national security consequences of money laundering threats funding narco-terrorism and other foreign adversary activity. Lastly, this assessment considers the social consequences of money laundering threats, such as the hundreds of thousands of Americans killed each year by illicit drugs smuggled into the United States or the American scam victims driven to financial ruin or self-harm by the devastating loss of their life savings.

The top money laundering threats have remained consistent—fraud and drug trafficking generate hundreds of billions of dollars in illicit proceeds each year. Cybercrime, human trafficking, human smuggling, and corruption also generate billions of dollars in illicit proceeds. Professional money launderers, ranging from complex Chinese money laundering networks (CMLNs) to independent money mules looking to make a quick dollar, amplify the threats posed by the underlying predicate crimes by making crime more lucrative through money laundering expertise and economies of scale. This assessment also examines illicit trade as a money laundering threat. Trade-based money laundering (TBML) has long been viewed as a money laundering vulnerability, but trafficking in stolen goods, smuggling to avoid tariffs, and other illicit tactics also generate billions of dollars in illicit proceeds each year.

I. Fraud

Americans and the U.S. government are under attack by foreign and domestic fraudsters. Consumer and government fraud losses continue to rise year after year. In 2024, the Federal Bureau of Investigation (FBI) Internet Crime Complaint Center (IC3) received 859,532 victim complaints of suspected internet crime with losses exceeding $16 billion—a 33 percent increase in losses from 2023.[2] That total only accounts for reported losses and likely underestimates actual losses by tens of billions of dollars.[3] The U.S. Government Accountability Office (GAO) estimates the federal government loses $233-521 billion to fraud each year.[4] Fraud at this scale harms consumers, distorts financial markets, and undermines public confidence in government programs and the financial system, which weaken the economic and national security of the United States.

Fraud can be perpetrated by nation states, TCOs, domestic criminal organizations, or individuals. Fraudsters may advance their financial fraud schemes by committing other crimes such as identity theft, property theft, or unauthorized computer access. They increasingly rely on technologies to increase the scale, scope, and speed of their fraud schemes.[5] This includes using social media to place malicious advertisements and recruit victims, encrypted messaging applications to communicate with victims and co-conspirators, digital assets to receive and launder funds, and, more recently, artificial intelligence (AI) tools to create fraudulent communications, identities, and websites.[6]

2 IC3, "Internet Crime Report 2024," (April 2025) https://www.ic3.gov/AnnualReport/Reports/2024_IC3Report.pdf; *See also*, Federal Trade Commission (FTC), "New FTC Data Show a Big Jump in Reported Losses to Fraud to $12.5 Billion in 2024," (March 10, 2025) https://www.ftc.gov/news-events/news/press-releases/2025/03/new-ftc-data-show-big-jump-reported-losses-fraud-125-billion-2024.

3 In 2024, the FTC estimated up to $195.9 billion total fraud losses compared to at least $12.7 billion reported fraud losses. *See* FTC, "Protecting Older Consumers, 2024-2025" (December 2025), p. 28, https://www.ftc.gov/system/files/ftc_gov/pdf/P144400-OlderAdultsReportDec2025.pdf.

4 GAO, "2018-2022 Data Show Federal Government Loses an Estimated $233 Billion to $521 Billion Annually to Fraud, Based on Various Risk Environments," (April 2024) https://www.gao.gov/assets/gao-24-105833.pdf.

5 Financial Action Task Force (FATF), "Illicit Financial Flows from Cyber-Enabled Fraud," (November 2023) https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Illicit-financial-flows-cyber-enabled-fraud.pdf.coredownload.inline.pdf.

6 IC3, "Criminals Use Generative Artificial Intelligence to Facilitate Financial Fraud," (December 3, 2024) https://www.ic3.gov/PSA/2024/PSA241203.

Fraud losses are also increasing in part due to foreign-based TCOs that target U.S. consumers, businesses, and government programs because of the openness of the U.S. economy, the size and sophistication of the U.S. financial system, and the relative wealth of U.S. citizens and companies. TCOs can perpetrate fraud on an industrial scale while based in foreign jurisdictions where governments do not take sufficient action against criminal operations within their borders. Some TCOs have expanded their fraud operations as another illicit revenue source alongside their drug trafficking or human smuggling operations.[7] Foreign fraudsters, including TCOs, often rely on U.S.-based money mules to launder fraud proceeds through the U.S. financial system to foreign jurisdictions where the perpetrators are based.

This assessment analyzes fraud as a driver of money laundering activity based on the volume of illicit proceeds generated and the overall impact on the U.S. financial sector. Fraud can be categorized by the victim, the method, or the exploited entity, and there is often significant overlap in how schemes are classified. For example, digital asset investment schemes are both a form of investment fraud and a confidence scam, with perpetrators using similar tactics to ensnare victims, including unsolicited contact, the development of romantic or close personal relationships between perpetrator and victim, and the solicitation of taxes or fees to resolve nonexistent issues.

Investment Fraud

Investment fraud encompasses any scheme where victims invest funds based on false or misleading information. In 2024, investment fraud led to the highest victim losses reported to IC3 totaling $6.57 billion, a 44 percent increase over the prior year largely attributable to growing loss amounts related to digital asset investment schemes described below.[8] The total number of investment fraud reports and the average loss per investment fraud report have increased steadily over the past three years (See Figure 1 below). In addition to stealing from innocent investors, investment fraud also diverts capital from legitimate business, makes investors skeptical of legitimate investment opportunities and emerging technologies and industries, and ultimately harms U.S. economic and national security by impeding economic and technological development.[9]

		2022	2023	2024
IC3	Total $ Loss	$3.31 b	$4.57 b	$6.57 b
	# of Reports	30,529	39,570	47,919
	Average $ Loss	$108,478	$115,498	$137,119

Figure 1

Investment fraud schemes often start with perpetrators providing victims with unsolicited investment offers and advertising high returns with minimal risks.[10] Fraudsters purport to invest victim funds in all types of asset classes, including traditional financial assets such as securities, derivatives, and foreign currency; digital assets; real estate and construction projects; and brick-and-mortar businesses. Some perpetrators convince victims to invest in businesses that generate few or no returns while enriching themselves in the process.[11] In other cases, fraudsters make no attempt to invest victim funds or else structure their operations as Ponzi schemes by using funds from

7 *See, e.g.*, Financial Crimes Enforcement Network (FinCEN), Office of Foreign Assets Control (OFAC) & FBI, "Joint Notice on Timeshare Fraud Associated with Mexico-Based Transnational Criminal Organizations," (July 16, 2024) https://www.fincen.gov/sites/default/files/shared/FinCEN-Joint-Notice-Timeshare-Mexico-508C-FINAL.pdf.

8 IC3, "Internet Crime Report 2024," (April 2025) https://www.ic3.gov/AnnualReport/Reports/2024_IC3Report.pdf.

9 *See* DOJ, "Tech CEO Charged In Artificial Intelligence Investment Fraud Scheme," (April 9, 2025) https://www.justice.gov/usao-sdny/pr/tech-ceo-charged-artificial-intelligence-investment-fraud-scheme.

10 Office of the Comptroller of the Currency (OCC), "Financial and Investment Fraud," (accessed July 3, 2025) https://www.occ.gov/topics/consumers-and-communities/consumer-protection/fraud-resources/financial-and-investment-fraud-.html.

11 *See, e.g.*, DOJ, "Investment Scammer Sentenced to 96 Months' Imprisonment for Defrauding Alpha Influence Investors of Over $20M, " (May 7, 2025) https://www.justice.gov/usao-ut/pr/investment-scammer-sentenced-96-months-imprisonment-defrauding-alpha-influence-investors.

new investors to pay earlier investors and give the appearance of legitimate investment returns.[12] These schemes increasingly involve promises to harness new and emerging technologies, such as AI, to trade assets or disrupt existing markets.[13]

Investment fraudsters frequently target specific identity groups, often religious or ethnic communities. These affinity-based fraud schemes can be harder for law enforcement and regulators to disrupt due to tight-knit community structures that may encourage victims to resolve disputes within the group.[14] Perpetrators generally launder investment fraud proceeds by attempting to pass off the illicit proceeds as legitimate investment gains or fees when they have actually misappropriated investor funds for personal expenses, often in a lavish manner meant to convey investment success that will entice additional victims. These overt displays of wealth, such as posting bank account screenshots on social media, can indicate investment fraud.[15]

Investment fraud also includes types of securities fraud, such as "ramp-and-dump" schemes, a variation of "pump-and-dump" schemes. In many of these schemes, China-based individuals fraudulently campaign to inflate the price and volume of a stock for variable interest entities (VIEs), which are Chinese-affiliated companies listed on U.S. exchanges. This scheme operates by fraudsters impersonating real financial advisers, among others, promoting the stock on social media, and creating a false impression of market-wide buying momentum. Once the stock price has been ramped up, fraudsters "dump" their own holdings of the stock, locking in profits and sending the share price tumbling to the detriment of American retail investors and others.[16] In just the first half of 2025, the IC3 reported a 300 percent increase in victim complaints from these types of investment schemes over the previous year.[17]

12 *See, e.g.*, DOJ, "San Diego Man Who Ran $35 Million Securities Fraud and COVID-Relief Fraud Scheme Sentenced to Almost 20 Years," (February 28, 2025) https://www.justice.gov/usao-sdca/pr/san-diego-man-who-ran-35-million-securities-fraud-and-covid-relief-fraud-scheme.

13 *See, e.g.*, DOJ, "Tech CEO Charged in Artificial Intelligence Investment Fraud Scheme," (April 9, 2025) https://www.justice.gov/usao-sdny/pr/tech-ceo-charged-artificial-intelligence-investment-fraud-scheme; SEC, "SEC Charges Three Purported Crypto Asset Trading Platforms and Four Investment Clubs with Scheme That Targeted Retail Investors on Social Media" (Dec. 22, 2025) https://www.sec.gov/newsroom/press-releases/2025-144-sec-charges-three-purported-crypto-asset-trading-platforms-four-investment-clubs-scheme-targeted.

14 SEC, "Stopping Affinity Fraud in Your Community," (July 2023) https://www.investor.gov/sites/investorgov/files/2023-09/Affinity-Fraud_English.pdf

15 FTC, "Can you spot an investment scam on social media?" (May 28, 2025) https://consumer.ftc.gov/consumer-alerts/2025/05/can-you-spot-investment-scam-social-media.

16 *See, e.g.*, DOJ, "Co-CEO of Chinese Publicly Traded Technology Company and Financial Advisor Indicted for Over $100M Securities Fraud Scheme," (September 12, 2025) https://www.justice.gov/opa/pr/co-ceo-chinese-publicly-traded-technology-company-and-financial-advisor-indicted-over-100m; *see also*, DOJ, "U.S. Attorney's Office in Chicago Obtains Forfeiture of $214 Million in Proceeds From Alleged "Pump and Dump" Investment Fraud Scheme," (May 28, 2025) https://www.justice.gov/usao-ndil/pr/us-attorneys-office-chicago-obtains-forfeiture-214-million-proceeds-alleged-pump-and; DOJ, "Hong Kong Businessman Indicted for Role in Filing False SEC Investment Adviser Forms on behalf of Sham Entities Used in Ramp-and-Dump Scheme," (November 14, 2025) https://www.justice.gov/opa/pr/hong-kong-businessman-indicted-role-filing-false-sec-investment-adviser-forms-behalf-sham; SEC, "Trading Suspension Release: Smart Digital Group Limited" (September 26, 2025) https://www.sec.gov/enforcement-litigation/trading-suspensions/34-104112-ts; SEC, "Trading Suspension Release: Magnitude International Ltd" (December 4, 2025) https://www.sec.gov/files/litigation/suspensions/2025/34-104317-ts.pdf

17 IC3, "Fraudsters Target US Stock Investors through Investment Clubs Accessed on Social Media and Messaging Applications," (July 3, 2025) https://www.ic3.gov/PSA/2025/PSA250703; *see also*, SEC, "Group Chats as a Gateway to Investment Scams – Investor Alert" (December 22, 2025), https://www.investor.gov/introduction-investing/general-resources/news-alerts/alerts-bulletins/investor-alerts/gateway-to-investment-scams; Financial Industry Regulatory Authority (FINRA) "Investor Alert: Social Media 'Investment Group' Imposter Scams Continue to Rise" ("FINRA Investment Group Alert") (December 9, 2025) https://www.finra.org/investors/insights/investment-group-imposter-scams. On September 5, 2025, the SEC announced the formation of a Cross-Border Task Force to combat fraud such as "pump-and-dump" and "ramp-and-dump" schemes related to foreign-based companies. The task force also focuses on securities law violations "related to companies from foreign jurisdictions, such as China." https://www.sec.gov/newsroom/press-releases/2025-113-sec-announces-formation-cross-border-task-force-combat-fraud.

Digital Asset Investment Scams

Digital asset investment scams, some of which are commonly referred to as "pig butchering" scams, are one of the most damaging forms of investment fraud. TCOs perpetrate these scams by operating industrial-scale scam centers throughout Southeast Asia, primarily in Cambodia, Burma, and Laos, from which they operate a variety of scams targeting Americans.[18] Recent reports indicate that TCOs are expanding operations to Africa, South America, and South Asia.[19] The size and scale of these scam operations have had devastating consequences. In 2024, victims reported $5.8 billion in losses related to digital asset investment scams to the IC3, a 47 percent increase over the prior year. These figures likely represent an undercount of the true losses to victims, as disclosures to the IC3 are voluntary and victims often do not report these scams because of feelings of shame for having been deceived.

Perpetrators often contact victims on social media, dating platforms, or by SMS (text) message on mobile devices and develop relationships with victims over the course of weeks or months before gradually introducing the idea of investing in digital assets.[20] The victim then sends wire transfers or digital assets to what they believe are accounts on a purported investment platform, but the accounts are actually bank accounts or digital asset exchange accounts controlled by the TCO. In some cases, the fake entities are fraudulently registered with FinCEN as money services businesses (MSBs) and use that self-registration to appear legitimate or otherwise gain credibility.[21] The victims see falsified gains on the fake investment platform app or website, which entice them to invest even more. When victims finally attempt to cash out their investments, the perpetrators tell them they must pay taxes or fees to withdraw funds. Once victims pay these additional amounts, the perpetrators cease communicating with the victim. Many victims are then contacted by scammers posing as fictitious law firms or asset recovery companies, which can further increase financial losses to the victim, compounding the harm to the consumer.[22]

Many of the individuals perpetrating the scams may themselves be victims of human trafficking who are forced to manipulate the scam victims. The TCOs place fake job advertisements for high-paying technical jobs on social media and online employment sites to attract young workers from around the world. Once the victims arrive for the job, they are held in prison-like conditions in scam centers and forced to perpetrate scams under the threat of violence. The TCOs punish poor performance and disobedience through physical abuse and torture, sexual abuse, pay docking, and debt bondage, and may "resell" those who cannot meet sales quotas or repay recruitment debts to other criminal networks for forced labor in similar fraud schemes, domestic servitude, or sex trafficking.[23]

Perpetrators use digital assets to both lure victims into the scheme and launder the illicit proceeds. In one case,

18 *See, e.g.*, United States Institute of Peace (USIP), "Transnational Crime in Southeast Asia: A Growing Threat to Global Peace and Security," (May 2024), p. 26, https://www.usip.org/sites/default/files/2024-05/ssg_transnational-crime-southeast-asia.pdf.

19 United Nations Office on Drugs and Crime (UNODC), "Inflection Point: Global Implications of Scam Centres, Underground Banking and Illicit Online Marketplaces in Southeast Asia," (April 2025), pp. 9-10, https://www.unodc.org/roseap/uploads/documents/Publications/2025/Inflection_Point_2025.pdf; Nigerian Economic & Financial Crimes Commission (EFCC), "EFCC, NIS, NCoS Complete Deportation of 192 Foreigners Convicted for Cyber-Terrorism in Lagos," (October 18, 2025) https://www.efcc.gov.ng/news/efcc-nis-ncos-complete-deportation-of-192-foreigners-convicted-for-cyber-terrorism-in-lagos.

20 FinCEN, "FinCEN Reminds Financial Institutions to Remain Vigilant Regarding Potential Relationship Investment Scams," (February 26, 2025) https://www.fincen.gov/news/news-releases/fincen-reminds-financial-institutions-remain-vigilant-regarding-potential; FinCEN, "FinCEN Alert on Prevalent Virtual Currency Investment Scam Commonly Known as 'Pig Butchering," (September 8, 2023) https://www.fincen.gov/system/files/shared/FinCEN_Alert_Pig_Butchering_FINAL_508c.pdf; *see also*, SEC, "5 Ways Fraudsters May Lure Victims Into Scams Involving Crypto Asset Securities," (May 29, 2024) https://www.investor.gov/introduction-investing/general-resources/news-alerts/alerts-bulletins/investor-alerts/crypto-scams; SEC, "Group Chats as a Gateway to Investment Scams – Investor Alert," (December 22, 2025) https://www.investor.gov/introduction-investing/general-resources/news-alerts/alerts-bulletins/investor-alerts/gateway-to-investment-scams.

21 FinCEN, "FinCEN Alert on Fraud Schemes Abusing FinCEN's Name, Insignia, and Authorities for Financial Gain," (December 18, 2024), p. 5, https://www.fincen.gov/system/files/2024-12/Alert-FinCEN-Scams-FINAL508.pdf.

22 IC3, "Fictitious Law Firms Targeting Cryptocurrency Scam Victims Combine Multiple Exploitation Tactics While Offering to Recover Funds," (August 13, 2025) https://www.ic3.gov/PSA/2025/PSA250813; *see also*, FINRA Investment Group Alert (alerting investors that the same investment group scams targeting affinity groups through WhatsApp and social media are also being applied to crypto asset schemes).

23 U.S. Department of State (State), "2025 Trafficking in Persons Report: Cambodia," (September 2025) https://www.state.gov/reports/2025-trafficking-in-persons-report/cambodia/.

a dual citizen of China and St. Kitts and Nevis pleaded guilty to his role in laundering over $73 million from digital asset investment scams. The man instructed co-conspirators to open U.S. bank accounts established on behalf of shell companies and would monitor the receipt and execution of inter-state and international wire transfers of victim funds. The man and co-conspirators would receive victim funds in financial accounts they controlled and then monitor the conversion of victim funds to digital assets, specifically stablecoins , and the subsequent distribution to co-conspirator-controlled wallets.[24]

TCOs can launder such a large volume of illicit proceeds from these scams in part due to complicit financial institutions operating in jurisdictions with weak or nonexistent anti-money laundering/countering the financing of terrorism (AML/CFT) controls, often in the same jurisdiction as the scam compounds. One such institution is Cambodia-based Huione Group, which offers services ranging from an online marketplace selling items useful for carrying out cyber scams, to fiat currency and digital asset payment services frequently used for money laundering.[25] In October 2025, FinCEN issued a final rule pursuant to Section 311 of the USA PATRIOT Act that severed Huione Group from the U.S. financial system for laundering at least $4 billion worth of illicit proceeds between August 2021 and January 2025.[26] FinCEN's final rule noted that risks presented by Huione Group's association with illicit actors and transactions linked to illicit activity are compounded by either an absence of, or ineffective, AML/Know Your Customer policies and procedures among Huione Group's components.

In October 2025, an indictment was unsealed against the founder and chairman of the Prince Group, a multinational business conglomerate based in Cambodia, for alleged wire fraud conspiracy and money laundering conspiracy for directing Prince Group's operation of forced-labor scam compounds across Cambodia. The DOJ also filed a civil forfeiture complaint against approximately 127,271 Bitcoin, worth approximately $15 billion at the time of seizure, that are proceeds and instrumentalities of the defendant's fraud and money laundering schemes and were stored in self-hosted[27] digital asset wallets whose private keys the defendant possessed. The complaint is the largest forfeiture action in the history of the DOJ.[28] The U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC), in a coordinated action with the United Kingdom, also imposed sweeping sanctions on 146 targets within the Prince Group TCO, including its leader Chen Zhi and key enterprises such as Prince Holding Group and Prince Bank, and a multitude of investment vehicles across Asia and the Caribbean.[29] In 2025, OFAC also designated 33 other individuals and entities involved in scam centers.[30]

24 DOJ, "Foreign National Pleads Guilty to Laundering Millions in Proceeds from Cryptocurrency Investment Scams," (November 12, 2024) https://www.justice.gov/archives/opa/pr/foreign-national-pleads-guilty-laundering-millions-proceeds-cryptocurrency-investment-scams.

25 FinCEN, "FinCEN Finds Cambodia-Based Huione Group to be of Primary Money Laundering Concern, Proposes a Rule to Combat Cyber Scams and Heists," (May 1, 2025) https://www.fincen.gov/news/news-releases/fincen-finds-cambodia-based-huione-group-be-primary-money-laundering-concern.

26 FinCEN, "FinCEN Issues Final Rule Severing Huione Group from the U.S. Financial System," (October 14, 2025) https://www.fincen.gov/news/news-releases/fincen-issues-final-rule-severing-huione-group-us-financial-system.

27 Also called "non-custodial," "self-custodial," or "unhosted." See The White House, "Strengthening American Leadership in Digital Financial Technology" (July 2025), p. 33, https://www.whitehouse.gov/wp-content/uploads/2025/07/Digital-Assets-Report-EO14178.pdf.

28 DOJ, "Chairman of Prince Group Indicted for Operating Cambodian Forced Labor Scam Compounds Engaged in Cryptocurrency Fraud Schemes," (October 14, 2025) https://www.justice.gov/opa/pr/chairman-prince-group-indicted-operating-cambodian-forced-labor-scam-compounds-engaged.

29 Treasury, "U.S. and U.K. Take Largest Action Ever Targeting Cybercriminal Networks in Southeast Asia," (October 14, 2025) https://home.treasury.gov/news/press-releases/sb0278.

30 See Treasury, "Treasury Sanctions Burma Warlord and Militia Tied to Scam Center Operations," (May 5, 2025) https://home.treasury.gov/news/press-releases/sb0129; Treasury, "Treasury Takes Action Against Major Cyber Scam Facilitator," (May 29, 2025) https://home.treasury.gov/news/press-releases/sb0149; Treasury, "Treasury Sanctions Southeast Asian Networks Targeting Americans with Cyber Scams," (September 8, 2025) https://home.treasury.gov/news/press-releases/sb0237; Treasury, "Treasury Sanctions Burma Armed Group and Companies Linked to Organized Crime Targeting Americans," (November 12, 2025) https://home.treasury.gov/news/press-releases/sb0312.

Healthcare Fraud

In 2023, the Centers for Medicare and Medicaid Services reported that health spending in the United States totaled over $4.9 trillion, accounting for 17.6 percent of the country's GDP.[31] The amount of funding available for exploitation makes it an attractive target for domestic and international criminals alike. Healthcare fraud costs taxpayers between three and ten percent of total healthcare expenditures estimated between $147 billion and $490 billion.[32]

Criminals engage in several different types of healthcare fraud schemes, including kickback and referral fraud, telemedicine fraud, upcoding, unbundling, duplicate billing, false diagnosis, and fraud related to unnecessary services and equipment.[33] Complicit clinicians and administrators often work within the same networks to obscure the scheme and mask the receipt of ill-gotten funds. Business owners are also frequent offenders, either through their legal entities or as lone individuals taking advantage of insurance companies and government programs. These persons may impersonate a healthcare professional or assume the identity of another person to use their insurance.[34] Bogus claims may also be submitted for patients who do not exist. Healthcare fraud also directly intersects with government benefits fraud, primarily because the programs most targeted—such as Medicare, Medicaid, and TRICARE—are funded by taxpayer dollars and administered by government agencies.

In June 2025, the DOJ announced the results of its 2025 National Health Care Fraud Takedown (Takedown), which resulted in criminal charges against 324 defendants, including 96 doctors, nurse practitioners, pharmacists, and other licensed medical professionals, in 50 federal districts and 12 State Attorneys General's Offices across the United States, for their alleged participation in various healthcare fraud schemes involving over $14.6 billion in intended loss. The Takedown involved federal and state law enforcement agencies across the country and represents an unprecedented effort to combat healthcare fraud schemes that exploit patients and taxpayers.[35]

As part of the Takedown, the United States indicted 11 defendants in a multi-billion-dollar healthcare fraud scheme that is the largest case by loss amount ever charged by the DOJ. In the case, dubbed "Operation Gold Rush" by law enforcement, 11 defendants, including members of a TCO based in Russia and elsewhere, allegedly orchestrated a multi-billion-dollar healthcare fraud and money laundering scheme to steal from the Medicare program and private health insurance companies. The TCO purchased dozens of durable medical equipment (DME) companies that already had the ability to submit claims to Medicare and Medicare Supplemental Insurers. The TCO executed these purchases by paying foreign nationals and others to serve as nominee owners of the DME companies. The TCO then created fictitious corporate records that falsely indicated that the nominee owners controlled the DME companies when, in fact, they were controlled by the TCO's foreign-based leadership. After the TCO gained control over the DME companies, it rapidly submitted billions of dollars in false and fraudulent healthcare claims to Medicare. The TCO did so by stealing the identities and personal identifying information of more than one million Americans in all 50 states, including elderly and disabled Americans. The TCO submitted over $10.6 billion in fraudulent Medicare claims for DME.

---

31 Centers for Medicare and Medicaid Services "National Health Expenditure Data – Historical," (December 18 2024) https://www.cms.gov/data-research/statistics-trends-and-reports/national-health-expenditure-data/historical.

32 According to the GAO, over $100 billion in improper payments were made in connection with Medicare and Medicaid in 2023. This includes payments that were for an incorrect amount or should not have been made at all. This total does not include potential fraud payments made in connection with private insurance or other government healthcare programs. GAO, "Medicare and Medicaid: Additional Actions Needed to Enhance Program Integrity and Save Billions," (April 16, 2024) https://www.gao.gov/assets/gao-24-107487.pdf.

33 Upcoding is a scheme in which practitioners submit multiple claims for the same service, either to the same insurer, or multiple insurers. Unbundling refers to the submission of multiple bills for services that are supposed to be billed together at a reduced rate. This increases reimbursement unfairly.

34 FBI, "Health Care Fraud," (accessed July 2025) https://www.fbi.gov/investigate/white-collar-crime/health-care-fraud.

35 DOJ, "National Health Care Fraud Takedown Results in 324 Defendants Charged in Connection with Over $14.6 Billion in Alleged Fraud," (June 30, 2025) https://www.justice.gov/opa/pr/national-health-care-fraud-takedown-results-324-defendants-charged-connection-over-146.

In another case, two California residents pleaded guilty in connection with their roles in a nearly $16 million Medicare fraud scheme involving fake hospice companies that billed for unnecessary or non-existent services. The conspirators created four sham hospice companies—three purportedly owned by foreign nationals but controlled by the defendants—and systematically used foreign nationals' personal information to open bank accounts, submit Medicare claims, and sign leases to conceal their fraud. As part of the money laundering operation, they maintained fraudulent banking documents and identification in the names of these purported foreign owners, with one perpetrator moving approximately $3.2 million through various accounts tied to foreign nationals and the fake companies.[36]

Government Benefits Fraud

As with healthcare fraud, other government programs, including legacy COVID-19 relief programs, are targeted by foreign and domestic fraudsters due to the amount of taxpayer funds available.[37] Unchecked fraud in U.S. markets and government programs robs hardworking Americans and harms the public fisc. Law enforcement continues to uncover years-long fraud schemes that went to great lengths to launder stolen taxpayer dollars from COVID-19 relief programs, including Economic Injury Disaster Loans (EIDL), the Paycheck Protection Program (PPP), and various pandemic-associated unemployment programs. In one case, a tax preparer was found guilty by a jury for his scheme seeking more than $170 million in fraudulent tax refunds from the Internal Revenue Service (IRS) by causing more than 1,900 false tax returns to be filed with the IRS claiming COVID-19-related employment tax credits. According to documents in this case and evidence at trial, the man successfully caused the government to pay out over $55 million in refunds. Throughout the scheme he also charged clients a percentage of the refund checks as his fee and requested cash payments. He failed to report the money he received from his clients, thereby evading his own taxes.[38]

Social Security,[39] veterans' benefits,[40] nutrition programs, and other government-funded programs are often targeted by fraudsters as well. For example, in November 2025, the DOJ announced charges against the 78th defendant in the Feeding Our Future fraud scheme, a $300 million fraud scheme that exploited a federally funded child nutrition program during the COVID-19 pandemic. As set forth in the indictment, between March 2021 and February 2022, the non-profit and its president received $1.1 million in Federal Child Nutrition Program funds from Feeding Our Future. However, little of this money was used by the man to purchase food. Instead, the individual and a co-conspirator laundered most of the taxpayer dollars to their families and to themselves. The individual used his cut of the fraud proceeds to travel and to buy real estate in Minnesota.[41] The United States continues to combat government benefits fraud, in particular, rampant and pervasive fraud in such programs in Minnesota.[42] The U.S. government is currently engaged in multiple active, ongoing, and extensive investigations into the fraudulent activity that has occurred in various government programs in Minnesota, including the state's Feeding Our Future, Housing Stabilization Services, and Early Intensive Developmental and Behavioral Intervention programs.[43]

36 DOJ, "Two California Residents Please Guilty in Connection with $16M Hospice Fraud Scheme and Money Laundering Scheme," (July 8, 2025) https://www.justice.gov/opa/pr/two-california-residents-plead-guilty-connection-16m-hospice-fraud-scheme-and-money.

37 The White House, "Protecting America's Bank Account Against Fraud, Waste, and Abuse," (March 25, 2025) https://www.whitehouse.gov/presidential-actions/2025/03/protecting-americas-bank-account-against-fraud-waste-and-abuse/.

38 DOJ, "New Jersey Tax Preparer Convicted for $170 Million COVID-19 Tax Credit Scheme," (November 19, 2025) https://www.justice.gov/usao-nj/pr/new-jersey-tax-preparer-convicted-170-million-covid-19-tax-credit-scheme.

39 *See, e.g.*, DOJ, "Social Security employee pleads guilty to multimillion-dollar fraud scheme," (June 5, 2025) https://www.justice.gov/usao-sdtx/pr/social-security-employee-pleads-guilty-multimillion-dollar-fraud-scheme; DOJ, "Austin Woman Sentenced in 25-Year Social Security Scam," (August 21, 2025) https://www.justice.gov/usao-mn/pr/austin-woman-sentenced-25-year-social-security-scam.

40 *See, e.g.*, DOJ, "Three Individuals Charged in Scheme to Defraud Department of Veterans Affairs of Over $9.1M," (May 2, 2025) https://www.justice.gov/opa/pr/three-individuals-charged-scheme-defraud-department-veterans-affairs-over-91m.

41 DOJ, "78th Defendant Charged in Feeding Our Future Fraud Scheme," (November 24, 2025) https://www.justice.gov/usao-mn/pr/78th-defendant-charged-feeding-our-future-fraud-scheme.

42 FinCEN, "FinCEN Alert on Fraud Rings and Their Exploitation of Federal Child Nutrition Programs in Minnesota," (January 9, 2026) https://www.fincen.gov/system/files/2026-01/FinCEN-Alert-Federal-Child-Nutrition-Programs.pdf.

43 See Treasury, "Secretary Bessent Announces Initiatives to Combat Rampant Fraud in Minnesota," (January 9, 2026) https://home.treasury.gov/news/press-releases/sb0354; DOJ, "Six Additional Defendants Charged, One Defendant Pleads Guilty in Ongoing Fraud Schemes," (December 18, 2025) https://www.justice.gov/usao-mn/pr/six-additional-defendants-charged-one-defendant-pleads-guilty-ongoing-fraud-schemes.

In response to the ongoing wave of fraud targeting federal government programs and benefits, the Trump Administration announced the upcoming creation of a new division of the DOJ focused on national fraud enforcement.[44] The new division will enforce federal criminal and civil laws against fraud targeting federal government programs, federally funded benefits, businesses, nonprofits, and private citizens nationwide. These enforcement efforts, alongside existing initiatives across the federal government, will serve to combat efforts to exploit government programs through waste, fraud, and abuse.

Confidence Scams

Confidence scams encompass a wide variety of schemes in which perpetrators deceive or manipulate victims into making authorized payments or providing information that allows perpetrators to make payments on the victim's behalf. During a confidence scam, the victim believes they are making a legitimate transaction either to conduct normal business, resolve a technical or legal issue, or help someone in need.[45] In 2024, victims reported losses to the IC3 totaling over $5.5 billion due to various types of confidence scams.[46] As with other victim-reported loss amounts, this total likely underestimates the actual losses by billions of dollars.

Confidence scams are most often perpetrated by foreign-based fraudsters, including TCOs, gangs, or individuals, and they can carry out several different schemes using various methods.[47] Businesses and consumers are being inundated with scam messages on nearly every communication platform. According to the FTC, victims are contacted via email, phone call, text, social media, and websites/apps, all of which allow these scams to be perpetrated from anywhere in the world. Scams originating on social media account for the highest victim-reported losses, totaling nearly $1.9 billion in 2024, but scams originating from phone calls lead to the highest median victim-reported loss, at $1,500.[48] This is due in part to the fact that scammers can spoof phone numbers and caller ID information, making it easier to convince victims they are speaking to legitimate actors.[49]

Four of the most common confidence scams include business email compromise (BEC), impersonation scams, romance scams, and advance-fee scams.

Business Email Compromise

Business email compromise (BEC) perpetrators take over legitimate email addresses or create their own email addresses that appear similar to a legitimate business email address to communicate with victims.[50] Perpetrators then send false wire instructions for normal business transactions that direct the funds to bank accounts controlled by the perpetrators or their co-conspirators. BEC complaints and loss totals reported to the IC3 have been relatively

44 The White House, "Fact Sheet: President Donald J. Trump Establishes New Department of Justice Division for National Fraud Enforcement," (January 8, 2026) https://www.whitehouse.gov/fact-sheets/2026/01/fact-sheet-president-donald-j-trump-establishes-new-department-of-justice-division-for-national-fraud-enforcement/.

45 See Cybercrime section for schemes where victims are extorted or coerced into making payments or situations where unauthorized payments are made against the victim's accounts using stolen credentials.

46 IC3, "Internet Crime Report 2024," (April 2025) https://www.ic3.gov/AnnualReport/Reports/2024_IC3Report.pdf. This total includes loss amounts reported for Business Email Compromise, Tech Support, Confidence/Romance, Government Impersonation, Lottery/Sweepstakes/Inheritance, and Advance-Fee scams.

47 *See, e.g.*, DOJ, "Nigerian Man Pleads Guilty After Extradition To Participating In Romance Scams And Other Fraud Schemes Targeting Elderly Victims," (September 24, 2024) https://www.justice.gov/usao-sdny/pr/nigerian-man-pleads-guilty-after-extradition-participating-romance-scams-and-other.

48 FTC, "All Fraud Reports by Contact Method," (May 6, 2025) https://public.tableau.com/app/profile/federal.trade.commission/viz/FraudReports/PaymentContactMethods.

49 Federal Communications Commission (FCC), "Caller ID Spoofing," (updated November 13, 2024) https://www.fcc.gov/consumers/guides/spoofing.

50 *See, e.g.*, DOJ, "Nigerian National Pleads Guilty To Laundering Millions In Criminal Proceeds Linked To Romance Scams And Business Email Compromise Schemes," (March 28, 2025) https://www.justice.gov/usao-wdnc/pr/nigerian-national-pleads-guilty-laundering-millions-criminal-proceeds-linked-romance; DOJ, "Extradited Nigerian National Sentenced to Eight Years in Prison for Business Email Compromise Scheme," (December 5, 2024) https://www.justice.gov/usao-ct/pr/extradited-nigerian-national-sentenced-eight-years-prison-business-email-compromise

stable over the past three years. In 2024, the IC3 received 21,422 complaints associated with over $2.7 billion in losses, making it the second highest total loss category after investment fraud.[51]

Impersonation Scams

Impersonation scams encompass several different schemes where perpetrators pose as tech support, government employees, or bank employees[52] to convince victims to pay to resolve nonexistent technical, legal, or financial issues or give their assets to supposed government agents for safekeeping during nonexistent law enforcement investigations. Impersonation scams primarily originate from India-based call centers, but they often rely on U.S.-based money mules to receive and launder the funds.[53] Tech support scams often begin with unsolicited emails, texts, phone calls, or malicious pop-up ads stating that there is an issue with the victim's computer that must be resolved by calling tech support.[54] When victims call the provided number, scammers purport to be legitimate tech support for well-known companies and will often stay on the phone for hours to walk the victim through purchasing and activating gift cards to pay to resolve the nonexistent issue.

Government impersonation scams often begin with phone calls from scammers with spoofed numbers that appear to be from a government or law enforcement agency.[55] The scammers use an urgent or aggressive tone to convince victims they need to act quickly to resolve an issue such as paying a fine for missing jury duty or placing their assets with the government for safekeeping because their identity was used to facilitate a crime. The victims are then directed to purchase gift cards or deposit cash into a digital asset kiosk[56] to quickly pay the alleged fine.[57] In some cases, victims are directed to liquidate bank and retirement accounts and convert their assets to cash or gold bars for supposed government agents to pick up.[58] Perpetrators often target older adults in these schemes. Roughly 98 percent of these losses were reported by individuals over the age of 60.[59] Scams where victims convert their assets to gold bars, which money mules pick up can be particularly devastating.[60] In 2024, victims reported 525 such incidents to the IC3 resulting in total losses over $219,000,000, an average of over $417,000 per victim.[61]

51 IC3, "Internet Crime Report 2024," (April 2025) https://www.ic3.gov/AnnualReport/Reports/2024_IC3Report.pdf.

52 See IC3, "Account Takeover Fraud via Impersonation of Financial Institution Support," (November 25, 2025) https://www.ic3.gov/PSA/2025/PSA251125.

53 IC3, "Internet Crime Report 2022," (April 23, 2025) p.14, https://www.ic3.gov/AnnualReport/Reports/2024_IC3Report.pdf; *see, e.g.*, DOJ, "Indian Nationals Convicted of Money Laundering Conspiracy That Took Life Savings from Victims in Ohio, Michigan, Illinois, and Indiana," (February 4, 2025) https://www.justice.gov/usao-ndoh/pr/indian-nationals-convicted-money-laundering-conspiracy-took-life-savings-victims-ohio

54 FTC, "How To Spot, Avoid, and Report Tech Support Scams," (updated September 2022) https://consumer.ftc.gov/articles/how-spot-avoid-and-report-tech-support-scams.

55 Several U.S. government agencies have warned about these scams. *See, e.g.*, FinCEN, "Alert on Fraud Schemes Abusing FinCEN's Name, Insignia, and Authorities for Financial Gain," (December 18, 2024) https://www.fincen.gov/system/files/2024-12/Alert-FinCEN-Scams-FINAL508.pdf; DEA, "Scam Alert," https://www.dea.gov/scam-alert; FTC, "No, that's not an FTC commissioner on the phone," (September 19, 2025) https://consumer.ftc.gov/consumer-alerts/2025/09/no-thats-not-ftc-commissioner-phone. Fraudsters may also impersonate foreign law enforcement. See IC3, "Criminals Impersonate US Health Insurance Providers and Chinese Law Enforcement to Target Chinese Speakers Residing in the United States," (November 13, 2025) https://www.ic3.gov/PSA/2025/PSA251113.

56 See Digital Assets section for further discussion on the use of digital asset kiosks in illicit finance.

57 FinCEN, "Notice on the Use of Convertible Virtual Currency Kiosks for Scam Payments and Other Illicit Activity," (August 4, 2025), pp. 6–7, https://www.fincen.gov/sites/default/files/shared/FinCEN-Notice-CVCKIOSK.pdf.

58 FTC, "False alarm, real scam: how scammers are stealing older adults' life savings," (August 7, 2025) https://www.ftc.gov/news-events/data-visualizations/data-spotlight/2025/08/false-alarm-real-scam-how-scammers-are-stealing-older-adults-life-savings.

59 FBI, "FBI Boston Warns of Increase in Gold Bar and Bulk Cash Courier Scams," (September 22, 2025) https://www.fbi.gov/contact-us/field-offices/boston/news/fbi-boston-warns-of-increase-in-gold-bar-and-bulk-cash-courier-scams.

60 FBI, "Scammers Use Couriers to Retrieve Cash and Precious Metals from Victims of Tech Support and Government Impersonation Scams," (January 29, 2024) https://www.ic3.gov/PSA/2024/PSA240129.

61 IC3, "Internet Crime Report 2024," (April 2025) https://www.ic3.gov/AnnualReport/Reports/2024_IC3Report.pdf.

Romance Scams

Romance scammers create fake personas to pursue online relationships with victims, gain the victims' trust, and solicit funds for a variety of reasons, such as a medical bill, a plane ticket to visit the victim, or even providing a loan to their romantic partner's purported business.[62] Perpetrators will solicit their victims on social media, dating applications, text, or other messaging applications. Perpetrators, often based in Nigeria or Ghana, operate in loosely connected groups, follow similar scripts to carry out their schemes, and rely on U.S.-based money mules to launder illicit proceeds. Black Axe, a Nigeria-based TCO operating in several countries, is one prominent criminal group organizing romance and other scams.[63] Sometimes the perpetrators use romance scam victims to launder the illicit proceeds of other scams.[64]

Advance-Fee Scams

In advance-fee scams, victims receive an unsolicited notice, via email, social media, text, messaging application, or physical mail, claiming they are entitled to a large amount of cash, either from an inheritance, a lottery or sweepstakes prize, or an exclusive business opportunity. The scammers then induce victims to pay in advance to cover purported taxes or administrative fees to access the nonexistent funds, sometimes soliciting multiple rounds of payments before the victims realize they have been scammed.[65] In another variation, scammers advertise fake jobs on social media or online job forums and tell candidates they need to pay advance fees to secure the job.[66] In 2024, victims reported over $204 million in losses to the IC3 due to various advance-fee scams.[67]

Mexico-based TCOs have also targeted U.S. owners of timeshares in Mexico through advance-fee scams operating out of call centers. According to the FBI, the terrorist Cartel Jalisco Nueva Generación (CJNG), Cartel de Golfo, and the Sinaloa Cartel have been running timeshare fraud schemes to help fund their illicit efforts for over 10 years, and CJNG is the dominant cartel engaging in timeshare fraud in Mexico based on complaint reporting and financial tracing.[68] Between 2019 and 2024, approximately 6,000 U.S. victims have reported losses of approximately $350 million attributable to timeshare fraud schemes in Mexico.[69] The TCOs generally obtain information about U.S. owners of timeshares in Mexico from complicit insiders at timeshare resorts and then contact the victims claiming to represent ready buyers, renters, or investors as part of timeshare exit, re-rent, and investment scams. The perpetrators then request upfront taxes or fees to ostensibly expedite the sale. In some cases, victims are targeted for follow-up scams where the perpetrators claim to be U.S.-based law firms or U.S. or Mexican government authorities able to help recover the lost proceeds of the initial timeshare fraud.[70]

---

62 FBI, "Romance Scams," (accessed July 11, 2025) https://www.fbi.gov/how-we-can-help-you/scams-and-safety/common-frauds-and-scams/romance-scams.

63 *See, e.g.*, DOJ, "Prominent Leader Of Black Axe Extradited To United States For Conspiring To Engage In Internet Scams And Money Laundering," (December 16, 2024) https://www.justice.gov/usao-nj/pr/prominent-leader-black-axe-extradited-united-states-conspiring-engage-internet-scams-and; INTERPOL, "INTERPOL operation strikes major blow against West African financial crime," (July 16, 2024) https://www.interpol.int/en/News-and-Events/News/2024/INTERPOL-operation-strikes-major-blow-against-West-African-financial-crime.

64 *See, e.g.*, DOJ, "Pennsylvania Woman Sentenced to Federal Prison for Role in Fraud and Money Laundering Scheme," (June 10, 2025) https://www.justice.gov/usao-ndia/pr/pennsylvania-woman-sentenced-federal-prison-role-fraud-and-money-laundering-scheme.

65 DOJ, "Man Sentenced for Sweepstakes Scam Targeting Elderly," (February 7, 2025) https://www.justice.gov/usao-sdca/pr/man-sentenced-sweepstakes-scam-targeting-elderly.

66 FTC, "Job Scams Explained," (updated August 2024) https://consumer.gov/scams-identity-theft/job-scams-explained.

67 IC3, "Internet Crime Report 2024," (April 2025) https://www.ic3.gov/AnnualReport/Reports/2024_IC3Report.pdf. This total includes the "Advanced Fee" and "Lottery/Sweepstakes" categories.

68 FBI, "Mexican Cartels Target Americans in Timeshare Fraud Scams, FBI Warns," (June 7, 2024) https://www.fbi.gov/news/stories/mexican-cartels-targeting-americans-in-timeshare-fraud-scams-fbi-warns.

69 DOJ, "Senior CJNG Member Indicted on Wire Fraud, Money Laundering, and Terrorism Charges for Operating Massive Timeshare Fraud Scheme," (September 22, 2025) https://www.justice.gov/opa/pr/senior-cjng-member-indicted-wire-fraud-money-laundering-and-terrorism-charges-operating.

70 FinCEN, OFAC & FBI, "Joint Notice on Timeshare Fraud Associated with Mexico-Based Transnational Criminal Organizations," (July 16, 2024) https://www.fincen.gov/sites/default/files/shared/FinCEN-Joint-Notice-Timeshare-Mexico-508C-FINAL.pdf.

Elder Financial Exploitation

Elder financial exploitation (EFE), a form of elder abuse, involves the misuse or exploitation of an older person's money, assets, or personal information for financial gain.[71] EFE can be perpetrated by family and friends, trusted professionals, or complete strangers.[72] Older adults are often targeted in various types of theft and confidence scams because the perpetrators believe they have larger accumulated savings, declining cognitive or physical abilities, fewer social contacts that could halt the scheme, and less familiarity with technology used to perpetrate the scheme.[73] In 2024, adults aged 60 and over reported nearly $4.9 billion in total losses to the IC3 across all internet-enabled fraud and scam types, a 44 percent increase over the prior year.[74] Financial institutions submitted over 155,000 suspicious activity reports (SARs) associated with more than $27 billion in reported suspicious activity in the year after FinCEN published an EFE Advisory in June 2022.[75]

In addition to the other fraud schemes described above, older adults are also the targets of elder-specific scams, such as Medicare scams or grandparent scams. In grandparent scams, fraudsters contact victims over the phone and say that a close relative, generally a grandchild, has been arrested following a car crash or other incident and needs money for bail or legal representation. In one recent case, 25 Canadian nationals were indicted for allegedly operating a grandparent scam out of call centers in and around Montréal, Québec. The victims were convinced to provide bail money to supposed "bail bondsmen" who would come to the victim's home to collect the money. The funds were then transmitted to Canada following cash deliveries and financial transactions, sometimes involving digital assets.[76]

Special Focus: Use of AI in Fraud and Scams

Since 2022, the commercial availability of large language models (LLMs) has led to an explosion in the use of advanced AI tools. These AI tools have several useful applications, including drafting text, explaining complex topics, writing code, and generating multimedia content, including images, audio, and video. However, these same capabilities are being leveraged by fraudsters to steal from American citizens and businesses. According to the FBI, criminals use AI-generated text, images, audio, and video to commit fraud on a larger scale and increase the believability of their schemes.[77] In the first seven months of 2025, AI accounted for more than 9,000 complaints to IC3, and those AI complaints spanned all types of scams.[78]

---

71 U.S. Government, "Interagency Statement on Elder Financial Exploitation," (December 4, 2024) https://www.occ.gov/news-issuances/news-releases/2024/nr-ia-2024-130a.pdf.

72 DOJ, "Elder Justice Initiative – Financial Exploitation," (accessed July 14, 2025) https://www.justice.gov/elderjustice/financial-exploitation-0. *See also*, DOJ, "Department of Justice Releases 2025 Annual Report to Congress on Efforts to Combat Elder Fraud and Abuse," (November 17, 2025) https://www.justice.gov/opa/pr/department-justice-releases-2025-annual-report-congress-efforts-combat-elder-fraud-and-abuse.

73 See SEC Investor Alert "Spotting and Reporting Investment Scams Targeting Older Investors," (February 5, 2024), https://www.investor.gov/introduction-investing/general-resources/news-alerts/alerts-bulletins/investor-alerts/spotting-and-reporting-investment-scams-targeting-older-investors.

74 IC3, "Internet Crime Report 2024," (April 2025) https://www.ic3.gov/AnnualReport/Reports/2024_IC3Report.pdf.

75 FinCEN, "Elder Financial Exploitation: Threat Pattern & Trend Information, June 2022 to June 2023," (April 2024), p. 1, https://www.fincen.gov/sites/default/files/shared/FTA_Elder_Financial_Exploitation_508Final.pdf; FinCEN, "Advisory on Elder Financial Exploitation" (June 15, 2022) https://www.fincen.gov/system/files/advisory/2022-06-15/FinCEN%20Advisory%20Elder%20Financial%20Exploitation%20FINAL%20508.pdf.

76 DOJ, "25 Canadian Nationals Charged in Vermont in Connection with Nationwide Multimillion-Dollar 'Grandparent Scam,'" (March 4, 2025) https://www.justice.gov/usao-vt/pr/25-canadian-nationals-charged-vermont-connection-nationwide-multimillion-dollar.

77 *See, e.g.*, IC3, "Criminals Use Generative Artificial Intelligence to Facilitate Financial Fraud," (December 3, 2024) https://www.ic3.gov/PSA/2024/PSA241203; IC3, "Senior U.S. Officials Continue to be Impersonated in Malicious Messaging Campaign," (December 19, 2025) https://www.ic3.gov/PSA/2025/PSA251219; American Bankers Association and FBI, "ABA Foundation and FBI Release New Infographic to Help Americans Spot and Avoid Deepfake Scams," (September 3, 2025) https://www.aba.com/about-us/press-room/press-releases/ABA-Foundation-and-FBI-Joint-Infographic-on-Deepfake-Scams.

78 IC3, "Don't Let Scammers Ruin Your Holiday Season," (December 8, 2025) https://www.fbi.gov/news/press-releases/dont-let-scammers-ruin-your-holiday-season.

Fraudsters use AI and other technology to create fake social media profiles, voice clones, identification documents, and videos with believable depictions of public figures or even loved ones, which accelerate the existing risks of phishing (email-based), smishing (SMS text-based), vishing (voice and video-based) and social engineering by crafting highly convincing messages that are difficult for consumers to detect.[79] This includes foreign fraudsters using AI tools to assist with language translations to avoid grammatical or spelling errors when targeting U.S. victims, allowing them to send believable content to more victims faster.[80]

Law enforcement and regulators also warn that criminals can use "deepfake" media content, such as AI-generated images, video, and documents, to aid in their attempts to perpetrate fraud and bypass customer identification checks at U.S. financial institutions.[81] Criminals create these deepfake images by modifying an authentic source image or creating a synthetic image, and criminals have also combined AI-generated images with stolen or fraudulently obtained personally identifiable information (PII) or entirely fake PII to create synthetic identities. FinCEN analysis of BSA data also shows that malicious actors have successfully opened accounts using fraudulent identities suspected to have been produced with generative AI and used those accounts to receive and launder the proceeds of other fraud schemes.[82]

Update: Check Fraud

Check fraud is the illicit use of paper or digital checks to gain unauthorized access to funds. The use of checks continues to decline,[83] but check fraud remains a persistent problem for consumers, businesses, and the government.[84] Fraudsters target checks because they can be acquired and exploited using low-tech methods such as check washing and counterfeiting. According to U.S. law enforcement, a significant volume of check fraud is enabled by mail theft.[85] According to BSA reporting, the techniques used to acquire and alter stolen checks vary widely in sophistication.[86]

Criminals often target government or business checks believing the underlying accounts are well funded and will allow them to steal greater amounts.[87] Recognizing the threat posed by government check fraud, starting

79 IC3, "Senior US Officials Impersonated in Malicious Messaging Campaign," (May 15, 2025) https://www.ic3.gov/PSA/2025/PSA250515. *See also*, SEC, "Investor Alert: Artificial Intelligence and Investment Fraud," (January 25, 2024), https://www.investor.gov/introduction-investing/general-resources/news-alerts/alerts-bulletins/investor-alerts/artificial-intelligence-fraud.

80 New York State Department of Financial Services, "Cybersecurity Risks Arising from Artificial Intelligence and Strategies to Combat Related Risks," (October 16, 2024) https://www.dfs.ny.gov/industry-guidance/industry-letters/il20241016-cyber-risks-ai-and-strategies-combat-related-risks.

81 FinCEN, "Alert on Fraud Schemes Involving Deepfake Media Targeting Financial Institutions," (November 13, 2024), pp. 1–2, https://www.fincen.gov/sites/default/files/shared/FinCEN-Alert-DeepFakes-Alert508FINAL.pdf.

82 *Id*. at p. 3.

83 In 2024, checks accounted for just three percent of all consumer payments, down from seven percent in 2016. During that same period, the volume of commercial checks collected and government checks processed through the Federal Reserve also declined by 43 percent and 38 percent, respectively. Federal Reserve Financial Services, "2025 Findings from the Diary of Consumer Payment Choice," (May 2025) https://www.frbservices.org/binaries/content/assets/crsocms/news/research/2025-diary-of-consumer-payment-choice.pdf; Federal Reserve Board (FRB), "Commercial Checks Collected through the Federal Reserve--Annual Data," (updated September 4, 2025) https://www.federalreserve.gov/paymentsystems/check_commcheckcolannual.htm; FRB, "Government Checks Processed by the Federal Reserve--Annual Data," (updated September 4, 2025) https://www.federalreserve.gov/paymentsystems/check_govcheckprocannual.htm/.

84 Federal Reserve Financial Services, "Check fraud remains top threat — learn how Federal Reserve Financial Services can help," (June 3, 2025) https://www.frbservices.org/news/fed360/issues/060325/check-fraud-remains-top-threat.

85 FBI and U.S. Postal Inspection Service (USPIS), "Mail Theft-Related Check Fraud is on the Rise," (January 27, 2025) https://www.ic3.gov/PSA/2025/PSA250127; *see generally also* FinCEN, "FinCEN Alert on Nationwide Surge in Mail Theft-Related Check Fraud Schemes Targeting the U.S. Mail" (February 27, 2023) https://www.fincen.gov/system/files/shared/FinCEN%20Alert%20Mail%20Theft-Related%20Check%20Fraud%20FINAL%20508.pdf.

86 FinCEN, "Financial Trend Analysis: Mail Theft-Related Check Fraud: Threat Pattern & Trend Information, February to August 2023," (September 2024), p. 5, https://www.fincen.gov/sites/default/files/shared/FTA-Check-Fraud-FINAL508.pdf.

87 *See, e.g.*, DOJ, "Nevada Man Who Stole Over $7M in Treasury Checks, Sentenced to Six Years in Prison," (May 29, 2025) https://www.justice.gov/usao-ut/pr/nevada-man-who-stole-over-7m-treasury-checks-sentenced-six-years-prison.

September 30, 2025, the federal government stopped issuing paper checks for most federal payments, which should greatly reduce one source of check fraud.[88] Treasury was also able to recover over $1 billion in FY2024 by implementing an enhanced process using AI to mitigate check fraud in near real-time by strengthening and expediting processes to recover potentially fraudulent payments.[89]

II. Drug Trafficking

TCOs, including international drug cartels, illicitly produce and traffic drugs that pose a major threat to U.S. public health and national security. Between 1999 and 2023, more than 800,000 people in the United States died from an opioid overdose, enriching foreign-based cartels at the expense of American lives.[90] Drug overdose deaths in the United States declined nearly 24 percent from 2023 to 2024, but illicitly manufactured fentanyl continues to be the largest driver of overdose deaths and a top counternarcotics priority for the U.S. government.[91]

Western Hemisphere-based TCOs, including the Sinaloa Cartel and CJNG in Mexico, remain the dominant illicit producers and suppliers of illicit drugs, including fentanyl.[92] TCOs can use various methods to launder their drug trafficking proceeds through the U.S. financial system, posing risks to banks and MSBs, as well as non-financial businesses and professions (such as attorneys and real estate professionals). In recent years, these TCOs have increasingly used CMLNs, which move value across borders through informal value transfer systems (IVTS), TBML schemes, and digital assets.[93]

Drug trafficking is driven by the illicit proceeds that TCOs seek to gain. This section focuses on the financing related to illicit drug production such as foreign-based chemical companies supplying precursor chemicals for fentanyl and methamphetamine destined for the United States and the subsequent money laundering of illegal proceeds from the sale of all drug types by TCO threat actors and professional money launderers.[94]

Drug Types

As described in the Drug Enforcement Administration's (DEA) 2025 National Drug Threat Assessment (NDTA), fentanyl manufactured by Mexico-based drug cartels is the main driver for drug overdose deaths in the United States.[95] Fentanyl is illicitly produced using precursor chemicals that are mainly sourced from China-based chemical suppliers, as well as India-based chemical suppliers.[96] Fentanyl, which can be 50 times stronger than heroin, has

88 The White House, Exec. Order No. 14247 – Modernizing Payments To and From America's Bank Account (March 25, 2025) https://www.federalregister.gov/documents/2025/03/28/2025-05522/modernizing-payments-to-and-from-americas-bank-account; Treasury, "Treasury Announces Federal Government Will Phase Out Paper Checks on September 30th," (August 14, 2025) https://fiscal.treasury.gov/news/paper-checks-going-away.html.

89 Treasury, "Treasury Announces Enhanced Fraud Detection Processes, Including Machine Learning AI, Prevented and Recovered Over $4 Billion in Fiscal Year 2024," (October 17, 2024) https://home.treasury.gov/news/press-releases/jy2650.

90 Centers for Disease Control and Prevention (CDC), "Understanding the Opioid Overdose Epidemic," (June 9, 2025) https://www.cdc.gov/overdose-prevention/about/understanding-the-opioid-overdose-epidemic.html.

91 CDC, "CDC Reports Nearly 24% Decline in U.S. Drug Overdose Deaths," (February 25, 2025) https://www.cdc.gov/media/releases/2025/2025-cdc-reports-decline-in-us-drug-overdose-deaths.html.

92 Office of the Director of National Intelligence (ODNI), "Annual Threat Assessment of the U.S. Intelligence Community," (March 2025), p. 5, https://www.dni.gov/files/ODNI/documents/assessments/ATA-2025-Unclassified-Report.pdf.

93 See section on Chinese Money Laundering Networks. *See also*, FinCEN, "FinCEN Advisory on the Use of Chinese Money Laundering Networks by Mexico-Based Transnational Criminal Organizations to Launder Illicit Proceeds," (August 28, 2025) https://www.fincen.gov/system/files/2025-08/FinCEN-Advisory-CMLN-508.pdf.

94 According to the FinCEN Year in Review 2024, the highest percentage of active investigations (40 percent) were linked to SARs/CTRs of the Organized Crime Drug Enforcement Program. For more information, see p.2: https://www.fincen.gov/system/files/2025-08/FinCEN-Infographic-Public-2025-508.pdf.

95 DEA, "2025 National Drug Threat Assessment (NDTA)," (May 2025), https://www.dea.gov/sites/default/files/2025-07/2025NationalDrugThreatAssessment.pdf.

96 FinCEN, "Fentanyl-Related Illicit Finance: 2024 Threat Pattern & Trend Information," (April 2025), p. 12, https://www.fincen.gov/system/files/shared/FinCEN-FTA-Fentanyl.pdf; DEA, 2025 NDTA, p. 8, https://www.dea.gov/sites/default/files/2025-07/2025NationalDrugThreatAssessment.pdf.

either replaced heroin or is regularly combined with heroin and other drugs in many U.S. drug markets.[97] Between 2020 and 2024, the volume of heroin seizures in the United States declined over 77 percent, while the volume of fentanyl seizures soared nearly 250 percent.[98] Fentanyl can also be combined with other drugs, such as nitazenes (a synthetic opioid) and xylazine (a non-opioid sedative), or pressed into fake prescription pills, greatly increasing the risk of poisoning and overdose. Other drugs, such as methamphetamine and cocaine, are also produced by TCOs outside the United States, smuggled into the country, and distributed and sold by local drug trafficking organizations (DTOs) partnering with the TCOs. Marijuana, which remains strictly controlled under federal law, can also be smuggled into the United States by TCOs or produced domestically by TCOs or unaffiliated criminal groups. Seven drug types account for over 98 percent of drug trafficking offenses, with the top three related to methamphetamine (46 percent), fentanyl and analogs (22 percent), and powder cocaine (20 percent).[99]

Threat Actors

The main TCO threat actors include the Sinaloa Cartel, CJNG, Cartel del Noreste, La Nueva Familia Michoacana, Cartel del Golfo, and Carteles Unidos, all of which were designated as Foreign Terrorist Organizations (FTOs) and Specially Designated Global Terrorists (SDGTs) in 2025.[100] The United States is committed to using all tools available to counter these TCOs, which are engaged in campaigns of violence and terror against the United States and other countries in the Western Hemisphere.[101] Because the main TCO threat actors are designated terrorist groups, the United States can pursue charges like narco-terrorism and material support for terrorism, which carry long prison sentences and hefty fines.[102] The FTO designations also allow for pragmatic solutions to the massive scale of the drug problem. For instance, in September 2025 U.S. law enforcement seized 300,000 kilograms of methamphetamine precursor chemicals sent from China destined for the Sinaloa Cartel in Mexico under the terrorism forfeiture provision. Among the U.S. government's forfeiture authorities, the terrorism forfeiture provision applies to the broadest range of property and includes all foreign or domestic assets connected to a federal crime of terrorism.[103] This was the largest seizure of methamphetamine precursor chemicals in U.S. history and enough to produce roughly 190,000 kilograms of methamphetamine, with a market value of up to $569 million.[104]

Sinaloa and CJNG

The two largest TCO threat actors remain the Sinaloa Cartel and CJNG, and they continue to play an outsized role in the drug crisis, which is killing tens of thousands of Americans each year.[105] The Sinaloa Cartel, one of the most

97 The White House, "Designating Fentanyl as a Weapon of Mass Destruction," (December 15, 2025) https://www.whitehouse.gov/presidential-actions/2025/12/designating-fentanyl-as-a-weapon-of-mass-destruction/.

98 DEA, 2025 NDTA, p. 21, 33, https://www.dea.gov/sites/default/files/2025-07/2025NationalDrugThreatAssessment.pdf.

99 USSC, "QuickFacts: Drug Trafficking Offenses FY2024," (May 2025) https://www.ussc.gov/sites/default/files/pdf/research-and-publications/quick-facts/Drug_Trafficking_FY24.pdf

100 State, "Designation of International Cartels," (February 20, 2025) https://www.state.gov/designation-of-international-cartels. The two other TCOs designated as part of this order, Tren de Aragua (TdA), and Mara Salvatrucha (MS-13), primarily engage in small-scale or retail-level drug trafficking activities, such as working as drug couriers, stash house guards, and street-level drug distributors, as part of their broader criminal operations. See 2025 NDTA, pp. 18-19, https://www.dea.gov/sites/default/files/2025-07/2025NationalDrugThreatAssessment.pdf.

101 Operation Take Back America requires that the Organized Crime Drug Enforcement Task Forces (OCDETF) surge existing resources to address the Justice Department's core enforcement priorities: stopping illegal immigration, eliminating cartels and TCOs, and ending illegal trafficking of dangerous drugs and human beings. Operation Take Back America will also include all efforts to target TdA, MS-13, the Sinaloa Cartel, CJNG, Cartel del Noreste, La Nueva Familia Michoacana, Cartel del Golfo, Carteles Unidos and any other Cartel or TCO designated pursuant to the process established in Executive Order 14157. https://www.justice.gov/dag/media/1393746/dl?inline

102 *See, e.g.*, DOJ, "Sinaloa Cartel Leaders Charged with Narco-Terrorism, Material Support of Terrorism and Drug Trafficking," (May 13, 2025) https://www.justice.gov/opa/pr/sinaloa-cartel-leaders-charged-narco-terrorism-material-support-terrorism-and-drug.

103 18 U.S.C. § 981(a)(1)(G)

104 DOJ, "U.S. Seizes 300,000 Kilos of Meth Precursor Chemicals Sent from China Destined for Mexico's Sinaloa Drug Cartel," (September 3, 2025) https://www.justice.gov/usao-dc/pr/us-seizes-300000-kilos-meth-precursor-chemicals-sent-china-destined-mexicos-sinaloa-drug.

105 CDC, "Provisional Drug Overdose Death Counts," (updated August 13, 2025) https://www.cdc.gov/nchs/nvss/vsrr/drug-overdose-data.htm.

powerful and pervasive TCOs in the world, is responsible for a significant portion of fentanyl and other deadly drugs trafficked into the United States. Similarly, CJNG is a brutally violent cartel responsible for a notable share of fentanyl and other drugs illicitly entering the United States. The Sinaloa Cartel and CJNG start the drug production process for fentanyl and methamphetamine by importing precursor chemicals from China, as well as India. They operate clandestine laboratories in Mexico to produce fentanyl, methamphetamine, cocaine, and other illicit drugs which are then trafficked into the United States through multiple ports of entry.[106]

Chart 1: Key Stages of the Fentanyl Supply Chain
Precursor Chemicals: China remains the primary source for substances used to produce fentanyl, but the cartels appear to be diversifying their source of supply to include India-based suppliers. Seemingly legitimate commercial operations can be abused by criminal networks to traffic chemicals essential for fentanyl and other drugs.[107]
Production and Manufacturing: The Sinaloa Cartel and CJNG are the primary illicit producers of fentanyl destined for the United States. Pill presses, often imported from China, can be used to press fentanyl into pills that resemble prescription medications like oxycodone.[108] Fentanyl is also mixed into other drugs, including methamphetamine and cocaine.
Trafficking and Distribution: Most illicit fentanyl crosses the U.S.-Mexico border in passenger vehicles. Because of fentanyl's potency, cartels can smuggle relatively small amounts by weight, which makes it difficult to detect. Once in the United States, affiliates of the Mexican drug cartels facilitate distribution for street-level sales.
Sale and Money Laundering: To repatriate drug proceeds to Mexico, cartels use various methods like bulk cash smuggling, TBML, and professional money launderers, including CMLNs.

The Sinaloa Cartel and CJNG employ a variety of money laundering methods. They are more likely than smaller TCOs to rely upon professional money laundering services, including CMLNs, which move large sums of cash with front and shell companies and multiple bank accounts that obscure the origin of funds. In exchange for a fee, it is common for professional money launderers to act as unlicensed MSBs that: 1) deposit cash at financial institutions throughout the United States; 2) move funds by wire, checks, and inter-bank transfers; and 3) transfer money to Mexico on behalf of third parties.[109] Additionally, the Sinaloa Cartel is known to use its own affiliates to launder money from the United States into Mexico.[110]

106 See FinCEN, "Supplemental Advisory on the Procurement of Precursor Chemicals and Manufacturing Equipment Used for the Synthesis of Illicit Fentanyl and Other Synthetic Opioids" (June 20, 2024), p. 3, https://www.fincen.gov/system/files/advisory/2024-06-20/FinCEN-Supplemental-Advisory-on-Fentanyl-508C.pdf; and FinCEN, "Fentanyl-Related Illicit Finance: 2024 Threat Pattern and Trend Information" (April 2025) https://www.fincen.gov/system/files/shared/FinCEN-FTA-Fentanyl.pdf.

107 In September 2025, OFAC designated Guangzhou Tengyue Chemical Co., Ltd., a chemical company involved in the manufacture and sale of synthetic opioids. Guangzhou Tengyue exploited legitimate trade channels to traffic illicit drugs into the United States. Treasury, "Treasury Sanctions China-Based Chemical Company to Combat Synthetic Opioid Trafficking," (September 3, 2025) https://home.treasury.gov/news/press-releases/sb0235.

108 *See, e.g.*, DOJ, "Chinese Company and Three Chinese Nationals Indicted for Unlawfully Importing Pill-Making Equipment Used to Manufacture Controlled Substances," (May 12, 2025) https://www.justice.gov/opa/pr/chinese-company-and-three-chinese-nationals-indicted-unlawfully-importing-pill-making.

109 *See, e.g.*, DOJ, "Ohio Siblings Sentenced for Laundering $784,045 in Drug Proceeds," (August 21, 2025) https://www.justice.gov/opa/pr/ohio-siblings-sentenced-laundering-784045-drug-proceeds.

110 In March 2025, OFAC designated six individuals and seven entities involved in one of the Sinaloa Cartel's money laundering networks. The network's activities included the use of currency arbitrage schemes, establishing straw businesses and business representatives, and coordinating bulk cash pickups on behalf of the organization. Treasury, "Treasury Sanctions Criminal Operators and Money Launderers for the Notorious Sinaloa Cartel," (March 31, 2025) https://home.treasury.gov/news/press-releases/sb0064.

Both Sinaloa and CJNG are known to use digital assets to purchase precursor chemicals, launder and repatriate funds, and for other purposes.[111] As described in the 2025 NDTA, the use of digital assets accelerates the laundering of drug proceeds, because professional money launderers are willing to immediately release an equivalent amount of digital assets as soon as they receive bulk cash from the TCOs. In the assessment, the DEA also specifically highlights CJNG's use of digital asset exchanges to launder drug proceeds.[112]

In addition to exploiting U.S. financial institutions, the cartels similarly exploit Mexican financial institutions to repatriate and launder their funds. In June 2025, FinCEN identified three Mexico-based financial institutions as being of primary money laundering concern in connection with illicit opioid trafficking and facilitating payments for the procurement of precursor chemicals to produce fentanyl as well as laundering activities benefitting the Sinaloa Cartel, CJNG, and other TCOs.[113]

Other TCOs and Threat Actors

Compared to the Sinaloa Cartel and CJNG, other TCOs, like, Cartel del Noreste (CDN), La Nueva Familia Michoacana (LNFM), Cartel de Golfo (CDG), Carteles Unidos (CU), Tren de Aragua (TdA), and Mara Salvatrucha (MS-13) play a smaller known role in the illicit production, trafficking, and sale of drugs in the United States but also engage in a diverse range of crimes. The United States is committed to ensuring that each of these FTOs do not emerge to become the next big player in the domestic illicit drug market.[114]

The Los Mayos faction of the Sinaloa Cartel provides CDN with illicit fentanyl, methamphetamine, and cocaine, which is smuggled into the United States, and then distributed and sold through routes under control of the Sinaloa Cartel. CDN is involved in a diverse range of criminal activities, including kidnapping, extortion, vehicle theft, human smuggling, money laundering, prostitution, and armed robbery.

LNFM and CU are significant TCOs based in the Mexican state of Michoacan. CU operates as a conglomerate of several powerful factions that traffic fentanyl, methamphetamine, cocaine, and heroin. LNFM also traffics drugs to the United States and launders drug proceeds through a variety of methods, including cartel-affiliated MSBs and unsuspecting legitimate businesses.

As of 2025, CDG split into multiple factions including Los Metros and Los Escorpiones, which are fighting each other for control of trafficking routes, territory, and organizational authority. CDG generates significant revenue from its migrant-smuggling activities. While drug and human smuggling proceeds are smuggled into Mexico through bulk cash, CDG also launders money via money exchange businesses.

TdA facilitates the smuggling of Venezuelan migrants into the United States and then extorts the migrants, forcing them into prostitution or other criminal activity to pay off "debts." TdA members are suspected and/or charged with a variety of crimes including drug trafficking, murder, kidnapping, extortion, migrant smuggling, human trafficking, prostitution, organized retail crime, robberies, and document fraud.[115]

---

111 *See, e.g.*, DOJ, "Justice Department Highlights DEA Drug Seizures for First Half of 2025, Successful Operations Over the Last Several Weeks," (July 15, 2025) https://www.justice.gov/opa/pr/justice-department-highlights-dea-drug-seizures-first-half-2025-successful-operations-over; DOJ, "Federal Indictment Alleges Alliance Between Sinaloa Cartel and Money Launderers Linked to Chinese Underground Banking," (June 2024) https://www.justice.gov/archives/opa/pr/federal-indictment-alleges-alliance-between-sinaloa-cartel-and-money-launderers-linked; DOJ, "Two Chinese Chemical Company Executives Convicted And Multiple Websites And Cryptocurrency Accounts Seized In Connection With Fentanyl Precursor Importation And Money Laundering Schemes," (February 3, 2025) https://www.justice.gov/usao-sdny/pr/two-chinese-chemical-company-executives-convicted-and-multiple-websites-and-0.

112 DEA, 2025 NDTA, p.64, https://www.dea.gov/sites/default/files/2025-07/2025NationalDrugThreatAssessment.pdf.

113 FinCEN's orders were issued pursuant to 21 U.S.C. 2313a. For more information, see: https://www.fincen.gov/news/news-releases/treasury-issues-unprecedented-orders-under-powerful-new-authority-counter.

114 All descriptions found in the DEA's 2025 NDTA, pp. 11-19, https://www.dea.gov/sites/default/files/2025-07/2025NationalDrugThreatAssessment.pdf.

115 See DOJ, "Justice Department Highlights Nationwide Crackdown on Tren de Aragua," (December 18, 2025) https://www.justice.gov/opa/pr/justice-department-highlights-nationwide-crackdown-tren-de-aragua.

MS-13 is an extremely violent international criminal gang, with an estimated thousands of members located in almost all 50 U.S. states. The brutality of their violent crimes has garnered significant law enforcement and media attention. MS-13 members also engage in retail-level drug trafficking, robbery, prostitution, extortion, firearms offenses, and other crimes.

There are also many other TCOs, businesses (including unlicensed and licensed MSBs), and individuals acquiring foreign-sourced precursor chemicals or refined drugs, smuggling the drugs into the United States for sale across the country, and laundering the illicit proceeds after the substances are distributed and sold. For example, in September 2025, OFAC sanctioned a China-based chemical company and two individuals for their role in manufacturing and shipping synthetic opioids and cutting agents directly to the United States.[116]

Additional Trends

Darknet Markets

Darknet markets enable users to illegally buy and sell drugs anonymously around the world using digital assets. The dispersed and opaque nature of this dark web distribution network makes it harder to detect and interdict. During the assessment period, there were an increasing number of relevant cases in which individuals took advantage of the ease of doing business and lack of regulatory oversight and enforcement of these online platforms. For example, in April 2025 a man was sentenced to 15 years in prison for his role in a drug conspiracy that distributed a wide variety of drugs. According to court documents, the man manufactured and obtained counterfeit Oxycodone, Adderall, and Xanax pills for sale. He posted advertisements for the controlled substances on Tor2Door and four other marketplaces and accepted payment in digital assets. During the conspiracy, the man shipped counterfeit oxycodone pills to the District of Columbia at least six times. These pills contained fentanyl, a Schedule II controlled substance, and metonitazene, a Schedule I controlled substance. The man and a co-conspirator also shipped counterfeit Xanax and Adderall pills to the District multiple times.[117]

These marketplaces also enable cross-border drug transactions. In March 2025, OFAC designated Iran-based Behrouz Parsarad, the sole administrator of Nemesis, an online darknet marketplace that was the subject of an international law enforcement operation and was taken down in 2024. Prior to its takedown by law enforcement, narcotics traffickers and cybercriminals openly traded in controlled drugs and services on Nemesis, which was designed with built-in money laundering features. Nemesis had over 30,000 active users and 1,000 vendors and facilitated the sale of nearly $30 million worth of drugs around the world between 2021 and 2024, including to the United States. In addition to providing criminals with a platform to conduct transactions, Parsarad laundered digital assets for narcotics traffickers and cybercriminals active on Nemesis.[118]

Marijuana Grow Operations

Although marijuana remains strictly controlled under federal law, it is the most commonly misused drug in the United States. According to law enforcement, marijuana grow operations are often run in states where cultivation is purportedly legal under state law for medicinal or recreational purposes, such as California, Oklahoma, and Maine. Despite legalization measures, the illicit marijuana market has expanded significantly over the last two decades due to the increasingly dominant role of Chinese and other Asian TCOs.[119] These TCOs, as well as Mexico-headquartered drug cartels, are profiting as a result.[120]

---

116 Treasury, "Treasury Sanctions China-Based Chemical Company to Combat Synthetic Opioid Trafficking," (September 3, 2025) https://home.treasury.gov/news/press-releases/sb0235.

117 DOJ, "Darknet Drug Trafficker from Western Pennsylvania Sentenced in D.C. for Selling Mass Quantities of Fentanyl Online," (April 23, 2025) https://www.justice.gov/usao-wdpa/pr/darknet-drug-trafficker-western-pennsylvania-sentenced-dc-selling-mass-quantities.

118 Treasury, "Treasury Sanctions Head of Online Darknet Marketplace Tied to Fentanyl Sales," (March 4, 2025) https://home.treasury.gov/news/press-releases/sb0040.

119 See Midwest High Intensity Drug Trafficking Area (HIDTA), "Marijuana Legalization in Midwest HIDTA: The Impacts Updated," Volume 5 (July 2025), pp. 13-20, https://img1.wsimg.com/blobby/go/893a8d74-0308-463e-b5f2-5dc56ff67d71/downloads/b326f5df-cd99-4327-b0fb-f9734237bcea/Midwest%20HIDTA%202025%20Marijuana%20Impact%20Report.pdf?ver=1766163078317.

120 DEA, 2025 NDTA, pp. 48-54, https://www.dea.gov/sites/default/files/2025-07/2025NationalDrugThreatAssessment.pdf.

For example, in July 2025, seven Chinese nationals were charged in connection with a multi-million-dollar conspiracy to cultivate and distribute marijuana across the Northeast region of the United States. According to the charging documents, the defendants allegedly owned, operated or partnered with a network of interconnected grow houses in Massachusetts and Maine to cultivate and distribute kilogram-sized quantities of marijuana in bulk. Data extracted from a defendant's cell phone allegedly revealed that he helped smuggle Chinese nationals into the United States—putting them to work at one of the grow houses he controlled while keeping possession of their passports until they repaid him for the cost associated with smuggling them into the country. It is further alleged that profits from the marijuana sales, which totaled millions of dollars, were used to purchase luxury homes, automobiles, jewelry and other items in Massachusetts including to expand the enterprise through the purchase of real estate. The criminal enterprise allegedly conducted bulk cash transactions with operators located in New York.[121] According to law enforcement, Chinese groups also repatriate marijuana proceeds by exchanging cash for intra-China renminbi transfers or digital asset transfers. Marijuana proceeds being laundered and not simply being repatriated to China undergo the same process, but utilize the value transferred to China to purchase goods, which are exported from China for sale. CMLNs are associated with the laundering of proceeds for marijuana trafficking.[122]

III. Cybercrime

Cybercrime comprises a variety of different threats that pose severe risks to U.S. citizens, institutions, critical infrastructure, and the U.S. financial system. Criminals and nation-states target the U.S. to compromise its technological networks, to steal financial and intellectual property, and to generate illicit proceeds from these activities either directly through extorted or ransomed funds or by stealing personally identifiable information (PII) to use in furtherance of other frauds and schemes.

This section focuses on the main types of cybercrime perpetrated by criminals and foreign adversaries to generate and launder illicit proceeds. These activities range in size and complexity from simple identity theft to advanced malware code generation. Perpetrators of these activities similarly range from lone thieves to sophisticated criminal organizations offering cybercrime-as-a-service. Of these malicious activities, identity-related fraud and scams represent the largest threat to U.S. citizens and U.S. financial institutions. However, cybercrime often consists of complex and overlapping threats to various critical parts of the U.S. financial system.

Identity Theft

Identity theft is a grave threat to the American public and a serious risk to U.S. financial institutions that generates large volumes of illicit proceeds for money laundering activity. In 2024, the Federal Trade Commission reported over one million identity theft incidents, representing 18 percent of all consumer complaints, based on direct victim reporting.[123] In January 2024, FinCEN issued its analysis of Identity-Related Suspicious Activity, which examined activity tied to the exploitation of identity processes during account creation, account access and transaction processing. FinCEN's analysis found that approximately 1.6 million reports, or 42 percent of reports filed by reporting institutions, related to identity, representing $212 billion in suspicious activity.[124]

Identity theft allows criminals to leverage a range of ways to acquire and launder criminal proceeds. Illegally obtained identities allow criminals to maximize loan amounts or obtain funds through illegally opened or acquired

121 DOJ, "Seven Chinese Nationals Charged for Alleged Roles in Multi-Million-Dollar Money Laundering, Alien Smuggling and Drug Trafficking Enterprise," (July 8, 2025) https://www.justice.gov/usao-ma/pr/seven-chinese-nationals-charged-alleged-roles-multi-million-dollar-money-laundering.

122 FinCEN, "FinCEN Advisory on the Use of Chinese Money Laundering Networks by Mexico-Based Transnational Criminal Organizations to Launder Illicit Proceeds," (August 28, 2025), p. 3, https://www.fincen.gov/system/files/2025-08/FinCEN-Advisory-CMLN-508.pdf.

123 FTC, "Consumer Sentinel Network Data Book 2024," (March 2025) https://www.ftc.gov/system/files/ftc_gov/pdf/csn-annual-data-book-2024.pdf.

124 FinCEN, "Identity-Related Suspicious Activity: 2021 Threats and Trends," (January 2024), p. 1, https://www.fincen.gov/sites/default/files/shared/FTA_Identity_Final508.pdf.

bank, MSB, or credit accounts; divert unemployment or other government benefit funds; or file false tax returns.[125] In April 2024, FinCEN published a Notice on an increase in the use of counterfeit U.S. passport cards by individuals and fraud rings to gain access to victim accounts at financial institutions nationwide.[126] Identity thieves are also leveraging new technologies, such as artificial intelligence tools, to exploit large quantities of information and publicly available documents in the pursuit of the highly technical and sophisticated operation of identity theft.

Once fraudulent accounts have been opened and funds acquired, criminals can deposit the proceeds of their crimes into freshly opened bank or money-service accounts, such as peer-to-peer (P2P) payment platforms, or fund other payment instruments, such as prepaid cards. They may then layer and launder these funds via rapid automated clearing house (ACH) transfers or deposits into digital asset accounts, money-mule networks, or the purchase of high-value items and goods.

FinCEN's Financial Trend Analysis describes two archetypes of third-party money laundering techniques in connection with identity theft: 1) money mules: individuals who are often recruited online and receive and forward stolen funds through ACH transfers, wire payments, digital asset accounts, and cash deposits, on behalf of fraud rings; and 2) straw buyers and borrowers: individuals who let their names, social security numbers, or credit files be used to open a bank, credit card, auto loan, mortgage, or money service account for someone else. In the first case, money mules help to obscure the audit trail and flow of funds stemming from identity theft crimes, by standing between the predicate crime and final destination of these funds. In the second case, legitimate credentials let criminals bypass a bank's customer identity verification processes and place illicit proceeds into apparently normal consumer or business accounts and channels.[127]

In one representative case, six people, including four Chinese nationals who entered the United States under false pretenses, were sentenced to federal prison for their participation in a complex identity theft and financial fraud scheme that defrauded multiple domestic retailers of at least $1.2 million.[128] As part of the scheme, these six defendants stole the victims' identities—including their Social Security numbers, dates of birth, and home addresses—and used that information to make fake driver's licenses that were used to access credit in the victims' names at large national retailers.

Ransomware

Ransomware refers to a type of malicious software (malware) designed to block access to a computer system or encrypt data until a ransom is paid.[129] It is typically used by cybercriminals to extort money from individuals, businesses, or government entities. Ransomware is often delivered by phishing emails or by exploiting system vulnerabilities. Once activated, the ransomware program encrypts files or locks the system, making data inaccessible to the user, and a ransom note is displayed, demanding payment—often in decentralized or anonymity-enhanced digital assets—in exchange for the decryption key. Ransomware actors may also use "double extortion," or the threat of leaking sensitive data to the public or deleting or tampering with it if victims refuse to pay ransoms.

Ransomware criminal actors and groups continue to perpetrate crimes against critical infrastructure and across all sectors of the U.S. economy, resulting in the theft of billions of dollars from U.S. persons and businesses every

125 *See, e.g.*, IRS, "2024 Annual Report of the Identity Theft and Tax Refund Fraud ISAC," (November 2024) https://www.irs.gov/pub/newsroom/2024-isac-annual-report.pdf.

126 See generally, FinCEN, "Notice on the Use of Counterfeit U.S. Passport Cards to Perpetrate Identity Theft and Fraud Schemes at Financial Institutions" (April 15, 2024) https://www.fincen.gov/system/files/shared/FinCEN_Notice_Counterfeit_US_Passport_FINAL508.pdf.

127 FinCEN, "Identity-Related Suspicious Activity: 2021 Threats and Trends," (January 2024) https://www.fincen.gov/sites/default/files/shared/FTA_Identity_Final508.pdf.

128 DOJ, "Four Chinese National Sentenced to Federal Prison in Scheme Targeting Hundreds of U.S. Consumers and Multiple U.S. Retailers", (March 17, 2025) https://www.justice.gov/usao-cdca/pr/four-chinese-nationals-sentenced-federal-prison-scheme-targeting-hundreds-us-consumers..

129 DHS Cybersecurity & Infrastructure Security Agency (CISA), "Stop Ransomware," (accessed August 2025) https://www.cisa.gov/stopransomware.

year. According to FinCEN, between 2022 and 2024, financial institutions filed nearly 7,400 reports in connection with nearly 4,200 ransomware incidents totaling nearly $2.1 billion in ransomware payments.[130] The total number of ransomware attacks worldwide, per year, has been increasing every year; the Office of the Director of National Intelligence marked 4,591 attacks in 2023 and 5,289 attacks in 2024. Attacks in the United States accounted for about half of that global total, in part because of the broad range of profitable targets.[131]

Ransomware criminal actors continue to innovate and expand their reach, including by using "ransomware-as-a-service" models. Ransomware-as-a-service (RaaS) is a subscription-based model where administrators create an easy-to-use interface and then offer their software to affiliates to deploy attacks. Affiliates of these groups identify targets and deploy malicious software and then share a percentage of each ransom payment. They often use specialized teams for various steps in the ransomware process, including the laundering process.

One of the most prolific RaaS actors is the Russia-based LockBit group, which has targeted U.S. financial institutions and critical infrastructure, including hospitals and schools. LockBit functions via an affiliate model, employs double extortion, and has been deployed against more than 2,500 victims, who have paid more than $500 million in ransom payments.[132] In February 2024, OFAC sanctioned affiliates of the LockBit Ransomware Group, in connection with LockBit's attack on a financial institution that affected the settlement of over $9 billion worth of assets backed by U.S. Treasury securities.[133] The DOJ successfully prosecuted cases against two criminal LockBit affiliates, who deployed LockBit against 12 victims. The DOJ also successfully obtained the extradition of a LockBit developer from Israel to the District of New Jersey, where he was charged by complaint, and indicted the primary developer of LockBit as well as additional affiliates."[134]

To launder the proceeds of their crimes, ransomware criminals often turn to digital assets and related service providers to conceal and send payments that enrich themselves and their affiliates.[135] In one case an Iranian national and his co-conspirators—all of whom were overseas—caused tens of millions of dollars in losses and disrupted essential public services by deploying the Robbinhood ransomware against U.S. cities, healthcare organizations, and businesses. They attempted to launder the ransom payments through digital asset mixing services and by moving assets between different types of digital assets, a practice known as chain-hopping. They also hid their identities and activities through several technical methods, including the use of virtual private networks and servers that they operated.[136]

130 FinCEN, "Ransomware Trends in Bank Secrecy Act Data Between 2022 and 2024," (December 2025), p. 1, https://www.fincen.gov/system/files/2025-12/FTA-Ransomware.pdf.

131 Office of the Director of National Intelligence (ODNI), "Worldwide Ransomware, 2024: Increasing Rate of Attacks Tempered by Law Enforcement Disruptions," (February 2025) https://www.dni.gov/files/CTIIC/documents/products/Worldwide_Ransomware_2024.pdf.

132 DOJ, "Lockbit," (updated July 22, 2024) https://www.justice.gov/usao-nj/lockbit. Ransomware actors will often target entities that they assess are more likely to pay a ransom, focusing the attack on the victim's most sensitive data. Attackers may also use multiple forms of extortion. Ransomware actors may pressure victims to pay a ransom, for example, by stealing confidential data and threatening to publish the data.

133 OFAC, "United States Sanctions Affiliates of Russia-Based LockBit Ransomware Group," (February 20, 2024) https://home.treasury.gov/news/press-releases/jy2114.

134 DOJ, "Two Foreign Nationals Plead Guilty to Participating in LockBit Ransomware Group," (July 18, 2024) https://www.justice.gov/archives/opa/pr/two-foreign-nationals-plead-guilty-participating-lockbit-ransomware-group; DOJ, " Dual Russian And Israeli National Extradited To The United States For His Role In The LockBit Ransomware Conspiracy," (March 13, 2025) https://www.justice.gov/usao-nj/pr/dual-russian-and-israeli-national-extradited-united-states-his-role-lockbit-ransomware; DOJ, " U.S. and U.K. Disrupt LockBit Ransomware Variant," (February 20, 2024) https://www.justice.gov/archives/opa/pr/us-and-uk-disrupt-lockbit-ransomware-variant.

135 FATF, "Countering Ransomware Financing," (March 2023) https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Countering-Ransomware-Financing.pdf.coredownload.pdf

136 DOJ, "Iranian Man Pleaded Guilty to Role in Robbinhood Ransomware," (May 27, 2025) https://www.justice.gov/opa/pr/iranian-man-pleaded-guilty-role-robbinhood-ransomware.

Special Focus: Financial Sextortion

Financially motivated sexual extortion (financial sextortion) occurs when individuals, increasingly children and teens, are coerced into sending explicit images online and are subsequently extorted for money.[137] The FBI and Department of Homeland Security (DHS) have identified an exponential increase in financial sextortion offenses targeting minors since 2022, particularly boys between 14 and 17 years old. Between October 2021 and March 2023, they received over 13,000 reports of online financial sextortion of minors. The sextortion involved at least 12,600 victims and led to at least 20 suicides.[138] In September 2025, FinCEN published a Notice on financial sextortion with red flag indicators to help financial institutions identify and report suspicious activity.[139]

The perpetrators of financial sextortion are organized and deliberate, often stealing or taking images, such as profile pictures of another person similar in age to the potential victim and of differing gender to communicate with the victim through fake accounts. They may also send explicit images to the victim to gain the victim's trust and use the threat of releasing the victim's explicit content to forcibly take over the victim's account to further sextort the victim's online friends. According to the FBI, financial sextortion is often a transnational crime with perpetrators operating in West Africa and Southeast Asia targeting U.S. victims.[140] Once the perpetrator obtains an explicit video or photo, they threaten to release the compromising material unless the victim sends money or gift cards. Frequently the perpetrators demand payment with digital assets and P2P payment platforms. These payments may be received by an unwitting money mule who may also be a victim of certain criminal activity and remitted via MSBs.[141]

In one case , five U.S.-based defendants pleaded guilty to conspiring to launder proceeds for Nigerian sextortionists. According to the indictment, the conspirators used online payment systems to collect sextortion proceeds and send them to a Nigerian individual they referred to as "The Plug." The sextortionists had boys and young men create nude images. After the sextortionists received those images, they allegedly had the victims send funds to the U.S.-based money launderers through online payment systems like Apple Pay, Cash App, and Zelle. The money launderers would keep about 20 percent of the money, convert the rest to Bitcoin, and send the Bitcoin to The Plug in Nigeria, who kept a portion and then sent the remainder to the sextortionists.[142] In another case, two defendants and others attempted to extort approximately $6 million from thousands of potential victims and successfully extorted approximately $1.7 million from those victims, using Cash App and Apple Pay accounts alone.[143]

137 FBI, "Sextortion," https://www.fbi.gov/how-we-can-help-you/scams-and-safety/common-frauds-and-scams/sextortion; FBI, "FBI and Partners Issue National Public Safety Alert on Financial Sextortion Schemes," (December 19, 2022) https://www.fbi.gov/news/press-releases/fbi-and-partners-issue-national-public-safety-alert-on-financial-sextortion-schemes; ICE, "Sextortion: It's more common than you think," (updated September 18, 2025); https://www.ice.gov/features/sextortion; FBI, "FBI Issues Warning About the Increase of Financial Sextortion Scheme Targeting Minors," (October 27, 2023) https://www.fbi.gov/contact-us/field-offices/losangeles/news/fbi-issues-warning-about-the-increase-of-financial-sextortion-schemes-targeting-minors.

138 FBI, "Sextortion: A Growing Threat Targeting Minors" (January 23, 2024), https://www.fbi.gov/contact-us/field-offices/nashville/news/sextortion-a-growing-threat-targeting-minors.

139 FinCEN, "Notice on Financially Motivated Sextortion" (September 8, 2025) https://www.fincen.gov/system/files/2025-09/FinCEN-Notice-FMS-508C.pdf

140 FBI, "Sextortion: A Growing Threat Targeting Minors" (January 23, 2024), https://www.fbi.gov/contact-us/field-offices/nashville/news/sextortion-a-growing-threat-targeting-minors.

141 Ibid.

142 DOJ, "All Charged Money Launderers Tied to Nigerian Sextortion Scheme Plead Guilty," (April 3, 2025) https://www.justice.gov/usao-wdmi/pr/2025_0403_Nigerian_Sextortion_Scheme_Plea.

143 DOJ, "Delaware Woman Arrested for International Sextortion and Money Laundering Scheme" (April 12, 2024), https://www.justice.gov/archives/opa/pr/delaware-woman-arrested-international-sextortion-and-money-laundering-scheme.

IV. Professional Money Laundering

Professional money laundering (PML) networks enable other threat actors by laundering illicit proceeds for a fee. Brokers that manage PML networks may have a cover story or profession, but their primary income-generating activity is coordinating the money laundering process. PML networks are generally not involved in the predicate offenses that generate illicit proceeds, but they often commit other crimes to facilitate money laundering, such as identity theft, access device fraud, and tax evasion. PML makes crime more lucrative because it provides expertise and economies of scale, as well as repatriation of funds for transnational schemes. It also makes criminal networks more complex and difficult to unravel.

PML brokers negotiate contracts with criminal organizations that cover how the illicit proceeds will be collected, laundered, and delivered. Brokers may charge a wide range of fees, depending on how difficult each of those steps can be, as well as how difficult it may be for the broker to dispose of "dirty" cash. The money laundering methods used depend on the form in which illicit proceeds are collected, the broker's expertise or cover story, and the criminal organization's preferred method of delivery.

PML networks will launder illicit proceeds from any type of crime, but most often work for TCOs engaged in drug trafficking, human trafficking, human smuggling, or fraud. PML networks often engage in more sophisticated laundering schemes. In April 2025, three men were indicted for allegedly conspiring to launder millions of dollars of proceeds derived from drug trafficking. According to court documents, the men allegedly worked for a money laundering organization that laundered at least $30 million in proceeds related to the distribution of illegal drugs, including cocaine and fentanyl, which were unlawfully imported into the United States, typically through Mexico. The men and their co-conspirators allegedly traveled throughout the United States to collect drug proceeds. They communicated with co-conspirators in China to arrange for the laundering of these proceeds through transactions designed to conceal the illegal source of the proceeds, including disguising the source of the drug proceeds by moving money through the shipment of electronic goods to China and the Middle East.[144]

Money Mules

Money mules are people who collect or receive illicit proceeds and then transport, transfer, or convert the funds on behalf of another person or organization. Perpetrators of all types of proceeds-generating crimes may use money mules, though, like other forms of PML, they are most often involved in fraud, drug trafficking, human trafficking, and human smuggling. Criminals use money mules to create distance between themselves and the criminal activity, making it harder for law enforcement to follow the money back to those benefiting from the crime. They are also frequently used by TCOs to repatriate illicit proceeds from the United States to the foreign jurisdictions where perpetrators are based.

Criminals recruit money mules via social media, job forums, messaging applications, and word of mouth. Money mules can be unwitting, witting, or complicit, and the sophistication of their money laundering methods generally depends on their level of awareness.[145]

- Unwitting money mules are unaware they are part of a criminal network and may believe they are helping a romantic partner, assisting an unbanked individual, or performing the regular duties of a new job. They are likely to use their own identity and bank accounts, and they may keep a portion of the proceeds because they believe they are performing a legitimate job or service.

144 DOJ, "Three Members of an International Money Laundering Organization Charged with Laundering Millions of Dollars in Drug Proceeds," (April 24, 2025) https://www.justice.gov/opa/pr/three-members-international-money-laundering-organization-charged-laundering-millions.

145 FBI, "Money Mules," (accessed July 15, 2025) https://www.fbi.gov/how-we-can-help-you/scams-and-safety/common-frauds-and-scams/money-mules.

- Witting money mules ignore obvious red flags and may have been alerted by financial institutions or law enforcement that their activities are illegal. They may have been unwitting to start but continue working as a money mule after becoming aware of the illegality due to the prospect of financial gain.
- Complicit money mules understand they are part of a money laundering network. They may advertise their services to multiple criminal groups, negotiate their own fees, or recruit and train other money mules. Their money laundering methods are more complex, often involving fake or stolen identities and using bank accounts held in the name of shell companies.

Many money mules are part of diaspora communities in the United States with connections to the foreign countries where TCOs or PML networks are based. They may be U.S. citizens, authorized immigrants, or illegal aliens. According to law enforcement, recent migrants with tenuous financial circumstances, such as those on student visas that do not allow for work authorization, are particularly vulnerable to being recruited as money mules.[146]

Money mule activity varies depending on how the predicate crime generates illicit proceeds. For drug trafficking and human trafficking, money mules are frequently used to collect bulk cash proceeds. After collection, they may deposit the cash into funnel accounts, transport the cash to consolidation points for co-conspirators to launder, or smuggle the cash outside of the United States, most often to Mexico. In one case, nine money mules were indicted for allegedly conspiring to launder bulk cash into digital assets on behalf of drug cartels in Mexico and Colombia. According to the superseding indictment, the defendants and co-conspirators worked together to pick up bulk cash derived from drug sales around the United States and exchange the cash for digital assets using black market digital asset launderers. The digital assets were then converted back to cash in Mexico or Colombia and delivered to cartel leaders.[147]

For fraud and cybercrime, money mules may receive wire transfers from victims in bank accounts they control; deposit cash, checks, or money orders they receive in the mail from victims in the same accounts; or pick up cash or gold bars from victims in person. From there, they can transmit the proceeds to the perpetrators via wire transfer or digital assets and ship any cash and gold bars to PML brokers coordinating the operation. In one case, a Maryland man was sentenced to 42 months in prison for serving as an unlicensed money transmitter in connection with various romance, business email compromise, and investment schemes. His fee for receiving and transmitting victim funds was usually 20 percent or more. After receiving victim funds in personal and business bank accounts he controlled, he would transfer the funds to scheme participants overseas.[148]

Chinese Money Laundering Networks (CMLNs)

Over the past decade, Chinese money laundering networks (CMLNs) have become the dominant PMLs for DTOs and other TCOs around the world. The rise of CMLNs was originally driven, in part, by Chinese nationals' increased demand for foreign currency needed to circumvent Chinese currency controls.[149] This sustained, global demand allows CMLN brokers to charge Chinese nationals high fees to purchase currency while charging criminals supplying the illicit cash lower fees than other money launderers. According to FinCEN, over the five-year period from January 1, 2020 to December 31, 2024, financial institutions filed over 137,000 reports in connection with $312 billion in suspicious activity associated with suspected CMLN activity.[150]

146 *See also*, FinCEN, "FinCEN Advisory on the Use of Chinese Money Laundering Networks by Mexico-Based Transnational Criminal Organizations to Launder Illicit Proceeds," (August 28, 2025), pp. 2-3, https://www.fincen.gov/system/files/2025-08/FinCEN-Advisory-CMLN-508.pdf.

147 DOJ, "Fifteen Defendants Charged in Operation Targeting Conversion of Bulk U.S. Cash Proceeds from Drug Sales into Cryptocurrency for Mexican Cartels," (November 20, 2024) https://www.justice.gov/usao-sdfl/pr/fifteen-defendants-charged-operation-targeting-conversion-bulk-us-cash-proceeds-drug.

148 DOJ, "Baltimore County Man Sentenced to Federal Prison for Role in Elder Fraud Schemes," (March 4, 2025) https://www.justice.gov/usao-md/pr/baltimore-county-man-sentenced-federal-prison-role-elder-fraud-schemes.

149 FinCEN, "FinCEN Advisory on the Use of Chinese Money Laundering Networks by Mexico-Based Transnational Criminal Organizations to Launder Illicit Proceeds," (August 28, 2025), p. 5, https://www.fincen.gov/system/files/2025-08/FinCEN-Advisory-CMLN-508.pdf.

150 FinCEN, "Chinese Money Laundering Networks: 2020 - 2024 Threat Pattern & Trend Information," (August 2025), p. 1, https://www.fincen.gov/sites/default/files/shared/4000-10-INV-144549-S3F6L-FTA-CMLN-508.pdf.

For drug trafficking and other cash-generating crimes, CMLN brokers will use networks of money mules across the United States to collect illicit U.S. dollar (USD) proceeds and offer it for sale to Chinese buyers on WeChat or other messaging applications. Chinese buyers generally purchase the USD by transferring an equivalent amount of renminbi, plus fees, to the CMLN broker's bank account in China. The CMLN broker then provides the USD to the purchaser in the United States via cash, checks, or wire transfers from U.S. bank accounts funded by cash deposits made by money mules.[151] These CMLN-controlled U.S. bank accounts may be opened using fraudulent Chinese passports and held in the name of shell companies.[152] According to law enforcement, CMLNs are also increasingly exchanging USD for digital assets, particularly stablecoins, in part to avoid large intra-China bank transfers that may raise capital flight suspicions.

In June 2024, the United States unsealed a superseding indictment charging Los Angeles-based associates of Mexico's Sinaloa drug cartel with conspiring with money-laundering groups to launder drug trafficking proceeds. According to the indictment, members of the CMLN allegedly laundered the illicit drug proceeds by either delivering USD directly to their money exchange customers or by purchasing real or personal property, including luxury goods and cars to be shipped to China. They also allegedly used a variety of traditional methods to place the funds into the traditional banking system such as purchasing cashier's checks, or structuring small amounts at a time into funnel bank accounts opened for this purpose to avoid banks from reporting large cash deposits to the U.S. government.[153]

According to law enforcement, CMLNs continue to adapt their techniques. CMLN brokers use several different encrypted messaging platforms to advertise their services and communicate with money mules, USD buyers, and TCO clients. They will silo different conversations on certain encrypted messaging platforms to increase operational security. Some CMLN money mules will now collect cash from DTOs in bank parking lots and immediately deposit the funds to limit opportunities for law enforcement interdiction. When some CMLN money mules are alerted by banks that their accounts may be closed due to suspicious activity, they will surge illicit cash deposits into the account knowing that when the bank closes the account, they will receive the balance via check, effectively laundering the funds. CMLN money mules can operate dozens of accounts at several different banks under different fake identities and may not actively try to avoid account closures or BSA reporting thresholds.

CMLNs are increasingly laundering the proceeds of various fraud schemes by using wire transfers and digital assets to move illicit proceeds for foreign-based fraudsters.[154] In February 2025, three individuals, including two Chinese nationals that entered the U.S. on student visas, were arrested for allegedly setting up shell companies that laundered more than $13 million stolen from victims of digital asset investment scams. After receiving victim funds via wire transfer, the defendants allegedly transferred those funds to overseas bank accounts and other domestic businesses and used the ill-gotten gains for personal expenses.[155]

CMLNs continue to launder gift card funds obtained through fraud to purchase high-value goods, as was highlighted in the 2024 NMLRA. In April 2025, three Chinese nationals were sentenced for laundering the proceeds of various gift card fraud schemes. According to court documents, China-based TCOs acquired well over $100 million in gift cards by hacking U.S. companies, tampering with physical gift cards, and targeting U.S. citizens through romance and elder fraud schemes. They then sent the gift card data to multiple cells of Chinese nationals operating in the United

151 FinCEN, "FinCEN Advisory on the Use of Chinese Money Laundering Networks by Mexico-Based Transnational Criminal Organizations to Launder Illicit Proceeds," (August 28, 2025) https://www.fincen.gov/sites/default/files/advisory/2025-08-28/FinCEN-Advisory-CMLN-508.pdf.

152 HSI Cornerstone, "Chinese Money Laundering Organizations (CMLOs) - Use of Counterfeit Chinese Passports," (January 2024) https://content.govdelivery.com/bulletins/gd/USDHSICE-37fff16?wgt_ref=USDHSICE_WIDGET_217

153 DOJ, "Federal Indictment Alleges Alliance Between Sinaloa Cartel and Money Launderers Linked to Chinese Underground Banking," (June 18, 2024) https://www.justice.gov/archives/opa/pr/federal-indictment-alleges-alliance-between-sinaloa-cartel-and-money-launderers-linked.

154 See "Digital Assets Investment Scams" section for digital assets case example.

155 DOJ, "Three Defendants Arrested on Federal Complaints Alleging They Knowingly Received More Than $13 Million in Scam Victims' Money," (February 25, 2025) https://www.justice.gov/usao-cdca/pr/three-defendants-arrested-federal-complaints-alleging-they-knowingly-received-more-13.

States through a Chinese-based messaging platform in exchange for digital assets. Once U.S.-based cells received the gift card data, they used the gift cards to purchase high-value electronics, principally Apple products. After purchasing the Apple products, cell members consolidated the electronics in warehouses for shipment to China, Hong Kong, or countries in Southeast Asia. The cells primarily operated in states with no sales tax, such as New Hampshire, to maximize their profits.[156]

V. Human Trafficking and Human Smuggling

Human trafficking and human smuggling are both multi-billion-dollar illicit industries for TCOs that value profit over human safety and often take advantage of vulnerable people. Human trafficking and human smuggling networks both pose a serious criminal threat with devastating consequences. Illegal immigration is a central enabling factor for both human smuggling and many forms of human trafficking, generating substantial illicit proceeds for TCOs and associated networks, and creating significant risk for money laundering through the U.S. financial system. While human trafficking and human smuggling are distinct crimes, individuals who are smuggled are especially vulnerable to human trafficking and other serious crimes. Human trafficking involves the exploitation of a person for labor, services, or commercial sex, whereas human smuggling involves bringing aliens into the United States by deliberately evading immigration laws and unlawfully transporting and harboring aliens who are already unlawfully present in the United States.[157] Both crimes generate large profits, some of which are laundered through the U.S. financial system by a variety of means, including real estate and luxury goods purchases, wire transfers, credit cards, P2P payment applications, digital assets, and bulk cash transfers. The successful laundering of illicit proceeds provides further incentives to perpetrate human exploitation.

Human Trafficking

Human trafficking is a crime that involves compelling or coercing a person to provide labor, services, or commercial sex. The coercion can be subtle or overt, physical or psychological. Exploitation of a minor for commercial sex is human trafficking, regardless of whether any form of force, fraud, or coercion was used.[158] Unlike human smuggling, human trafficking does not require transportation or movement across a border and can occur within a single country, state, city, or community.[159] Victims in the United States include U.S. citizens, foreign nationals who have lawful immigration status, and individuals who are unlawfully present, particularly those who entered the United States through illegal smuggling routes and are subsequently exploited by criminal networks. Victims come from all socioeconomic backgrounds. Recent migration, substance use, mental health concerns, involvement with the child welfare system, and youth homelessness are significant risk factors for human trafficking.[160]

Human trafficking is a profitable crime, and trafficking offenses serve as a predicate for money laundering offenses.[161] In 2024, the U.S. National Human Trafficking Hotline received notification of 11,999 situations of potential human trafficking involving 21,865 victims—increases of 25 and 29 percent respectively compared to

156 DOJ, "Chinese Nationals Sentenced to Federal Prison for Participating in a Fraudulent Gift Card Conspiracy Involving the Purchase and Export of Apple Products to China," (April 22, 2025) https://www.justice.gov/usao-nh/pr/chinese-nationals-sentenced-federal-prison-participating-fraudulent-gift-card-conspiracy.

157 See, DOJ, "Human Trafficking Defined," https://www.justice.gov/humantrafficking; ICE, "Human Smuggling," (updated August 20, 2025) https://www.ice.gov/about-ice/hsi/investigate/human-smuggling.

158 DOJ, "What is Human Trafficking?" (updated June 26, 2023) https://www.justice.gov/humantrafficking/what-is-human-trafficking; State, "2024 Trafficking in Persons Report," (June 2024) https://www.state.gov/wp-content/uploads/2025/02/TIP-Report-2024_Introduction_V10_508-accessible_2.13.2025.pdf.

159 DHS, "Blue Campaign, Myths and Misconceptions," (updated August 25, 2022) https://www.dhs.gov/blue-campaign/myths-and-misconceptions.

160 National Human Trafficking Hotline, "Human Trafficking: Who is Vulnerable?" (accessed December 15, 2025) https://humantraffickinghotline.org/en/human-trafficking#:~:text=Who%20is%20Vulnerable%3F,a%20runaway%20or%20homeless%20youth; DHS, "Human Trafficking Quick Facts," (updated May 22, 2025) https://www.dhs.gov/human-trafficking-quick-facts.

161 State and Treasury, "Report to Congress on An Analysis of Anti-Money Laundering Efforts Related to Human trafficking" (October 7, 2020) https://home.treasury.gov/system/files/136/Report-Money-Laundering-Human-Trafficking.pdf.

the prior year.[162] One U.S. federal law enforcement agency initiated over 1,500 cases related to possible human trafficking between October 2023 and September 2024.[163] These law enforcement investigations and government reporting indicates that human trafficking is a multi-billion dollar criminal industry in the United States.

Data and exact estimates of criminal proceeds remain difficult to ascertain because of the illicit nature of the criminal activity. In March 2024, the United Nations (UN) International Labor Organization (ILO) estimated that forced labor generated more than $236 billion in global illicit profits annually with $52 billion in the Americas and that forced commercial sexual exploitation constitutes more than two-thirds (73 percent) of total illegal profits globally while accounting for only 27 percent of the victims.[164]

Financial activity from human trafficking intersects with the regulated financial system during the recruitment, transportation, and exploitation stages. Transactions related to human trafficking include payments associated with the transportation and housing of victims; the collection of proceeds generated by the exploitation of victims; and the movement of proceeds.[165] Designated FTOs and TCOs also fund human trafficking-related activities to generate illicit proceeds for their organizations and launder funds. TCOs invest in transportation companies, food distributors, and import/export companies to operate and conceal their trafficking-related activities. Companies that otherwise appear legitimate may be laundering money to abet human trafficking.[166]

Illicit proceeds from human trafficking can be paid in cash, electronic funds transfers/remittance systems, credit card transactions, payment apps, or digital assets. In recent years, social media platforms have emerged as a facilitator for sex trafficking.[167] In the United States, human trafficking occurs in a broad range of industries including hospitality, agriculture, healthcare (such as domestic health aides or nursing homes), forestry and logging, manufacturing, commercial cleaning services, construction, health and beauty services, peddling and begging, food service industries, salon services, domestic work, fairs and carnivals, illicit massage and escort services, and drug smuggling and distribution.[168]

In April 2025, the United States charged 27 individuals currently or formerly associated with Tren de Aragua, a FTO designated by the U.S. State Department in February 2025, with multiple crimes, including sex trafficking conspiracy.[169] According to the allegations contained in the indictments, women smuggled into the United States would pay back "debts" incurred with Tren de Aragua by engaging in commercial sex acts in the United States. Members of the criminal organization enforced compliance by threatening to kill the women and their families;

---

162 National Human Trafficking Hotline, "National Statistics, Cases Identified in 2024," (accessed December 15, 2025) https://humantraffickinghotline.org/en/statistics.

163 DHS, "Countering Human Trafficking: Fiscal Year 2024 in Review," (July 2025), https://www.dhs.gov/sites/default/files/2025-08/25_00809_ccht_fy24-year-in-review-annual-report_508.pdf.

164 International Labor Organization, United Nations, "Profits and Poverty: The Economics of Forced Labor," (March 19, 2024) https://www.ilo.org/resource/news/annual-profits-forced-labour-amount-us-236-billion-ilo-report-finds. The ILO found that traffickers and criminals are generating close to $10,000 USD per victim.

165 FinCEN, "Supplemental Advisory on Identifying and Reporting Human Trafficking and Related Activity," (October 15, 2020) https://www.fincen.gov/sites/default/files/advisory/2020-10-15/Advisory%20Human%20Trafficking%20508%20FINAL_0.pdf; *See also*, FinCEN, "Alert on Human Smuggling along the Southwest Border of the United States," (January 13, 2023) https://www.fincen.gov/sites/default/files/shared/FinCEN%20Alert%20Human%20Smuggling%20FINAL_508.pdf

166 GAO, "Trafficking and Money Laundering: Strategies Used by Criminal Groups and Terrorists and Federal Efforts to Combat Them," (December 2021), p. 10, https://www.gao.gov/assets/gao-22-104807.pdf.

167 *See, e.g.*, DOJ, "Repeat Sex Trafficker Is Sentenced To 27 Years In Prison," (July 7, 2025) https://www.justice.gov/usao-wdnc/pr/repeat-sex-trafficker-sentenced-27-years-prison.; DOJ, "St. Louis County Man Sentenced to 125 Months in Prison for Sex Trafficking of Runaway Teen," (December 11, 2025) https://www.justice.gov/usao-edmo/pr/st-louis-county-man-sentenced-125-months-prison-sex-trafficking-runaway-teen.

168 DHS, "Countering Human Trafficking: A Year in Review," (February 2024) https://www.dhs.gov/sites/default/files/2024-03/24_0223_ccht_year-in-review-annual-report_508.pdf; Polaris, "The Typology of Modern Slavery," (August 30, 2023) https://polarisproject.org/the-typology-of-modern-slavery/.

169 DOJ, "27 Members or Associates of Tren de Aragua Charged with Racketeering, Narcotics, Sex Trafficking, Robbery and Firearms Offenses," (April 21, 2025) https://www.justice.gov/opa/pr/27-members-or-associates-tren-de-aragua-charged-racketeering-narcotics-sex-trafficking.

assaulting, shooting or killing them; seizing U.S. immigration documents belonging to the women and their families; and tracking down and kidnapping women who tried to flee.

In March 2025, a mother and son were sentenced for their roles in operating massage parlors that operated as fronts for commercial sex operations. Court documents revealed that, on at least 10 occasions between June 2023 and February 2024, undercover officers purchased massages for varying dollar amounts at the parlors in Texas and New Mexico. Officers also observed the defendant's vehicle transporting Asian females directly from the airport to her massage parlors. Neighbors said the women never left the building. Searches of the premises revealed beds placed on the floors, suggesting the women lived at the massage parlors. Casino records revealed that the defendant frequently traveled to California to launder the proceeds of her illicit massage parlor businesses. Between January 2018 and August 2023, she cashed out approximately $1,771,360 in chips from the casino.[170]

Human Smuggling

Human smugglers engage in the crime of facilitating the illegal entry of individuals across international borders through deliberate evasion of immigration laws, often generating substantial illicit profits that are laundered through domestic and international financial systems. Human smuggling is an inherently transnational crime, with smugglers exploiting legitimate trade and travel routes to bring people into the United States on foot and through various means of transportation, such as planes, boats, tractor-trailers and automobiles. Smuggling networks may be linked to other forms of organized crime, such as drug trafficking, weapons smuggling and terrorism.[171] While the examples below focus on the southern border, human smugglers also operate along the northern border and other points of entry.[172]

Human smuggling networks are lucrative. In just one case, federal investigators uncovered evidence suggesting that a Guatemala-based TCO generated between $104 million and $416 million in illicit proceeds from their human smuggling activities between September 2020 and April 2023.[173] The ILO estimates that traffickers and criminals are generating close to $10,000 per victim or higher as found in U.S. cases. In one smuggling and labor trafficking scheme from 2022 to 2023, smugglers in Mexico and the United States charged individuals between $15,000 and $20,000 to cross the border into the United States.[174] The smugglers also required many victims to turn over property as collateral before leaving Mexico. As this crime generates significant profits, smugglers may pursue dangerous routes, exposing migrants to dehydration, suffocation, or other harms. Migrants frequently experience assault, rape, and extortion committed by human smugglers, who are motivated by financial gain.

In another case filed in September 2025, 12 defendants operated a prolific alien smuggling operation that facilitated the unlawful entry of Cuban nationals into the United States by preparing purported visa applications, laundering millions of dollars in payment, and exploiting the immigration process. According to the superseding indictment, from January 2021 through June 2025, the defendants promoted bogus visa services online, claiming Cuban nationals could secure U.S. entry through false claims of European citizenship. They filed hundreds of fraudulent Electronic System for Travel Authorization (ESTA) applications with U.S. Customs and Border Protection (CBP), using fake addresses and fabricated documents. The defendants charged clients between $1,500 and $40,000, sometimes even chartering private planes to move groups of aliens. Records show they spent over $2.5 million on flights alone and funneled more than $7 million through payment apps such as Zelle. Based on a financial analysis conducted of 27 known accounts associated with the

170 DOJ, "Illicit Massage Parlor Operators Sentenced," (March 19, 2025) https://www.justice.gov/usao-ndtx/pr/illicit-massage-parlor-operators-sentenced.

171 DHS, "Understanding Human Smuggling," https://www.ice.gov/about-ice/hsi/investigate/human-smuggling.

172 DOJ, "Canadian Man Arrested and Detained for Role in Deadly Alien Smuggling Conspiracy at the U.S.'s Northern Border," (July 1, 2025) https://www.justice.gov/opa/pr/canadian-man-arrested-and-detained-role-deadly-alien-smuggling-conspiracy-uss-northern.

173 DOJ, "Eight Members of Lopez Human Smuggling Organization Operating in Guatemala, Mexico, and the United States Indicted and Two Arrested" (July 25, 2024) https://www.justice.gov/usao-nm/pr/eight-members-lopez-human-smuggling-organization-operating-guatemala-mexico-and-united.; DOJ, "Nine Members of Lopez Human Smuggling Organization Plead Guilty to Federal Charges" (June 16, 2025) https://www.justice.gov/usao-nm/pr/nine-members-lopez-human-smuggling-organization-plead-guilty-federal-charges

174 DOJ, "Mexican National Admits Role in Smuggling and Labor Trafficking Scheme," (October 24, 2024) https://www.justice.gov/usao-ct/pr/mexican-national-admits-role-smuggling-and-labor-trafficking-scheme.

defendants and their co-conspirators, the alien smuggling organization took in over $18 million during the conspiracy.[175]

Cartels have increasingly diversified into human smuggling as part of their illicit money-making operations. In November 2024, two high-ranking cartel members were sentenced to prison for their roles in an extensive human smuggling conspiracy involving CDN, one of the most violent TCOs in Mexico and a U.S.-designated FTO. CDN exerts significant influence over all economic activity near Nuevo Laredo[176] and uses social media to advertise their transportations services for individuals trying to illegally enter the United States.[177] TCOs and FTOs that maintain control over drug smuggling territory also profit from this illegal activity by charging smuggling organizations a fee or tax to pass through their territories.[178]

In March 2025, Treasury took actions against the Lopez Human Smuggling Organization (HSO), a Guatemala-based TCO responsible for smuggling thousands of illegal aliens from Guatemala, through Mexico, and into the United States. Treasury's designations occurred in coordination with U.S. law enforcement actions against the Lopez HSO and a La Linea cartel member who assisted the organization's human smuggling operations across Mexico and into the United States.[179] La Linea is aligned with CJNG, an FTO-designated TCO, with CJNG serving as La Linea's supply source for cocaine, methamphetamine, and fentanyl.[180] As described above, evidence uncovered by federal investigators suggests that the Lopez HSO generated between $104 million and $416 million in illicit proceeds from their human smuggling activities between September 2020 and April 2023.[181] The Lopez HSO employed a network of mid-level smugglers to carry out the day-to-day operations and open U.S. bank accounts. In addition, the organization used P2P money transfer applications, and bulk cash to facilitate payments among co-conspirators. Members of the organization also purchased real estate and used MSBs to wire money to Lopez HSO members in Guatemala.[182]

Taken together, these cases demonstrate that illegal immigration has become a significant revenue stream for TCOs and FTOs, with human smuggling proceeds increasingly intersecting with formal financial institutions, payment platforms, and U.S.-based assets.

VI. Corruption

Corruption continues to generate significant amounts of illicit proceeds that both domestic and foreign corrupt actors alike seek to launder through the United States. Corrupt activities can include bribery, embezzlement, extortion, receipt of kickbacks, the rigging or manipulation of government contracts, various types of fraud, and a range of other activities and offenses relating to abuses of public power, position, and trust. Across domestic and foreign cases, corruption-related typologies most often involve the misuse of legal entities, the laundering of corrupt funds through real estate purchases, over- or under-invoicing for goods or services provided as part of government contracts, and bribe payments involving cash or offshore bank accounts. The United States

175 DOJ, "Twelve People Charged for Their Roles in International Alien Smuggling, Asylum Fraud, and Money Laundering Conspiracies," (September 4, 2025) https://www.justice.gov/opa/pr/twelve-people-charged-their-roles-international-alien-smuggling-asylum-fraud-and-money.

176 Treasury, "Treasury Sanctions High-Ranking Members of Foreign Terrorist Organization Cartel del Noreste," (May 21, 2025) https://home.treasury.gov/news/press-releases/sb0146.

177 ICE, "Cartel Del Noreste Members Sent to Prison for Roles in Cartel-Linked Human Smuggling Scheme," (November 4, 2024) https://www.ice.gov/news/releases/cartel-del-noreste-members-sent-prison-roles-cartel-linked-human-smuggling-scheme.

178 ICE, "Human smuggling equals grave danger, big money," (updated January 29, 2025) https://www.ice.gov/features/human-smuggling-danger.

179 Treasury, "Treasury Targets Mexico-Based Leader of Transnational Criminal Organization Responsible for Smuggling Thousands of Migrants Across the U.S. Southern Border," (March 18, 2025) https://home.treasury.gov/news/press-releases/sb0051.

180 Treasury, "Treasury Sanctions Key Members of La Linea, a Group Involved in Trafficking Fentanyl into the United States," (October 31, 2024) https://home.treasury.gov/news/press-releases/jy2704.

181 DOJ, "Eight Members of Lopez Human Smuggling Organization Operating in Guatemala, Mexico, and the United States Indicted and Two Arrested" (July 25, 2024) https://www.justice.gov/usao-nm/pr/eight-members-lopez-human-smuggling-organization-operating-guatemala-mexico-and-united.

182 DOJ, "Nine Members of Lopez Human Smuggling Organization Plead Guilty to Federal Charges" (June 16, 2025) https://www.justice.gov/usao-nm/pr/nine-members-lopez-human-smuggling-organization-plead-guilty-federal-charges.

investigates and prosecutes alleged misconduct that bears strong indicia of corrupt intent, such as substantial bribe payments, proven and sophisticated efforts to conceal bribe payments, fraudulent conduct in furtherance of bribery schemes, and efforts to obstruct justice, regardless of the nationality of the individuals or entities involved.[183]

Domestic Corruption

Corruption within the United States occurs at all levels of government—from local authorities to federal officials. Across these cases, instances of corruption increasingly involve not only officials' attempts to enrich themselves through their public positions, but also illicit actors—including TCOs and foreign governments—engaging in corrupt practices to advance their strategic interests. Domestic corruption cases vary widely in their sophistication, with some of these activities carried out through simple cash payments, and others concealed through the misuse of shell companies, consultancy fees, and bank accounts in the names of public officials' associates, among other methods.

In one case, four men, including a government contracting officer for the U.S. Agency for International Development (USAID), pleaded guilty to their roles in a decade-long bribery scheme involving at least 14 prime contracts worth more than $550 million in U.S. taxpayer dollars. According to court documents, the USAID contracting officer agreed to receive bribes in exchange for influencing contract awards. Throughout the scheme, he received cash, laptops, thousands of dollars in tickets to a suite at an NBA game, a country club wedding, downpayments on two residential mortgages, cellular phones, and jobs for relatives. The bribes were also often concealed through electronic bank transfers falsely listing him on the payroll, incorporated shell companies, and false invoices. He is alleged to have received bribes valued at more than approximately $1 million as part of the scheme.[184]

TCOs and foreign governments also attempt to engage U.S. law enforcement or other current or former public officials to seek strategic advantage. These schemes often involve cash payments to law enforcement personnel, the misuse of shell companies, or layered payments to public officials' associates. In July 2025, two CBP officers pleaded guilty to conspiring with members of a Mexican-based DTO to allow drug-laden vehicles to enter the United States free from inspection. As part of the scheme, the two men, working at California ports of entry, would let members of the DTO know what time and lane they were assigned by utilizing a secret emoji-based code. The DTO would then send the drug-laden cars through the officers' lanes, knowing that the two men would inspect these vehicles. The United States has alleged that both defendants profited handsomely, funding both domestic and international trips as well as purchases of luxury items and attempts to purchase real estate in Mexico.[185]

Foreign Corruption

Money laundering associated with foreign corruption may involve foreign corrupt proceeds either passing through the U.S. financial system or being moved to the United States, using an array of methods. Law enforcement reports that foreign corrupt actors often seek to move the proceeds of bribery, embezzlement, and other corrupt acts to the United States given the stability of the U.S. market and the potential for investment returns. Moreover, they report that—paradoxically—the strong rule of law in the United States relative to other jurisdictions helps to shield corrupt actors' proceeds from theft, extortion, or other activities. Foreign corrupt proceeds that are laundered through the United States most often involve bribe payments to government officials in developing countries, especially in Latin America, in exchange for preferential treatment or the awarding of government contracts. Officials in such countries often have the highest incentives to move their corrupt proceeds to a geographically close and stable economy with strong privacy protections, with the United States being an ideal candidate for these illicit purposes.

183 DOJ, "Guidelines for Investigations and Enforcement of the Foreign Corrupt Practices Act (FCPA)," (June 9, 2025) https://www.justice.gov/dag/media/1403031/dl.

184 DOJ, "USAID Official and Three Corporate Executives Plead Guilty to Decade-Long Bribery Scheme Involving More Than $550 Million in Contracts; Two Companies Admit Criminal Liability for Bribery Scheme and Securities Fraud," (June 12, 2025) https://www.justice.gov/usao-md/pr/usaid-officer-and-company-owners-and-three-corporate-executives-plead-guilty-decade-long.

185 DOJ, "Two CBP Officers Plead Guilty to Allowing Drugs to Enter the U.S. Through Their Inspection Lanes," (July 28, 2025) https://www.justice.gov/usao-sdca/pr/two-cbp-officers-plead-guilty-allowing-drugs-enter-us-through-their-inspection-lanes.

In one case, a Colombian national was sentenced to 12 years and seven months in prison for conspiring to launder proceeds of bribes. As part of his plea, the man admitted that while he was a port official in Colombia, he accepted at least $1,000,000 in illegal bribes that he and co-conspirators laundered to the United States from Colombia. As part of the scheme, the man and his co-conspirators laundered the funds for his benefit and used the funds to purchase luxury vehicles and pay rent on waterfront property, among other things.[186]

Given the centrality of the U.S. financial system to the global payments architecture, among other factors, funds associated with foreign bribery, embezzlement, kickbacks, or other corrupt practices have transited the United States via correspondent banking accounts and other channels. Such payments most often relate to bribes paid by foreign or domestic companies to government officials in third countries in exchange for contract awards or preferential treatment.[187] The laundering of these funds frequently involves sham invoices, over-invoicing for goods or services, domestic and foreign shell companies, and offshore bank accounts to help conceal the payments.

In December 2025, a Mexican businessman residing in the United States was convicted for his role in a scheme to bribe Mexican government officials at Petróleos Mexicanos (PEMEX), the state-owned oil company of Mexico, and its wholly owned subsidiary, PEMEX Exploración y Producción (PEP). According to court documents and evidence presented at trial, the man paid more than $150,000 in bribes to officials at PEP to retain contracts and payments from PEMEX and PEP and obtain other improper advantages in business with PEMEX and PEP, for the benefit of companies associated with him. The trial evidence showed that between approximately 2019 and 2021, the man and his co-conspirators offered to pay and paid bribes in the form of cash payments, luxury goods and other valuable items to at least three PEMEX and PEP officials in exchange for those officials taking certain actions to help companies associated with him obtain and retain business with PEMEX and PEP. Those improper advantages assisted companies associated with the man in obtaining contracts with PEMEX and PEP worth at least $2.5 million.[188]

VII. Illicit Trade

Trafficking in stolen, illicit, or regulated goods is a lucrative business that attracts criminal organizations of all sizes and levels of sophistication. For TCOs, this can also be a way to diversify illicit revenue streams and expand their areas of influence. Illicit trade is not a victimless crime; it defrauds taxpayers and deprives the government of vital revenue used to reinvest in America, while also threatening critical domestic industries, undermining consumer confidence, and weakening national security. To combat illicit trade, in August 2025 the DOJ and DHS launched a cross-agency Trade Fraud Task Force to bring robust enforcement against importers and other parties who seek to defraud the United States. The Task Force will augment the existing coordination mechanisms to aggressively pursue enforcement actions against any parties who seek to evade tariffs and other duties, as well as smugglers who seek to import prohibited goods into the American economy.[189]

Illicit trade occurs in nearly every sector of the economy, though specific schemes can vary widely depending on the type of good and existing laws and regulations. The proceeds of illicit trade are generally laundered by being passed off as legitimate trade income, bolstered by fraudulent documentation, complicit merchants, or corrupt officials. In addition to generating proceeds through illicit trade, criminals may also launder the proceeds of other crimes as

186 DOJ, "Former Colombian Port Official Sentenced to Over Twelve Years in Prison for Money Laundering ," (May 9, 2025) https://www.justice.gov/opa/pr/former-colombian-port-official-sentenced-over-twelve-years-prison-money-laundering.

187 *See, e.g.*, DOJ, "Raytheon Company to Pay Over $950M in Connection with Defective Pricing, Foreign Bribery, and Export Control Schemes," (October 16, 21024) https://www.justice.gov/archives/opa/pr/raytheon-company-pay-over-950m-connection-defective-pricing-foreign-bribery-and-export.

188 DOJ, "Texas Businessman Convicted for Scheme to Bribe Mexican Government Officials," (December 5, 2025) https://www.justice.gov/opa/pr/texas-businessman-convicted-scheme-bribe-mexican-government-officials.

189 DOJ, "Departments of Justice and Homeland Security Partnering on Cross-Agency Trade Fraud Task Force," (August 29, 2025) https://www.justice.gov/opa/pr/departments-justice-and-homeland-security-partnering-cross-agency-trade-fraud-task-force.

part of their operations in TBML schemes. The examples below highlight just some of the ways criminals use illicit trade to generate proceeds.

Oil Smuggling

In recent years, fuel theft and crude oil smuggling schemes have become the most significant non-drug revenue source for Mexico-based TCOs.[190] As described in a May 2025 FinCEN Alert, Mexico-based TCOs use complicit Mexican brokers to smuggle and sell crude oil stolen from Mexico's state-owned energy company, PEMEX, to complicit, small U.S.-based oil and natural gas importers.[191] During these transactions, the stolen and smuggled oiled is often mislabeled as "waste oil" or another supposedly hazardous material. The complicit businesses then sell the products on U.S. and global energy markets and repatriate the illicit proceeds back to Mexico.

In May 2025, OFAC sanctioned three Mexican nationals and two Mexico-based entities involved in a drug trafficking, fuel theft, and oil smuggling network that generates hundreds of millions of dollars annually for the CJNG.[192] That same month, two U.S. citizens were indicted on charges related to providing material support to CJNG for allegedly illegally importing tens of millions of dollars in crude oil and conspiring to conduct financial transactions to conceal and disguise the nature and source of the proceeds of illegally smuggled crude oil.[193]

Tariff Evasion

To import merchandise into the United States, the party making the entry must declare, among other things, the value of the goods, whether the goods are subject to tariffs, the applicable tariff rate, and the amount owed. CBP relies on these representations to levy and collect duties on imported merchandise.[194] Those seeking to evade tariffs often rely on fraudulent documents to make false representations to CBP. In one case, an Indonesian jewelry company, its Indonesian co-owner, and two other Indonesian and Italian employees were charged with engaging in a scheme to illegally evade more than $86 million in customs duties and tariffs on more than $1.2 billion in jewelry imports into the United States. According to documents filed in this case and statements made in court, the defendants engaged in at least two related and overlapping schemes. In one scheme, the company and its co-conspirators evaded duties by making jewelry in Indonesia and then shipping it to Jordan, which had a Free Trade Agreement with the United States, before sending it to the United States. The defendants then falsely claimed that the company's jewelry had been manufactured in Jordan, which avoided the duty that would otherwise apply.[195]

Complicit Merchants

Complicit merchants can aid criminal organizations by purchasing stolen goods for resale or allowing stolen goods to be sold through their markets. Depending on the type of stolen good, these transactions can occur through wholesale brokers, online marketplaces,[196] or brick-and-mortar retailers. Domestic crime rings can also generate hundreds of millions of dollars thanks to complicit merchants willing to traffic in stolen goods. In July 2025, a

190 Treasury, "Treasury Targets Major Mexican Cartel Involved in Fentanyl Trafficking and Fuel Theft," (May 1, 2025) https://home.treasury.gov/news/press-releases/sb0125.

191 See generally, FinCEN, "Alert on Oil Smuggling Schemes on the U.S. Southwest Border Associated with Mexico-Based Cartels," (May 1, 2025) https://www.fincen.gov/sites/default/files/shared/FinCEN-Alert-Oil-Smuggling-FINAL-508C.pdf.

192 Treasury, "Treasury Targets Major Mexican Cartel Involved in Fentanyl Trafficking and Fuel Theft," (May 1, 2025) https://home.treasury.gov/news/press-releases/sb0125.

193 DOJ, "Father and son indicted for providing material support to Mexican cartel engaged in terrorism," (May 30, 2025) https://www.justice.gov/usao-sdtx/pr/father-and-son-indicted-providing-material-support-mexican-cartel-engaged-terrorism.

194 *See, e.g.*, DOJ, "United States Files Complaint Against Barco Uniforms and Its Suppliers, Alleging False Claims Act Violations in Connection with Underpaid Customs Duties," (April 18, 2025) https://www.justice.gov/opa/pr/united-states-files-complaint-against-barco-uniforms-and-its-suppliers-alleging-false-claims; DOJ, "Miami Importer Pleads Guilty to Scheme to Evade U.S. Tariffs on Chinese-Made Truck Tires," (December 6, 2024) https://www.justice.gov/usao-sdfl/pr/miami-importer-pleads-guilty-scheme-evade-us-tariffs-chinese-made-truck-tires.

195 DOJ, "Indonesian Jewelry Company, Co-Owner, and Two Other Employees Charged in Large-Scale Duty and Tariff Evasion Scheme," (November 17, 2025) https://www.justice.gov/usao-nj/pr/indonesian-jewelry-company-co-owner-and-two-other-employees-charged-large-scale-duty-and.

196 *See, e.g.*, DOJ, "First of a pair of men charged in massive stolen goods trafficking scheme enters guilty plea," (September 15, 2025) https://www.justice.gov/usao-wdwa/pr/first-pair-men-charged-massive-stolen-goods-trafficking-scheme-enters-guilty-plea.

New Jersey man pleaded guilty to leading a multi-state operation that stole thousands of catalytic converters from private vehicles and receiving more than $600 million through his business by reselling the stolen catalytic converters to a metal refinery that extracted the precious metals.[197]

Complicit merchants trafficking stolen goods can also aid other TCOs that target Americans. In one case, a man pleaded guilty to receiving and purchasing stolen property, including jewelry, watches, handbags, and assorted luxury items stolen by crews based out of South America, who traveled around the United States committing burglaries. The man and his codefendant were linked to at least two dozen residential or commercial burglaries across the United States. They also purchased items at their business location in Manhattan's Diamond District from an undercover detective after the detective told the defendants that the items had been stolen.[198]

Wildlife Trafficking and Other Nature Crimes

As an update to the 2024 NMLRA's section on wildlife trafficking and other nature crimes, Treasury continues to monitor the intersection of this criminal activity with other threats like drug trafficking and transnational organized crime. Nature crimes include illicit forms of logging, mining, wildlife trade,[199] land conversion, and associated criminal activities, as well as crimes associated with illegal unreported and unregulated (IUU) fishing.[200] This broad category of crime involves illicit actors misusing the international financial system to launder associated illicit proceeds, gain unfair competitive advantages over American businesses, and rob our country of its natural beauty and resources.[201]

The United States has sought to cut off revenue from TCOs benefitting from nature crimes, including IUU fishing. For instance, in November 2024, OFAC sanctioned five Mexican nationals associated with CDG and criminal activities associated with IUU fishing. Often, IUU fishing is a revenue stream for a growing number of criminal organizations, and their illicit activities can represent unfair competition for legal fishing by U.S. fishermen. IUU fishing is also a threat to U.S. maritime security, as criminal organizations may use the same vessels for smuggling narcotics and humans across borders.[202]

Illicit actors continue to target the U.S. financial system to facilitate large gold smuggling and money laundering schemes. According to allegations in the indictment in one recent case, three individuals received shipments from a Colombian company that purported to contain various types of metal widgets when, in fact, half of the packages would contain undeclared gold cylinders that were inserted within the widgets and painted over to avoid detection. The individuals would extract the gold cylinders, sell the gold through two U.S. corporate entities, and then wire the funds between the entities' bank accounts before ultimately wiring the funds to the Colombian company's accounts in Colombia.[203] Additionally, OFAC sanctioned members of one of Guyana's wealthiest families and their company for promoting public corruption through the exploitation of the country's gold sector. For example, the entity paid bribes to Guyanese government officials to facilitate the award of government contracts. Once mined, Guyana-origin gold is sold and traded throughout international markets, including the United States.[204]

---

197 DOJ, "Leader of National Catalytic Converter Theft Ring Pleads Guilty and Admits to Selling Stolen Goods for More Than $600M," (July 21, 2025) https://www.justice.gov/opa/pr/leader-national-catalytic-converter-theft-ring-pleads-guilty-and-admits-selling-stolen-goods.

198 DOJ, " Diamond District Fence Pleads Guilty in Connection with Large Scale Stolen Property Operation," (July 18, 2025) https://www.justice.gov/usao-edny/pr/diamond-district-fence-pleads-guilty-connection-large-scale-stolen-property-operation.

199 *See, e.g.*, DOJ, "Chinese National Sentenced for Smuggling Turtles from the United States to Hong Kong," (March 14, 2025) https://www.justice.gov/opa/pr/chinese-national-sentenced-smuggling-turtles-united-states-hong-kong.

200 Conversely, the definition of the term "environmental crime" varies from jurisdiction to jurisdiction.

201 Globally, nature crime also has a significant negative impact on local communities that might otherwise benefit from tourism, or legal, sustainable trade. In smaller countries (such as in the Pacific Islands region and certain African countries like Madagascar), the loss of revenue has an outsized impact on the economy.

202 Treasury, "Treasury Targets Cartel-Enabled Illegal, Unreported, and Unregulated Fishing Operations," (November 6, 2024) https://home.treasury.gov/news/press-releases/jy2729.

203 DOJ, "Three Indicted for Elaborate $24 Million Transnational Gold Smuggling and Money Laundering Scheme," (June 13, 2025) https://www.justice.gov/usao-sdfl/pr/three-indicted-24-million-transnational-gold-smuggling-and-money-laundering-scheme.

204 Treasury, "Treasury Targets Corruption Network in Guyana," (June 11, 2024)https://home.treasury.gov/news/press-releases/jy2401; DOJ, "Former Guyanese Presidential Candidate and Businessman Charged in $50 Million Tax Evasion and Money Laundering Scheme," (November 28, 2025) https://www.justice.gov/usao-sdfl/pr/former-guyanese-presidential-candidate-and-businessman-charged-50-million-tax-evasion.

VULNERABILITIES

A money laundering vulnerability is something that facilitates or creates the opportunity to launder money. Vulnerabilities may relate to a specific financial sector or product or a weakness in regulation, supervision, or enforcement. They may also reflect unique circumstances in which it may be difficult to distinguish legal and illegal activity. The methods that allow for the largest amount of money to be laundered quickly or with little risk of being caught present the greatest potential vulnerabilities. This assessment primarily examines the residual risk of a particular sector or service, taking into consideration any remaining inherent risk after accounting for the effect of mitigating measures including regulation, supervision, and enforcement, among other factors.

Financial institutions and other entities are subject to varying degrees of AML/CFT requirements depending on the inherent risk of their operations. There are more tailored requirements for certain types of financial transactions and entities that are more vulnerable to money laundering abuse, such as certain cash transactions, non-financed residential real estate transfers, and foreign companies that are non-transparent about their beneficial owners. Most U.S. financial institutions carry out their legal and regulatory requirements to prevent, detect, and report potential money laundering, sanctions evasion and other financial crimes. The small minority of regulated entities that fail to meet their requirements, negligently or complicity, are subject to dissuasive penalties.

Illicit actors will always exist and find ways to penetrate even the most highly regulated financial sectors and products. As illicit actors modify and shift their tactics and techniques, U.S. authorities respond and adapt law enforcement strategies and regulatory policies to hold illicit actors accountable. Countering illicit finance should ultimately allow legitimate business to flourish. Policies, regulations, and investigations must be balanced and not impose disproportionate costs on U.S. persons and businesses with little or marginal benefits for U.S. law enforcement.

VIII. Financial Institutions and Related Entities

Banks

Banks are the backbone of the U.S. financial system and a critical component of the global financial system.[205] As of December 2025, U.S. commercial banks and credit unions held roughly $27 trillion in total assets.[206] The banking sector is not monolithic; the top ten largest U.S. banks account for roughly half of total commercial bank assets, and roughly 60 percent of the 3,800 commercial banks in the United States have $500 million or less in total assets.[207] Supervision of all parts of the banking sector is mature and robust, as the BSA is over half a century old. The various supervisory agencies coordinate effectively at both the state and federal levels, and most banks have robust AML/CFT programs that successfully prevent, identify, and counter illicit activity.

Banks remain a key vector through which criminals seek to move funds given the sheer volume of financial activity in the banking sector. U.S. banks face a wide range of money laundering risks that are influenced by their customer base, financial products and services offered, distribution channels, and geographic footprint, among several other factors. Most of these risks are mitigated by vigilance and strong AML/CFT programs, as only one percent of banks are subject to AML/CFT enforcement actions annually. These robust and public enforcement actions serve to both deter similar behavior and educate the banking sector on how to mitigate risks.

---

205 Banks include commercial banks, private banks, savings banks, industrial banks, savings and loan associations, credit unions, and other types of entities. See 31 CFR 1010.100(d).

206 FRB, "Assets and Liabilities of Commercial Banks in the United States – H.8," (December 31, 2025) https://www.federalreserve.gov/releases/h8/current/default.htm; National Credit Union Administration (NCUA), "NCUA Releases Third Quarter 2025 Credit Union System Performance Data," (December 5, 2025) https://ncua.gov/newsroom/press-release/2025/ncua-releases-third-quarter-2025-credit-union-system-performance-data.

207 Federal Deposit Insurance Corporation (FDIC), "Summary of deposits—Summary Tables, National Totals by Asset Size" (updated June 30, 2025) https://banks.data.fdic.gov/bankfind-suite/SOD/summaryTables.

While infrequent, enforcement actions can reveal important illicit finance trends. Since January 1, 2024, the federal financial institution regulatory agencies have issued 33 cease-and-desist or consent orders, made seven formal agreements, and assessed five civil money penalties totaling over $2 billion against five banks for AML/CFT compliance deficiencies.[208] Many of these deficiencies are related to the threats described in this assessment, particularly criminal groups seeking to misuse banks to deposit bulk cash and facilitate complex money laundering schemes. While these groups can sometimes succeed in leveraging financial services to perpetuate illicit activity, banks generally identify TCO typologies (e.g. bulk cash deposits) through effective transaction monitoring systems and suspicious activity report/currency transaction report (SAR/CTR) filing, as these are less frequently cited as parts of banks' remedial actions in public enforcement actions. Banks OFAC sanctions compliance programs are also generally adept at identifying economic sanctions violations, as less than one third of enforcement actions during this reporting period required remedial actions related to OFAC sanctions programs.

While most banks establish appropriately risk-based AML/CFT programs, a review of recent AML/CFT-related enforcement actions shows that remedial actions often include directing banks to make meaningful improvements in identifying and understanding the money laundering and terrorist financing-related risks posed by illicit actors. The most common component of a bank's AML/CFT program cited in enforcement actions was deficiencies in internal controls (i.e., insufficient policies, procedures and processes to manage risks), deficiencies related to the BSA Officer, and insufficient customer due diligence (CDD) programs. While banks have long established CDD programs, even before the formal requirements of the CDD Rule went into effect in May 2018, banks recognize that changes in customer behavior and market dynamics necessitate constant vigilance and adaptations of these programs.

As banks must continuously adapt their programs to keep pace with new risks, the current Administration remains focused on better calibrating the balance between burden and outcomes. There are ongoing efforts to modernize the BSA AML/CFT regime in the United States so that it is effective, risk-based, and focused on the greatest threats to financial institutions and national security. Excessive compliance burdens not based on risk can result in resource expenditures that are not commensurate with the intended effect of securing financial institutions from illicit finance schemes.

Banks face pressure to onboard new customers quickly to compete with other emerging financial service providers. In line with the broader trend of industry consolidation, bank mergers and acquisitions can also lead some banks to acquire new customers. As these customers would have been vetted and onboarded through different procedures, the acquiring bank might face difficulties in understanding and mitigating these customers' risks. Other common deficiencies include not appropriately assessing the risks of new products and services and adopting new AML/CFT solutions through third party relationships with service providers that introduce vulnerabilities that can be exploited by illicit actors.

Case Studies:

- **TD Bank:** According to court documents and enforcement actions published by various regulators, between January 2014 and October 2023, TD Bank had long-term, pervasive, and systemic deficiencies in its U.S. AML policies, procedures, and controls but failed to take appropriate remedial action. Instead, senior executives at TD Bank enforced a budget mandate, referred to internally as a "flat cost paradigm," that set expectations that TD Bank's AML budget not increase year-over-year, despite its profits and risk profile increasing significantly over the same period. Although TD Bank maintained elements of an AML program that appeared adequate on paper, fundamental, widespread flaws in its AML program made TD Bank an "easy target" for perpetrators of financial crime. The DOJ, FinCEN, Office of the Comptroller of the Currency (OCC), and Federal Reserve Board (FRB) took parallel criminal and regulatory actions against TD Bank and announced penalties totaling approximately $3.1 billion.[209]

208 Three banks received both a cease-and-desist order and a civil monetary penalty during the assessment period.

209 DOJ, "TD Bank Pleads Guilty to Bank Secrecy Act and Money Laundering Conspiracy Violations in $1.8B Resolution," (October 10, 2024) https://www.justice.gov/archives/opa/pr/td-bank-pleads-guilty-bank-secrecy-act-and-money-laundering-conspiracy-violations-18b; FinCEN, " FinCEN Assesses Record $1.3 Billion Penalty against TD Bank," (October 10, 2024) https://www.fincen.gov/news/news-releases/fincen-assesses-record-13-billion-penalty-against-td-bank; OCC, "OCC Issues Cease and Desist Order, Assesses $450 Million Civil Money Penalty, and Imposes Growth Restriction Upon TD Bank, N.A. for BSA/AML Deficiencies," (October 10, 2024) https://www.occ.treas.gov/news-issuances/news-releases/2024/nr-occ-2024-116.html; FRB, "Federal Reserve Board fines Toronto-Dominion Bank $123.5 million for violations related to anti-money laundering laws," (October 10, 2024) https://www.federalreserve.gov/newsevents/pressreleases/enforcement20241010a.htm.

- **Silvergate Bank:** From approximately 2014 through March 2023, Silvergate focused on providing banking and financial services to foreign and domestic companies engaged in, among other things, buying and selling digital assets. In 2017, to facilitate U.S. dollar internal bank transfers among Silvergate customers engaged in buying and selling digital assets, Silvergate launched the Silvergate Exchange Network (SEN), an internal payments platform that permitted Silvergate customers participating in the SEN to make and receive, in near real time, internal bank transfers of U.S. dollars to and from other bank customers participating in the SEN. An investigation by the FRB identified deficiencies in Silvergate's monitoring of internal transactions through the SEN. Silvergate announced that it was self-liquidating in March 2023. Subsequently, in May 2023 the FRB and California's Department of Financial Protection and Innovation (DFPI) issued a cease-and-desist order to facilitate the voluntary self-liquidation Silvergate had announced. The FRB separately fined Silvergate $43 million for noncompliance with the AML laws. Silvergate completed its liquidation and wind-down plan in July 2024, has paid back all deposits to its customers, and no longer functions as a bank.[210]

In recent years, banks have increasingly partnered with third parties, including financial technology companies (fintechs), to deliver expanded products and services. Often referenced as banking-as-a-service (BaaS), a bank typically integrates its infrastructure and services into the platforms of fintechs or other businesses. While BaaS can provide benefits to banks (e.g., new fee income, access to data) and fintechs (e.g., rapid, capital-light market entry and access to banking infrastructure), there are several risks involved in these arrangements. For instance, layered third-party relationships can blur responsibility for AML/CFT supervision, and create attribution challenges when failures occur. In addition, the rapid product iteration and venture-driven growth of fintechs can drive volume beyond the capacity of compliance staffing and controls.

In June 2023, the FRB, Federal Deposit Insurance Corporation (FDIC), and OCC issued guidance for supervised banks regarding the risks of third-party relationships. The guidance noted that a bank's use of third parties does not diminish its responsibility to meet its regulatory requirements, and that the use of third parties can reduce a bank's direct control over activities and may introduce new risks or increase existing risks.[211] In July 2024, the FRB, FDIC, and OCC issued a joint statement on banks' arrangements with third parties to deliver bank deposit products and services, reemphasizing existing guidance.[212] In June 2025, the OCC again discussed in its Semiannual Risk Perspective that fintechs may not always have appropriate experience, technical expertise, and resources in place, which could undermine the ability to effectively manage these associated risks.[213]

Money Services Businesses (MSBs)

MSBs are non-bank financial institutions that include: (1) currency dealers or exchangers; (2) check cashers; (3) issuers of traveler's checks or money orders, or stored value; (4) sellers or redeemers of traveler's checks or money

210 FRB, "Federal Reserve Board fines Silvergate Capital Corporation and Silvergate Bank $43 million for deficiencies in Silvergate's monitoring of transactions in compliance with anti-money laundering law," (July 1, 2024) https://www.federalreserve.gov/newsevents/pressreleases/enforcement20240701a.htm; DFPI, "Silvergate to Pay $63 Million in Combined Penalties Following Coordinated Investigations by DFPI, Federal Partners," (July 1, 2024) https://dfpi.ca.gov/press_release/silvergate-to-pay-63-million-in-combined-penalties-following-coordinated-investigations-by-dfpi-federal-partners/.

211 "Interagency Guidance on Third-Party Relationships: Risk Management," (June 9, 2023), https://www.federalregister.gov/documents/2023/06/09/2023-12340/interagency-guidance-on-third-party-relationships-risk-management.

212 FRB, FDIC, and OCC, "Joint Statement on Banks' Arrangements with Third Parties to Deliver Bank Deposit Products and Services," (July 25, 2024) https://www.occ.treas.gov/news-issuances/news-releases/2024/nr-ia-2024-85a.pdf.

213 OCC, "Semiannual Risk Perspective – Spring 2025," (June 2025) https://www.occ.treas.gov/publications-and-resources/publications/semiannual-risk-perspective/files/pub-semiannual-risk-perspective-spring-2025.pdf. In November 2025, the OCC released a request for information (RFI) on community banks' engagement with their core service providers and other essential third-party service providers. The RFI solicits comments on the key challenges and barriers faced by community banks in engaging with their core service providers and other essential third-party service providers. The RFI focuses on ensuring that community banks can remain competitive in a rapidly evolving marketplace.

orders, or stored value; (5) money transmitters; and (6) the U.S. Postal Service.[214] As of December 15, 2025, there are 29,514 principal MSBs registered with FinCEN pursuant to the BSA regulations.[215] There are over 200,000 MSB agents, which may not be required to register with FinCEN, but are subject to state banking authorities' licensing and supervision requirements, including for AML/CFT requirements. In general, MSBs, including agents and their principals, are required to develop and implement an AML/CFT program, file CTRs and SARs, and maintain records of certain other transactions and currency exchanges.[216]

Like banks, MSBs face a range of money laundering risks influenced by their user base, services offered, and geographic footprint, among several other factors. MSBs employ a transaction-based business model with risks emanating from cross-border transfers, cash prevalence, and more flexible customer identification requirements compared to other types of financial institutions. Given the large number of principal and agent MSBs throughout the United States, illicit actors may also spread money laundering transactions across several providers, structure cash activities below certain BSA reporting thresholds, and register for services using fake or stolen identities, making it more difficult for law enforcement track illicit financial flows. During the assessment period, the United States found that MSBs were exploited by illicit actors in connection with several different predicate crimes, including domestic fraud,[217] transnational fraud and sextortion,[218] drug trafficking,[219] and weapons smuggling,[220] as well as terrorist and proliferation financing schemes.[221]

Illicit actors are also able to exploit complicit MSBs that willfully neglect AML/CFT obligations, most often by failing to file SARs and CTRs, structuring transactions, or allowing the use of fake identities.[222] Several recent cases have demonstrated how foreign-based TCOs use complicit MSBs to launder illicit drug trafficking proceeds to Mexico. In one case, the owner and operator of an MSB with locations in Oregon and Washington pleaded guilty to conspiring to launder drug trafficking proceeds. According to court documents, the woman's stores sent over $4.2 million dollars in wire transfers to places in Mexico. The woman and other co-conspirators also accepted $49,500 in cash represented as drug proceeds and laundered the funds through her stores. The woman charged a ten percent commission to help launder the money. She admitted that when she wired these funds, she used false sender information, structured wire transfers into smaller amounts, and used different stores she owned to help conceal

214 FinCEN, "Money Services Business Definition," (accessed December 15, 2025) https://www.fincen.gov/money-services-business-definition.

215 31 CFR 1022.380(a)-(f); FinCEN, "MSB Registrant Search," (updated December 15, 2025) https://www.fincen.gov/resources/msb-state-selector.

216 See generally 31 CFR Part 1022. Many digital asset service providers are MSBs. See FinCEN, "Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies," (March 18, 2013) https://www.fincen.gov/resources/statutes-regulations/guidance/application-fincens-regulations-persons-administering. See the Digital Assets section for a discussion of money laundering risks associated with digital service providers that are also MSBs.

217 *See, e.g.*, DOJ, "Leader of $1.4 million bank fraud and identity theft scheme pleads guilty to victimizing bank customers nationwide," (March 4, 2025) https://www.justice.gov/usao-wdwa/pr/leader-14-million-bank-fraud-and-identity-theft-scheme-pleads-guilty-victimizing-bank.

218 *See, e.g.*, DOJ, "Three New York Residents Sentenced For Fraud And Money Laundering Using Funds From Elderly Lottery Scam Victims," (November 18, 2024) https://www.justice.gov/usao-mdpa/pr/three-new-york-residents-sentenced-fraud-and-money-laundering-using-funds-elderly.

219 *See, e.g.*, DOJ, "Local man & woman plead guilty to drug, money laundering crimes," (April 2, 2025) https://www.justice.gov/usao-sdoh/pr/local-man-woman-plead-guilty-drug-money-laundering-crimes; DOJ, "California man sentenced for drug distribution, money laundering, and human smuggling scheme," (June 7, 2024) https://www.justice.gov/usao-wdwa/pr/california-man-sentenced-drug-distribution-money-laundering-and-human-smuggling-scheme.

220 *See, e.g.*, DOJ, "'King' of Violent Haitian Gang Pleads Guilty to Gun Smuggling and Money Laundering After Government's Case," (January 31, 2024) https://www.justice.gov/usao-dc/pr/king-violent-haitian-gang-pleads-guilty-gun-smuggling-and-money-laundering-after.

221 See 2026 National Terrorist Financing Risk Assessment (NTFRA) and National Proliferation Financing Risk Assessment (NPFRA).

222 *See, e.g.* DOJ, "Money Transmitting Business Pleads Guilty to Failing to Report Transactions; Agrees to Forfeit $700,000," (June 26, 2024) https://www.justice.gov/usao-sdca/pr/money-transmitting-business-pleads-guilty-failing-report-transactions-agrees-forfeit; DOJ, "New Jersey Owner of Check Casher and Money Service (sic) Business Admits Filing More Than $325 Million in False Currency Transaction Reports, Operating and Aiding and Abetting an Unlicensed Money Transmitting Business," (October 16, 2024) https://www.justice.gov/usao-nj/pr/new-jersey-owner-check-casher-and-money-serivce-business-admits-filing-more-325-million.

the drug proceeds.[223] Similar methods were used in two separate cases related to CJNG and LNFM filed in Atlanta, Georgia in April 2025.[224]

In December 2025, FinCEN announced a multi-tiered operation targeting more than 100 U.S. MSBs operating along the southwest border to examine the MSBs for potential non-compliance with regulations designed to detect money laundering and combat illicit finance. FinCEN's operation resulted in the issuance of six notices of investigation, dozens of examination referrals to the IRS Small Business/Self-Employed (SBSE) division, and over 50 compliance outreach letters. This data-driven operation is based on a review of, among other things, over one million CTRs and 87,000 SARs.

Another typology, first highlighted in the 2024 NMLRA, involves complicit MSBs cashing checks for shell construction companies to facilitate under-the-table payments to construction workers who are often not legally authorized to work in the United States with no taxes being withheld or reported to the IRS. In one case, according to court documents and trial testimony, construction companies would notify the president of a check cashing company when they planned to bring checks into one of his check cashing locations so that he could ensure he had enough cash on hand to complete the transaction. Hundreds of thousands of dollars of payroll checks were cashed daily, and the man was aware that at least one of his co-conspirators used a false name and Social Security number. Acting as a compliance officer, the man allowed hundreds of false regulatory reports to be filed knowing they contained the fake identity. Over the course of their conspiracy, the man and his co-conspirators prevented the IRS from collecting more than $44 million in payroll and income taxes due on the cash wages.[225]

Unregistered MSBs

Failing to register an MSB, at the federal or state level, is not simply an administrative omission. Entities that operate as unregistered MSBs pose an outsized risk within the MSB sector because they are unlikely to follow other BSA requirements, such as developing and implementing an AML/CFT program or filing CTRs and SARs. In February 2025, FinCEN assessed a $37 million civil money penalty against Brink's Global Services USA, Inc. (Brink's) for willful violations of the BSA. As a result of Brink's failures, hundreds of millions of dollars in bulk currency shipments were transmitted across the Southwest Border on behalf of high-risk entities—including a Mexican currency exchanger that later pleaded guilty to violating the BSA.[226] As part of a non-prosecution agreement with the DOJ, Brink's also admitted that it illegally transported money domestically and internationally between third parties and outside the limited regulatory protections for currency transporters. During this illegal conduct, Brink's failed to have compliance controls in place to ensure its business activities remained within the regulatory safe harbor provided to the armored car industry.[227]

Unregistered MSBs can also include individuals operating as part of IVTS, or underground banking, as well as individuals who misuse their personal or business bank accounts to independently offer money transmission

223 DOJ, "Owner of Money Service Business Unlawfully Residing in the United States Pleads Guilty to Conspiracy to Launder Drug Proceeds," (October 24, 2025) https://www.justice.gov/usao-or/pr/owner-money-service-business-unlawfully-residing-united-states-pleads-guilty-conspiracy.

224 DOJ, "Leaders of La Nueva Familia Michoacana and Atlanta-Based Money Launderer Indicted," (April 15, 2025) https://www.justice.gov/opa/pr/leaders-la-nueva-familia-michoacana-and-atlanta-based-money-launderer-indicted; DOJ, "Members of a Massive International Drug Trafficking and Money Laundering Ring Indicted in Atlanta," (April 15, 2025) https://www.justice.gov/usao-ndga/pr/members-massive-international-drug-trafficking-and-money-laundering-ring-indicted.

225 DOJ, "Oregon Check Casher Sentenced to Federal Prison for Payroll Tax Scheme Involving $177 Million," (February 4, 2025) https://www.justice.gov/usao-or/pr/oregon-check-casher-sentenced-federal-prison-payroll-tax-scheme-involving-177-million.

226 FinCEN, "FinCEN Announces $37,000,000 Civil Money Penalty Against Brink's Global Services USA, Inc. for Violations of the Bank Secrecy Act," (February 6, 2025) https://www.fincen.gov/news/news-releases/fincen-announces-37000000-civil-money-penalty-against-brinks-global-services-usa.

227 DOJ, "Brink's Forfeits $50 Million for Failing to Register as a Money Transmitting Business," (February 6, 2025) https://www.justice.gov/usao-sdca/pr/brinks-forfeits-50-million-failing-register-money-transmitting-business.

services.[228] In one case, an Iraqi citizen residing in the United States was sentenced to 54 months in prison following his conviction of unlicensed money remitting. At the hearing, the court heard how the man provided money services to criminal organizations in the tens of thousands of dollars. During the trial, the jury heard evidence about the man's money transmitting business, which he operated at his residence. Since 2020, he transferred and wired millions of dollars from U.S. bank accounts to ones all over the world, including in China, Indonesia, and India.[229]

Broker-Dealers and Investment Advisers

Broker-dealers and investment advisers are two different types of securities firms, which help clients grow and manage their assets by providing a wide variety of services ranging from one-off transactions to long-term wealth management. These entities have varying AML/CFT obligations and exposure to money laundering risks.

Broker-Dealers

Broker-dealers buy or sell securities either for their own account or on behalf of customers and generally handle lower volumes of cash-based transactions than banks. According to the Securities and Exchange Commission (SEC), as of 2024, there were approximately 3,300 broker-dealers with total assets of approximately $6.4 trillion.[230] Assets within the broker-dealer industry are highly concentrated. Most broker-dealers (67 percent) have less than $5 million in assets, and about two percent of total broker-dealers account for 94 percent of total assets. While the number of broker-dealers has decreased over the past 15 years, their assets have grown by $1.7 trillion—a sign of industry consolidation.[231]

Given the large sums of funds and other assets they could move through customer accounts, broker-dealers have exposure from customers seeking to disguise illicit proceeds within otherwise legitimate trades or engage in fraudulent trading activity (e.g., pump-and-dump schemes involving low-priced securities). Customers based in high-risk jurisdictions impose other AML/CFT-related risks on broker-dealers, such as those associated with their source of wealth or the counterparties with which they may transact. Broker-dealers have comprehensive and longstanding BSA obligations. They are subject to oversight by multiple federal and state regulators, including the SEC, in addition to self-regulatory organizations (SROs), such as the Financial Industry Regulatory Authority (FINRA).

The SEC's examination priorities for FY2026 note that the Division of Examinations will continue to focus on AML programs and review whether broker-dealers and certain registered investment companies (RICs), including mutual funds[232], are: 1) appropriately tailoring and updating their AML program to their business model and associated money laundering risks, including accounting for risks associated with omnibus accounts maintained for foreign financial institutions; 2) adequately conducting independent testing; 3) establishing an adequate customer identification program, including for beneficial owners of legal entity customers; and 4) meeting their SAR filing obligations. Examinations of certain RICs will also review policies and procedures for oversight of applicable financial intermediaries. Lastly, examinations will review whether broker-dealers, advisers, and RICs are monitoring

228 *See, e.g.*, DOJ, "Two Men Responsible For Running Hawala Scheme Involving More Than $65 Million Sentenced To Three Years In Prison," (April 23, 2025) https://www.justice.gov/usao-sdny/pr/two-men-responsible-running-hawala-scheme-involving-more-65-million-sentenced-three; DOJ, "Four Honduran Nationals Indicted in Florida for Years-Long Off-the-Books Payroll Scheme," (May 6, 2025) https://www.justice.gov/opa/pr/four-honduran-nationals-indicted-florida-years-long-books-payroll-scheme; DOJ, "Brooklyn Business Owner Sentenced to 15 Years in Prison for $55 Million Illegal Check Cashing, Bank Fraud, and Tax Evasion Scheme," (November 19, 2025) https://www.justice.gov/usao-edny/pr/brooklyn-business-owner-sentenced-15-years-prison-55-million-illegal-check-cashing.

229 DOJ, "Multimillion-dollar unlicensed money transmitter sent to prison," (October 16, 2025) https://www.justice.gov/usao-sdtx/pr/multimillion-dollar-unlicensed-money-transmitter-sent-prison.

230 SEC, "SEC Publishes Data on Broker-Dealers, Mergers & Acquisitions, and Business Development Companies," (June 26,2025) https://www.sec.gov/newsroom/press-releases/2025-96-sec-publishes-data-broker-dealers-mergers-acquisitions-business-development-companies.

231 Diana Knyazeva and Daniel Bresler, "Broker-Dealer Activity in the United States," (June 2025), p. 4, https://www.sec.gov/files/dera-broker-dealer-activity-2506.pdf.

232 Under FinCEN regulations, "mutual funds" (as defined at 31 CFR 1010.100(gg)) are "financial institutions" and, accordingly, subject to several BSA/AML obligations, including establishing an AML compliance program, establishing a customer identification program, and monitoring, detecting, and filing reports of suspicious activity.

OFAC's sanctions and ensuring compliance with such sanctions.[233]

During the assessment period the SEC took 12 enforcement actions against broker-dealers in connection with failures related to AML/CFT obligations, while FINRA took 34 enforcement actions. For example, in December 2024, the SEC settled charges against SogoTrade, Inc., a registered broker-dealer, for failing to file SARs, and against SogoTrade's former AML Compliance Officer, for willfully aiding and abetting and causing SogoTrade's violations. The SEC found that on numerous occasions, the AML Compliance Officer failed to investigate suspicious activity and failed to file SARs concerning suspicious activity that SogoTrade systems or personnel, or employees of SogoTrade's clearing firm, brought to his attention. According to the SEC's order, he also had a practice of alerting customers that SogoTrade's surveillance reports had identified their suspicious trading activity and would advise or direct employees to advise customers to keep their trading activities below the average daily volume threshold to avoid triggering firm review.[234]

Additionally, in July 2025, Interactive Brokers LLC, a Greenwich, Connecticut-based global electronic broker-dealer providing brokerage and investment services to millions of customers worldwide through its online brokerage platform agreed to pay OFAC nearly $12 million to settle its potential civil liability for apparent violations of multiple OFAC sanctions programs.[235]

Investment Advisers

Investment advisers (IAs) provide a range of financial services relating to asset management. IA clients include local, state, and foreign governments, institutional investors, retail investors, and high-net-worth individuals. Certain larger IAs register with the SEC (Registered Investment Advisers, or RIAs). Certain IAs for private funds and venture capital funds are exempt from SEC registration but still file periodic reports with the SEC (Exempt Reporting Advisers, or ERAs). Other investment advisers are exempt or are prohibited from SEC registration but still may be required to register with one or more states (state-registered IAs).[236]

As reported on April 27, 2025, over 15,900 RIAs were reporting $148.5 trillion in assets under management (AUM), with over $26 trillion in aggregate gross assets of RIA-advised private funds.[237] There are also nearly 5,800 ERAs, which can only provide investment advice to private funds, such as hedge funds, venture capital funds, and private equity funds. According to the SEC, as reported on April 27, 2025, ERAs reported roughly $8.4 trillion in aggregate gross assets of ERA-advised private funds.[238] Lastly, according to the North American Securities Administrators Association (NASAA), as reported in September 2025, there are approximately 16,500 state-registered IAs managing over $380 billion in assets.[239]

In February 2024, Treasury published an IA sectoral risk assessment that identified several illicit finance threats involving IAs, including that IAs have served as an entry point into the U.S. market for illicit proceeds associated with foreign corruption, fraud, tax evasion, and sanctions evasion. The assessment found that ERAs faced the highest illicit finance risks in the IA sector, followed by RIAs who advise private funds. The assessment also highlighted that IAs and their advised funds,

233 SEC, "Fiscal Year 2026 Examination Priorities," (November 18, 2025) https://www.sec.gov/files/2026-exam-priorities.pdf.

234 SEC, "SEC Charges SogoTrade Inc. and Former Anti-Money Laundering Compliance Officer for Failure to File Suspicious Activity Reports (SARs)," (December 17, 2024) https://www.sec.gov/enforcement-litigation/administrative-proceedings/34-101936-s.

235 OFAC, "Interactive Brokers LLC Settles with OFAC for $11,832,136 Related to Apparent Violations of Multiple Sanctions Regulations," (July 15, 2025) https://ofac.treasury.gov/media/934501/download?inline.

236 Generally, the SEC regulates RIAs that manage $100 million or more in client assets. There are certain exemptions to this rule that allow for SEC registration even if the assets threshold hasn't been met. In instances where SEC registration requirements aren't met, IAs with less than $100 million in assets under management (AUM) are generally regulated by the state regulator for the state where the adviser has its principal place of business. FINRA, "Investment Advisers," https://www.finra.org/investors/investing/working-with-investment-professional/investment-advisers.

237 SEC, "Investment Adviser Statistics: Form ADV Data, period ending December 2024," (April 27, 2025), p. 3, 5, https://www.sec.gov/files/investment/im-investment-adviser-statistics-20250430.pdf. This total includes discretionary and non-discretionary regulatory assets under management (RAUM) as detailed in Form ADV instruction 5.b. See "FORM ADV (Paper Version)," (accessed December 30, 2025), pp. 19-22, https://www.sec.gov/about/forms/formadv-instructions.pdf.

238 Ibid, p. 14. See SEC, "Exempt Reporting Adviser (ERA)," (accessed December 30, 2025) https://www.investor.gov/introduction-investing/investing-basics/glossary/exempt-reporting-adviser-era.

239 NASAA, "NASAA Investment Adviser Section 2025 Annual Report" (September 8, 2025), p. 3, https://www.nasaa.org/wp-content/uploads/2025/09/IA-Section-2025-Report-FINAL.pdf.

particularly venture capital funds, may be used by foreign states to access certain technology and services with long-term national security implications through investments in early-stage companies.[240]

To address these risks, Treasury finalized a rule imposing AML/CFT obligations (e.g., AML/CFT program, reporting, and recordkeeping requirements) on certain IAs (i.e., RIAs and ERAs) (IA AML Rule). On December 31, 2025, FinCEN adopted a final rule delaying the effective of date of the IA AML Rule until January 1, 2028.[241] Many IAs' activities are still subject to an enterprise-wide AML/CFT program or otherwise indirectly subject to such controls due to their affiliations or interactions with other covered financial institutions (e.g., banks and broker-dealers).

During the assessment period, the SEC took two AML-related enforcement actions against RIAs.[242] In January 2015, the SEC charged Navy Capital Green Management, LLC (Navy Capital) with making misrepresentations related to its AML procedures and for compliance failures. The SEC's order found that, from at least October 2018 until January 2022, Navy Capital stated in offering and other documents provided to prospective and existing private fund investors that the firm was voluntarily complying with customer due diligence laws despite those laws not applying to IAs, including by conducting specific types of customer due diligence on prospective investors and conducting ongoing customer due diligence monitoring on existing investors. According to the order, Navy Capital's private fund investors included multiple foreign-based entities with opaque beneficial ownership and sources of wealth. The order found that Navy Capital did not, in fact, always conduct the customer due diligence as described, including with respect to an entity owned by an individual publicly reported to have suspected connections to money laundering activities.[243]

OFAC has also taken two enforcement actions against investment advisers during the assessment period:

- In December 2025, IPI Partners, LLC (IPI), a Chicago-based private equity firm that specializes in buying, developing, and operating data centers, has agreed to pay over $11 million to OFAC to settle its potential civil liability for apparent violations of Ukraine-/Russia-related sanctions. In 2017 and 2018, IPI solicited and received investments from Russian oligarch Suleiman Kerimov through a series of legal structures and continued to maintain those investments for four years after OFAC designated Kerimov on April 6, 2018.[244]

- In June 2025, OFAC issued a Penalty Notice imposing a $215 million penalty on GVA Capital Ltd., a venture capital firm based in San Francisco, California, for violating OFAC's Ukraine-/Russia-related sanctions and for failing to comply with an OFAC subpoena. Between April 2018 and May 2021, GVA Capital knowingly managed an investment for sanctioned Russian oligarch Suleiman Kerimov while aware of his blocked status. In 2016, GVA Capital officials met with Kerimov at his estate in France to secure his personal approval for the investments. In April 2018, OFAC sanctioned Kerimov. GVA Capital nonetheless continued managing these investments by working through Kerimov's nephew, who GVA Capital knew served as Kerimov's proxy.[245]

240 Treasury, "Investment Adviser Risk Assessment," (February 2024), https://home.treasury.gov/system/files/136/US-Sectoral-Illicit-Finance-Risk-Assessment-Investment-Advisers.pdf.

241 FinCEN, "Final Rule: Delaying the Effective Date of the Anti-Money Laundering/Countering the Financing of Terrorism Program and Suspicious Activity Report Filing Requirements for Registered Investment Advisers and Exempt Reporting Advisers," (December 31, 2025), 91 FR 36, https://www.federalregister.gov/documents/2026/01/02/2025-24184/delaying-the-effective-date-of-the-anti-money-launderingcountering-the-financing-of-terrorism.

242 One of these enforcement actions was taken against a dual-registered broker-dealer and investment adviser.

243 SEC, "SEC Charges Advisory Firm Navy Capital With Misrepresenting Its Anti-Money Laundering Procedures to Investors," (January 14, 2025) https://www.sec.gov/newsroom/press-releases/2025-8.

244 OFAC, "IPI Partners, LLC Settles with OFAC for $11,485,352 Related to Apparent Violations of Ukraine-/Russia-Related Sanctions," (December 2, 2025) https://ofac.treasury.gov/media/934786/download?inline.

245 OFAC, "OFAC Imposes $215,988,868 Penalty on GVA Capital Ltd. for Violating Ukraine/Russia-Related Sanctions and Reporting Obligations," (June 12, 2025) https://ofac.treasury.gov/media/934366/download?inline

Casinos and Gaming

There are varying levels of risks associated with casinos and other gaming activities in the United States. These risks span traditional casinos and card clubs, non-casino gambling and gaming activities (such as sports betting, fantasy sports, and sweepstakes competitions), and the illegal gambling market. Across these interrelated markets, gaming in the United States remains particularly vulnerable to the laundering of the proceeds of drug trafficking, organized crime, foreign criminal activities, and illegal gambling and bookmaking, among other predicate offenses. These activities are exacerbated by uneven licensing and regulatory frameworks across different gaming markets and deficient compliance practices. However, as described further below, in general, casinos and other gaming entities may be subject to AML/CFT programmatic, reporting, and recordkeeping requirements. Overall, the money laundering risks associated with these sectors continue to grow and evolve, mirroring the broader trajectory of nationwide legal and illegal gaming activities.

Casinos and Card Clubs

Casinos and card clubs remain attractive venues for laundering funds, with illicit actors continuing to rely on methods such as chip-walking, minimal play, structuring, the use of money mules, and patrons' collusion on bets to launder funds. Casinos' AML/CFT measures and reporting practices, as required by the BSA for decades, have had a demonstrable effect on disrupting illicit activity.[246] Conversely, casinos' failure to comply with their applicable BSA obligations creates opportunities for money launderers to process illicit proceeds undetected.[247] For example, in 2024, FinCEN assessed a $900,000 civil monetary penalty against a California card club for its willfully deficient AML/CFT controls, including inadequate internal controls, failure to conduct independent testing, failures to train personnel, and failure to detect and report suspicious activity and certain currency transactions, among other weaknesses.[248]

Another problematic compliance deficiency involves the failure of casino management to either apply CDD practices or report suspicious activity in connection with patrons that the casino knows or suspects to be engaged in criminal activity. Multiple casinos have been identified as having failed to conduct due diligence or file SARs on illegal bookmakers who patronize the casino. For example, in August 2024, the Nevada Gaming Control Board (NGCB) filed a complaint against the Resorts World Las Vegas casino, alleging that the casino "welcomed certain individuals to wager at its casino…while [casino] executives and employees knew, or should have known, that certain individuals were likely illegal bookmakers, that they had criminal convictions related to illegal gambling operations, or that they had ties to organized crime."[249] The NGCB further alleged that the casino's executives facilitated "a culture where information of suspicious or illegal activity is, at a minimum, negligently disregarded, or at worst, willfully ignored for financial gain."[250] In line with the conclusions of the 2024 NMLRA, this trend may be indicative of casino's under-resourcing or sidelining BSA compliance functions in favor of attracting more profitable—even if higher risk—patrons.[251]

246 *See, e.g.*, DOJ, "Leader and Money Launderer for the KDY Drug Tracking Crew Sentenced to 160 Months in Federal Prison," (April 17, 2025) https://www.justice.gov/usao-dc/pr/leader-and-money-launderer-kdy-drug-trafficking-crew-sentenced-160-months-federal-prison; DOJ, "Pensacola Man Pleads Guilty to Multi-Million Dollar Drug Trafficking and Money Laundering Crimes, (June 27, 2025) https://www.justice.gov/usao-ndfl/pr/pensacola-man-pleads-guilty-multi-million-dollar-drug-trafficking-and-money-laundering.

247 Casinos and card clubs are generally included in the definition of a financial institution under the BSA, provided they are state-licensed and have gross annual gaming revenue (GAGR) over $1 million. Briefly, casinos and card clubs must establish AML/CFT programs, including written AML procedures and internal controls, a designated compliance officer, independent testing functions, and abide by certain reporting obligations, including SAR filing obligations (see 31 CFR Part 1021, Subparts B, C, and D). While these obligations have changed over time, casinos were first subjected to BSA obligations in 1985. The IRS examines casinos and card clubs for compliance with these BSA requirements, as delegated by FinCEN.

248 FinCEN, "FinCEN Assesses $900,000 Civil Money Penalty Against Lake Elsinore Hotel and Casino for Violations of the Bank Secrecy Act," (October 23, 2024) https://www.fincen.gov/news/news-releases/fincen-assesses-900000-civil-money-penalty-against-lake-elsinore-hotel-and.

249 "Nevada Gaming Control Board vs. Resorts World Las Vegas, LLC," (August 15, 2024) https://www.gaming.nv.gov/siteassets/content/gaming/complaints/NGC_24-04_Genting_Berhad.pdf

250 Id.

251 *See, e.g.*, NGCB, "Nevada Gaming Control Board and MGM Resorts International Enter Into Proposed Stipulation for Settlement Regarding Disciplinary Complaint," (April 18, 2025) https://www.gaming.nv.gov/siteassets/content/about/press-release/NGCB_News_Release_-_MGMRI__18April2025.pdf.

Relatedly, there are significant risks associated with casinos' practices aimed at facilitating gambling by wealthy foreign patrons by engaging in illegal and unlicensed money transmission practices to do so. In September 2024, as part of a Non-Prosecution Agreement, Wynn Las Vegas (WLV) admitted that it illegally used unregistered money transmitting businesses to circumvent the conventional financial system. For example, WLV regularly contracted with third-party independent agents acting as unlicensed money transmitting businesses to recruit foreign gamblers to WLV. For the gamblers to repay debts to WLV or have funds available to gamble at WLV, the independent agents transferred the gamblers' funds through companies, bank accounts, and other third-party nominees in Latin America and elsewhere, and ultimately into a WLV-controlled bank account in California. Funds deposited into the WLV-controlled account were transferred into the WLV cage account. WLV employees, with the knowledge of their supervisors, and working with the independent agents, eventually credited the WLV account of each individual patron. The convoluted transactions enabled foreign gamblers at WLV to evade foreign and U.S. laws governing monetary transfer and reporting.[252]

These illegal money transmission practices are also closely linked to CMLNs, which have engaged in illicit finance activity at or through casinos. CMLN activities were present in the money transfer schemes identified in the previously described case against the WLV casino. Additionally, cash transfers and hand-offs by CMLNs have allegedly occurred on casino premises, as documented in the indictment of a June 2024 case against an alleged CMLN aiding the laundering of Sinaloa Cartel drug trafficking proceeds.[253]

Non-Casino Gaming and Gambling

The legal non-casino gaming market—including sports betting, fantasy sports, and sweepstakes casinos—is vulnerable to many of the same money laundering methods as traditional casinos, as well as other typologies also associated with internet fraud and cybercrime. Non-casino gaming is subject to varying licensing and regulatory frameworks. These activities often do not occur in connection with a BSA-covered casino, though FinCEN guidance has stated that certain gaming businesses may nonetheless be regulated under the BSA as money transmitters.[254]

For licensed sports betting, there are increasing indications of this sector's misuse for illicit finance purposes. Money launderers' misuse of licensed online sports betting platforms using stolen PII remains a major risk. In April 2025, a man was sentenced to 46 months in prison for crimes related to laundering hundreds of thousands of dollars from a Columbus strength training equipment manufacturer. The man used the online gambling site FanDuel to conspire to launder money. He and others would steal a victim's identity and use it to create a FanDuel account. Then criminal proceeds were deposited into the account and later withdrawn. In total, the man and others used this scheme to deposit nearly $572,000 and withdraw more than $485,000 of the criminal proceeds.[255]

There are also growing risks associated with fantasy sports and sweepstakes casino activities, which generally fall beyond the scope of casino and gambling regulation in the United States. This lack of regulatory oversight increases illicit finance risk. Fantasy sports services are often offered by a wide array of businesses, including many of the same platforms that also offer licensed sports betting services. However, fantasy sports are considered "games of skill" and are often not subject to gambling-related licensing or regulatory requirements. Nonetheless, fantasy sports (including daily fantasy sports, or "DFS") have been misused for fraudulent purposes. For example, in March 2024 a Florida man was sentenced to over six years in prison for committing wire fraud and engaging in an illegal monetary transaction. According to court documents, the man operated a fraud scheme through which he embezzled approximately $22,221,454 from the Jacksonville Jaguars. He used the proceeds of this scheme, in

252 DOJ, "Wynn Las Vegas Forfeits $130 Million for Illegally Conspiring with Unlicensed Money Transmitting Businesses," (September 6, 2024) https://www.justice.gov/usao-sdca/pr/wynn-las-vegas-forfeits-130-million-illegally-conspiring-unlicensed-money-transmitting.

253 First Superseding Indictment, United States v. Edgar Joel Martinez-Reyes, et al, No. 2:23-cr-545(A)-DMG (C.D. Cal. June 4, 2024), p. 17, https://www.justice.gov/archives/opa/media/1356301/dl?inline.

254 FinCEN, "Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies," (May 9, 2019) https://www.fincen.gov/system/files/2019-05/FinCEN%20Guidance%20CVC%20FINAL%20508.pdf.

255 DOJ, "New York man sentenced to prison for money laundering crimes related to nearly half million dollars stolen from local business through computer malware," (April 11, 2025) https://www.justice.gov/usao-sdoh/pr/new-york-man-sentenced-prison-money-laundering-crimes-related-nearly-half-million.

whole or part, to place bets with online gambling websites.[256] This case illustrates the risk of large sums of criminal proceeds entering the fantasy sports ecosystem, even if these activities may fall beyond the scope of licensed gambling activities.

There are also risks associated with sweepstakes casinos. The American Gaming Association describes sweepstakes casinos as services that offer traditional casino games to customers for free (typically online), but that use a dual-currency system in which players can earn game-specific credits or "coins" that they can later cash out for fiat currency or digital assets.[257] This dual-currency system allows sweepstakes to not be subject to many casino or online gambling regulations. Even if sweepstakes casinos generally fall beyond the casino regulatory framework, they are still vulnerable to many of the same money laundering methodologies as are casinos, and they may be especially attractive venues for criminals to launder funds given their lack of oversight.

Illegal Gambling

Across gaming activities in the United States, risks remain the highest in the illegal gambling market, which spans unlicensed casinos and poker rooms, illegal online gambling platforms (including those based in the U.S. or domiciled offshore), and other forms.[258] Illegal gambling operations not only generate significant illicit proceeds for their owners (funds that may subsequently be laundered), but they also afford opportunities for large-scale money laundering by the customers of these operations. Illegal gambling operators generally do not implement AML/CFT, or identity verification measures. On the contrary, it is often the lack of AML/CFT controls that may attract criminals or other high-risk gamblers to the illegal gambling market.

There are numerous recent examples of illegal gambling operations engaging in money laundering or related activities. In October 2025, an indictment was unsealed charging six defendants with wire fraud conspiracy and money laundering conspiracy for their alleged roles in a scheme to use inside information from National Basketball Association (NBA) players and coaches to profit from illegal betting activity. As set forth in the indictment, between December 2022 and March 2024, the defendants and their associates obtained and misused non-public information about upcoming NBA games to place fraudulent sports wagers for profit and then laundered the proceeds.[259]

Online illegal gambling and sports betting platforms are another major risk area. Illegal gambling platforms generate illicit proceeds for their owners and operators, as well as provide opportunities to criminals to launder funds with enhanced anonymity through misuse of their gambling and betting services. These platforms are often based in offshore jurisdictions that have more permissive regulatory or supervisory regimes for gambling activities, and U.S. persons frequently wager via these platforms using virtual private networks (VPNs) or other technologies that mask their U.S.-based location. In one case, ten individuals pleaded guilty to managing a multi-million-dollar sports betting operation. According to the plea agreements, one of the defendants began operating a bookmaking organization at least 17 years ago. The organization eventually became known as "Red44," and bookmaking and betting activities occurred online via an offshore server located in Costa Rica. It is estimated that the organization accepted over $2 billion in wagers during its existence.[260]

256 DOJ, "Former Jacksonville Jaguars Employee Sentenced To More Than Six Years For Embezzling In Excess Of $22 Million," (March 12, 2024) https://www.justice.gov/usao-mdfl/pr/former-jacksonville-jaguars-employee-sentenced-more-six-years-embezzling-excess-22.

257 American Gaming Association, "Regulatory Vigilance Critical to Ensure 'Sweepstakes' Don't Threaten Consumers and Undermine Gaming Regulation," (August 2024) https://gamblingcompliance.vixio.com/sites/default/files/inline-files/AGA%20Sweepstakes%20Memo%20(1).pdf.

258 See IC3, "Great Odds, High Risk: The FBI Encourages U.S. Bettors to Know the Risks of Illegal Gambling," (December 17, 2025) https://www.ic3.gov/PSA/2025/PSA251217.

259 DOJ, "Current and Former National Basketball Association Players and Four Other Individuals Charged in Widespread Sports Betting and Money Laundering Conspiracy," (October 23, 2025) https://www.justice.gov/usao-edny/pr/current-and-former-national-basketball-association-players-and-four-other-individuals.

260 DOJ, "Ten Defendants Plead Guilty in Multi-Million-Dollar Sports-Betting and Money Laundering Scheme," (February 12, 2025) https://www.justice.gov/usao-ndal/pr/ten-defendants-plead-guilty-multi-million-dollar-sports-betting-and-money-laundering.

Complicit Insiders

Complicit insiders are employees of financial institutions that perpetrate financial crime independently or in support of other illicit actors. As was first identified in the 2015 NMLRA, every organization faces insider threats, but the stakes are higher for financial institutions given the volume and value of transactions in the U.S. financial system. Complicit insiders at financial institutions present varying levels of risk depending on their level of access and authority, as well as the strength of the institution's internal controls. Cases from the assessment period show that complicit insiders remain a consistent vulnerability for fraud and money laundering by opening and maintaining fraudulent accounts, sometimes in exchange for bribes;[261] knowingly processing fraudulent transactions;[262] and helping illicit actors evade a financial institution's internal audit systems that may flag or disrupt suspicious activity.[263] Complicit insiders at financial institutions can also embezzle funds themselves with no outside involvement.[264] These risks exist for full-time and part-time employees, as well as contractors.[265]

Complicit insiders can occupy positions of any level at a financial institution.[266] When senior executives are compromised and fail to fulfill an institution's AML/CFT requirements, it can lead to institutional failure. In December 2025, a federal grand jury returned an indictment charging the former president and chief executive officer (CEO) of the First National Bank of Lindsay for his role in a conspiracy to commit bank fraud and other crimes. As alleged, the CEO caused the bank to issue loans to certain customers, many of whom were his personal friends and neighbors, that the borrowers never repaid. It is alleged that the CEO then manipulated the bank's records and falsified various bank reports to falsely overstate the performance of the loans, including by using new loans or transfers of the bank's own funds to cover overdrafts of outstanding loans. The indictment alleges that the CEO frequently modified bank records to conceal this activity from the OCC, which was the bank's federal regulator, as well as from the bank's Board of Directors and others. During the summer of 2024, when the OCC was conducting an onsite examination at the bank, the CEO allegedly provided OCC staff with a false document that concealed hundreds of changes that the man had made to loan data. The indictment also alleges that the CEO failed to implement an AML program at the bank as required by the BSA. For example, the CEO allegedly failed to file any SARs on his own fraudulent scheme, and he advised bank customers to make cash deposits below $10,000 to avoid relevant reporting requirements.[267]

261 *See, e.g.*, DOJ, "TD Bank Insider Pleads Guilty to Accepting Bribes to Fraudulently Open More Than 100 Bank Accounts," (June 25, 2025) https://www.justice.gov/usao-nj/pr/td-bank-insider-pleads-guilty-accepting-bribes-fraudulently-open-more-100-bank-accounts.

262 *See, e.g.*, DOJ, "Two East Bay Residents, One Of Whom Was A Bank Teller, Indicted On Charges Of Cashing Stolen U.S. Treasury Checks," (February 13, 2025) https://www.justice.gov/usao-ndca/pr/two-east-bay-residents-one-whom-was-bank-teller-indicted-charges-cashing-stolen-us.

263 *See, e.g.*, DOJ, "Former Bank Employee Pleads Guilty to Role in International Money Laundering Conspiracy," (February 27, 2025) https://www.justice.gov/usao-ma/pr/former-bank-employee-pleads-guilty-role-international-money-laundering-conspiracy.

264 *See, e.g.*, DOJ, "Former Banker Sentenced For Embezzlement," (November 14, 2025) https://www.justice.gov/usao-mdfl/pr/former-banker-sentenced-embezzlement.

265 *See, e.g.*, DOJ, "Bank contractor sentenced for participation in $8 million debit card scheme," (July 22, 2025) https://www.justice.gov/usao-sdtx/pr/bank-contractor-sentenced-participation-8-million-debit-card-scheme.

266 *See, e.g.*, DOJ, "Paxful Inc. Co-Founder Pleads Guilty to Conspiracy to Fail to Maintain Effective Anti-Money Laundering Program," (July 8, 2024) https://www.justice.gov/archives/opa/pr/paxful-inc-co-founder-pleads-guilty-conspiracy-fail-maintain-effective-anti-money-laundering.

267 DOJ, "Former President of Failed Oklahoma Bank Indicted for Bank Fraud," (December 4, 2025) https://www.justice.gov/usao-wdok/pr/former-president-failed-oklahoma-bank-indicted-bank-fraud. According to Treasury's Office of Inspector General, the "primary cause of the Bank's failure was a critical breakdown in the Bank's internal controls which allowed fraudulent activity to occur that affected a substantial portion of the Bank's loan portfolio and liquid assets. Deficiencies in the Bank's Board oversight and internal controls and other unsafe or unsound practices allowed one or more Bank employees to alter Bank records and hide weaknesses in the Bank's loan portfolio from examiners. As a result of the identification of discrepancies in its books and records, the Bank had to recognize losses that exceeded the Bank's capital, rendering the Bank insolvent." Treasury, "Safety and Soundness: Failed Bank Limited Review – First National Bank of Lindsay," (March 27, 2025) https://oig.treasury.gov/system/files/2025-03/Failed-Bank-Limited-Review-Memorandum---First-National-Bank-of-Lindsay-508-Locked.pdf.

IX. Cash

After declining at the start of the COVID-19 pandemic, the number of cash payments the average American makes each month has remained stable, even as credit and debit card payments have increased.[268] Cash also remains frequently used in transactions involving illicit goods and services because the payments are immediate, lower cost, widely accepted, and relatively anonymous, allowing all parties involved to potentially avoid immediate scrutiny from financial institutions and law enforcement. As a result, criminal organizations often have large amounts of cash they need to launder for use in the United States or smuggle to foreign jurisdictions.

Generally, the first step to laundering bulk cash is to consolidate the cash at a single point within a city or region depending on the size and nature of the criminal operation. Transporting bulk cash is a time-intensive activity that typically requires a network of couriers to drive or fly around the United States and pick up illicit cash proceeds.[269] Criminal organizations then contract with professional money launderers or take steps themselves to either smuggle the bulk cash out of the country, introduce the cash into the financial system, or launder the cash through cash-intensive businesses to acquire goods or comingle the illicit cash with legitimate income. As detailed in other sections, criminals may also use the cash to purchase goods or real estate or exchange the cash for digital assets through black market exchangers.

Bulk Cash Smuggling

It is legal to transport any amount of currency or other monetary instrument into or out of the United States, but if the amount is greater than $10,000, the carrier, sender, or receiver must file a Currency or Monetary Instruments Report (CMIR, also known as FinCEN Form 105).[270] Bulk cash smuggling occurs when an individual knowingly conceals more than $10,000 in currency or other monetary instruments for transport into or outside the United States with the intent to evade a currency reporting requirement, such as a CMIR. This requirement applies regardless of how the currency is transported and the activity does not necessarily have to occur at a border or port of entry if it is proven that the person intended to cross the border.[271]

According to law enforcement, bulk cash smuggling remains a popular method for TCOs to move illicit cash proceeds out of the country. The cash may be concealed in private or commercial vehicles, in private or commercial aircraft, or on an individual. The couriers responsible for the smuggling are often directed by professional money launderers or senior members of a TCO. In one case, a Mexican national illegally residing in Arizona pleaded guilty to money laundering conspiracy in connection with providing over $100,000 in proceeds from drug sales to couriers who smuggled the money into Mexico to promote a drug trafficking operation.[272] In another case, four flight attendants pleaded guilty to operating an unlicensed money transmission business for accepting bulk cash from a money laundering organization, getting past security via the Known Crewmember lane, and passing the cash off to

268 Federal Reserve Financial Services, "2025 Findings from the Diary of Consumer Payment Choice," (May 2025), p. 4, https://www.frbservices.org/binaries/content/assets/crsocms/news/research/2025-diary-of-consumer-payment-choice.pdf.

269 *See, e.g.*, DOJ, "Two Members of a Transnational Money Laundering Organization Sentenced for Laundering Millions of Dollars in Drug Proceeds," (April 11, 2025) https://www.justice.gov/opa/pr/two-members-transnational-money-laundering-organization-sentenced-laundering-millions.

270 For a full explanation of what constitutes currency and monetary instruments, see CBP, "Currency / Monetary Instruments – Definition of Negotiable Monetary Instruments for currency reporting requirements," (May 1, 2025) https://www.help.cbp.gov/s/article/Article-1413?language=en_US; FinCEN, "Report of International Transportation of Currency or Monetary Instruments," https://fincen105.cbp.dhs.gov/#/.

271 U.S. Immigration and Customs Enforcement (ICE), "Combating Bulk Cash Smuggling," (updated May 29, 2025) https://www.ice.gov/about-ice/hsi/centers-labs/bcsc/faq.

272 DOJ, "Mexican Man Pleads Guilty to Violating Federal Kingpin Statute and Money Laundering in Connection with Arizona-Based Transnational Drug Trafficking Organization," (July 8, 2025) https://www.justice.gov/usao-wdpa/pr/mexican-man-pleads-guilty-violating-federal-kingpin-statute-and-money-laundering.

co-conspirators in the Dominican Republic. According to the complaint, the defendants smuggled approximately $8 million in bulk cash.[273]

Bulk cash can also be brought back into the United States as part of the laundering process or to further criminal schemes. In March 2025, FinCEN published an alert describing how TCOs can smuggle illicit cash proceeds into Mexico and then bring the cash back into the United States through armored car services, declaring the cash as the legitimate revenue of Mexico-based businesses. This cash can then be introduced into the U.S. financial system and may be wired back to Mexico.[274] As noted earlier, in February 2025, FinCEN assessed a $37 million civil money penalty against Brink's for money laundering violations related to bulk cash transportation.[275]

TCOs can also smuggle cash into the United States to purchase weapons for export to Mexico to further their campaigns of terror. In one case, a Mexican national pleaded guilty to his role in a money laundering conspiracy that involved smuggling currency and monetary instruments from Mexico into the United States to place large scale ammunition orders through various internet retailers. The ammunition was subsequently shipped to various locations in the Rio Grande Valley for their intended unlawful export to Mexico.[276]

Funnel Accounts

Criminals will also introduce illicit cash proceeds into the U.S. financial system directly despite the risk of financial institutions filing BSA reports that would draw law enforcement scrutiny. One common method is the use of funnel accounts, which are bank accounts, often held in the name of nominees, used to "funnel" cash deposits from multiple people, often from different locations. According to law enforcement, professional money launderers operating on a national scale tend to open funnel accounts at large banks with national footprints so their couriers can deposit bulk cash from anywhere in the country and minimize the amount of time they must spend transporting bulk cash on highways.

In some cases, criminals may structure cash deposits into the funnel accounts in amounts below $10,000 to prevent the bank from filing CTRs. However, if the criminal organization operates several accounts under nominee owners at different banks and makes deposits using fake IDs, they may choose to deposit cash without regard to reporting thresholds believing these obfuscation steps can impede law enforcement investigations. Funds are moved through several different financial institutions, cross-border wire transfers, or shell companies, making it more difficult to trace.

Small, disparate deposits at different locations can initially appear legitimate at a local level. Only at an aggregated level does the pattern of funneling reveal itself, generally after money has been moved from the account. In December 2024, a former Florida-based employee of TD Bank was arrested and charged by criminal complaint for facilitating money laundering to Colombia. As alleged in the complaint, after another TD Bank employee opened accounts in the names of shell companies with nominee owners, the man assisted the money laundering network by issuing dozens of debit cards for the accounts in exchange for bribes. Those accounts were then allegedly used to launder millions of dollars in narcotics proceeds through cash withdrawals at ATMs in Colombia.[277]

273 DOJ, "Flight Attendants Charged in Connection With Smuggling Drug Money To The Dominican Republic," (May 8, 2024) https://www.justice.gov/usao-sdny/pr/flight-attendants-charged-connection-smuggling-drug-money-dominican-republic; DOJ, "Four Flight Attendants Plead Guilty To Smuggling Drug Money To The Dominican Republic," (August 14, 2024) https://www.justice.gov/usao-sdny/pr/four-flight-attendants-plead-guilty-smuggling-drug-money-dominican-republic.

274 FinCEN, "FinCEN Alert on Bulk Cash Smuggling and Repatriation by Mexico-Based Transnational Criminal Organizations," (March 31, 2025) https://www.fincen.gov/system/files/shared/BCS-Alert-FINAL-508C.pdf.

275 FinCEN, "FinCEN Announces $37,000,000 Civil Money Penalty Against Brink's Global Services USA, Inc. for Violations of the Bank Secrecy Act," (February 6, 2025) https://www.fincen.gov/news/news-releases/fincen-announces-37000000-civil-money-penalty-against-brinks-global-services-usa.

276 DOJ, "Million-dollar ammunition smuggling ring dismantled," (June 28, 2024) https://www.justice.gov/usao-sdtx/pr/million-dollar-ammunition-smuggling-ring-dismantled.

277 DOJ, "TD Bank Insider Arrested and Charged with Facilitating Money Laundering," (December 11, 2024) https://www.justice.gov/archives/opa/pr/td-bank-insider-arrested-and-charged-facilitating-money-laundering; *see also*, FinCEN Consent Order Number 2024-02 (October 10, 2024), pp. 31-32, https://www.fincen.gov/system/files?file=enforcement_action/2024-10-10/FinCEN-TD-Bank-Consent-Order-508FINAL.pdf.

Cash-Intensive Businesses

Criminals use cash-intensive businesses to launder illicit cash proceeds because it is easier to commingle illicit and legitimate cash transactions compared to other payment methods since cash-intensive businesses often make bulk cash deposits in their bank accounts rather than reporting each transaction separately. In some instances, criminals may own a cash-intensive business outright and use it as a front company, and in other instances criminals may purchase goods at a third-party cash-intensive business that unwittingly or complicitly helps criminals launder their cash. To combat this method of money laundering, businesses are required to file a Report of Cash Payments Over $10,000 in a Trade or Business (Form 8300) when they receive more than $10,000 in cash in a single transaction or in related transactions.[278]

Whether a business is cash-intensive depends on the type of goods and services it offers, the social customs of the city or region it operates in, and the policies or preferences of the business owner. According to the Federal Reserve, cash use by Americans has stabilized after declining at the onset of the COVID-19 pandemic, averaging at roughly seven cash payments per consumer per month. Cash continues to be used more often at businesses where in-person payments are common, such as grocery stores, restaurants, gas stations, and general merchandise stores.[279]

In September 2025, a Florida man was sentenced to prison for engaging in money laundering through multiple businesses he owned, including a grocery store and a restaurant. According to court documents and evidence presented at the sentencing hearing, the man advertised his abilities to launder money in various states and countries. The man told undercover agents they may need to create invoices to make it appear as though they were buying or selling merchandise, and he mentioned that he would not deposit currency he received all at once; instead, he would split it up and deposit the money in increments like $5,000 per day.[280]

X. Digital Assets[281]

Since the publication of the 2024 NMLRA, the digital asset ecosystem has grown substantially. For example, the number of successful, monthly transactions on public blockchains reached highs of 3.8 billion in early 2025—a 96 percent year-over-year increase.[282] Digital asset service providers play a wide range of roles within the digital asset ecosystem. Additionally, other entities, like banks, continue to evaluate digital asset-related products and services, including offering digital asset custody, digital assets-backed lending, and exchange traded products that track the price of digital assets or issuing their own digital assets . In general, the volume of money laundering via digital assets remains well below that conducted through fiat currency and other methods that do not involve digital assets. However, certain illicit actors, particularly those engaged in digital asset-native crimes, may primarily use digital assets in the laundering process.

People use digital assets for a variety of legitimate purposes, including investments, remittances, and payments for goods and services. The ability to transfer assets quickly across borders and perceptions of anonymity, which appeal to some digital asset users, also make digital assets attractive to illicit actors. As the use of digital assets has grown, illicit actors have become more familiar with digital assets and have increasingly committed illicit activity involving digital assets, including conducting digital asset investment scams, or using digital assets in their

278 IRS, "Form 8300 and reporting cash payments of over $10,000," (updated July 24, 2025) https://www.irs.gov/businesses/small-businesses-self-employed/form-8300-and-reporting-cash-payments-of-over-10000.

279 Federal Reserve Financial Services, "2025 Findings from the Diary of Consumer Payment Choice," (May 2025) https://www.frbservices.org/binaries/content/assets/crsocms/news/research/2025-diary-of-consumer-payment-choice.pdf.

280 DOJ, "Jacksonville Man Sentenced To Federal Prison For Agreeing To Launder Over $250,000," (September 8, 2025) https://www.justice.gov/usao-mdfl/pr/jacksonville-man-sentenced-federal-prison-agreeing-launder-over-250000.

281 While various terms are used by parts of the U.S. government and the private sector, this report uses the term digital asset to refer to any digital representation of value that is recorded on a distributed ledger, including cryptocurrencies, digital tokens, and stablecoins. For the purpose of consistency, this terminology is also used in case examples, but this is intended only to facilitate an understanding of illicit finance risk and does not alter any existing legal obligations.

282 a16zcrypto, "State of Crypto Index," https://a16zcrypto.com/stateofcryptoindex. These data serve as a proxy for activity across certain blockchains (specifically, Ethereum, Polygon, Solana, Avalanche, Fantom, Celo, Optimism, Base, and Arbitrum).

laundering processes. In particular, many illicit actors using digital assets prefer stablecoins due to the relative stability compared to other digital assets as well as the liquidity in stablecoin markets. As part of the laundering process, illicit actors often seek to convert digital assets, specifically stablecoins, into fiat currency via diffuse networks of over-the-counter (OTC) brokers in third countries. These OTC brokers can receive substantial fees from illicit actors for providing cash-out services that leverage proxy accounts to circumvent digital asset service providers' CDD processes or exploit providers with weaker AML/CFT controls, among other tactics.

The United States is taking steps to ensure that the existing AML/CFT and sanctions frameworks are properly scoped to mitigate illicit finance risks associated with digital assets and encouraging innovation and protecting the liberty and privacy of Americans. In July 2025, President Trump's Working Group on Digital Asset Markets published a report on "Strengthening American Leadership in Digital Financial Technology," which included recommendations to establish a comprehensive digital assets framework in the United States.[283] The recommendations highlight that effective and clear regulation coupled with law enforcement actions against malicious actors can build confidence among U.S. users and firms seeking to grow domestically and ensure American innovators lead the digital asset industry. Also in July 2025, the president signed into law the Guiding and Establishing National Innovation for U.S. Stablecoins (GENIUS) Act, which created the first-ever federal regulatory system for stablecoins, providing regulatory clarity for stablecoin issuers.[284] As the United States pursues this work, the existing AML/CFT and sanctions frameworks continue to apply to digital assets and related covered service providers.

In the United States, digital asset service providers have AML/CFT obligations if they fall under the BSA definition of a financial institution.[285] Currently, most of the digital asset service providers licensed or registered in the United States are registered as MSBs. However, depending on the activities in which the service provider engages, certain service providers may be considered another type of financial institution, such as broker-dealers or FCMs, and have different AML/CFT obligations compared to those registered as MSBs. Further, digital asset service providers that are U.S. persons, wherever located, are required to comply with economic sanctions programs administered and enforced by OFAC. Non-U.S. persons may also have OFAC sanctions compliance obligations in some circumstances. Sanctions compliance obligations are the same regardless of whether a transaction is denominated in digital assets or fiat currency.[286]

For some predicate crimes, including certain investment scams and ransomware attacks, digital assets are the primary way in which funds are generated and laundered. For others, such as drug trafficking, fraud, and professional money laundering, digital assets are one of many ways to launder illicit proceeds, alongside the misuse of shell companies, bulk cash smuggling, or wire transfers. As described below, the most common ways illicit actors misuse digital assets include: 1) exploitation of U.S. digital asset providers that fail to comply with AML/CFT obligations; 2) jurisdictional arbitrage; 3) obfuscation tools and methods; and 4) use of digital assets outside a regulated financial institution.

Failure to Comply with AML/CFT Obligations

When covered digital asset service providers fail to register with the appropriate regulator, fail to establish and maintain sufficient AML/CFT controls, or do not comply with sanctions obligations, criminals may more easily exploit their services for nefarious purposes. In some cases, digital asset service providers may claim not to be subject to U.S. jurisdiction despite doing business wholly or in substantial part in the United States. Some digital asset service providers have even directed U.S. customers to provide false information or to use a virtual private

283 The White House, "Strengthening American Leadership in Digital Financial Technology" (July 2025), https://www.whitehouse.gov/wp-content/uploads/2025/07/Digital-Assets-Report-EO14178.pdf.

284 The White House, "Fact Sheet: President Donald J. Trump Signs GENIUS Act into Law" (July 2025), https://www.whitehouse.gov/fact-sheets/2025/07/fact-sheet-president-donald-j-trump-signs-genius-act-into-law/.

285 31 U.S.C. § 5312(a)(2); 31 C.F.R. § 1010.100(t).

286 Treasury, "Sanctions Compliance Guidance for the Virtual Currency Industry," (October 2021) https://ofac.treasury.gov/media/913571/download?inline; *see, e.g.*, OFAC, "Frequently Asked Questions," (March 19, 2018), https://ofac.treasury.gov/faqs/topic/1626; OFAC, "Frequently Asked Questions: 646," (October 15, 2021) https://ofac.treasury.gov/faqs/646; OFAC, "Frequently Asked Questions: 1021," (March 11, 2022) https://ofac.treasury.gov/faqs/1021.

network to conceal their U.S. presence when establishing accounts at onboarding to conceal their base of U.S. customers in attempts to appear as if the firm were exempt from U.S. regulatory requirements.[287]

Some digital asset service providers, including purportedly decentralized finance (DeFi) services or P2P platforms, may claim not to be regulated financial institutions subject to the BSA. Determining whether an entity, including purported DeFi services, is a covered financial institution will depend on specific facts and circumstances surrounding its financial activities.[288] In other instances, covered digital asset service providers have failed to meet AML program requirements or other requirements under the BSA and its implementing regulations, thereby allowing illicit actors to launder their illicit proceeds. In some instances, BSA-obliged digital asset service providers fail to collect customer identification information or, when subsequently introducing customer information requirements, only implement them when onboarding new customers.[289]

In one case unsealed in June 2025, a Russian citizen was charged with various offenses related to using his digital asset company Evita to funnel more than $500 million of overseas payments through U.S. banks and digital asset exchanges while hiding the source and purpose of the transactions. As alleged in the indictment, the man used his companies to enable foreign customers—many of whom held funds at sanctioned Russian banks—to provide him with digital assets, which he then laundered through digital asset wallets and U.S. bank accounts. The man ultimately converted the funds into U.S. dollars or other fiat currencies and then made payments through bank accounts in Manhattan on behalf of his foreign customers. In the process, the sources of the funds were obscured, disguising the audit trail and hiding the true counterparties to the transactions.[290]

Digital asset service providers should have adequate controls in place to mitigate risks associated with "nested" exchanges, which refers to digital asset service providers that offer trading services and pool customer deposits into an account hosted by a larger exchange to offer expanded services to their own customers. Nested exchanges may serve legitimate purposes, such as providing enhanced liquidity for their customers, but they can also present illicit finance risks.[291] For example, nested exchanges may operate fully or partially within the infrastructure of the host provider, rather than as a unique entity, potentially providing illicit actors with an additional layer of obfuscation. In such cases, the nested exchange transactions may appear to be conducted by the host provider, which can delay or impede law enforcement efforts to investigate suspicious activity. Moreover, this obfuscation may be compounded if the nested exchange lacks AML/CFT controls, which could allow illicit actors to access the host provider's services without providing identifying information and likely without detection. To mitigate this risk, digital asset service providers subject to the BSA (e.g., those registered as MSBs) are expected to ensure that their AML program has appropriate policies, procedures, and internal controls to identify "nested" activity and comply with applicable BSA requirements.

287 *See, e.g.*, DOJ, "OKX Pleads Guilty To Violating U.S. Anti-Money Laundering Laws And Agrees To Pay Penalties Totaling More Than $500 Million," (February 24, 2025) https://www.justice.gov/usao-sdny/pr/okx-pleads-guilty-violating-us-anti-money-laundering-laws-and-agrees-pay-penalties.

288 Treasury, "Illicit Finance Risk Assessment of Decentralized Finance," (April 2023), p. 2, https://home.treasury.gov/system/files/136/DeFi-Risk-Full-Review.pdf.

289 *See, e.g.*, DOJ, "OKX Pleads Guilty To Violating U.S. Anti-Money Laundering Laws And Agrees To Pay Penalties Totaling More Than $500 Million," (February 24, 2025) https://www.justice.gov/usao-sdny/pr/okx-pleads-guilty-violating-us-anti-money-laundering-laws-and-agrees-pay-penalties; DOJ, "Kucoin Pleads Guilty To Unlicensed Money Transmission Charge And Agrees To Pay Penalties Totaling Nearly $300 Million," (January 27, 2025) https://www.justice.gov/usao-sdny/pr/kucoin-pleads-guilty-unlicensed-money-transmission-charge-and-agrees-pay-penalties; DOJ, "Paxful Inc. Co-Founder Pleads Guilty to Conspiracy to Fail to Maintain Effective Anti-Money Laundering Program," (July 8, 2024) https://www.justice.gov/usao-edca/pr/paxful-inc-co-founder-pleads-guilty-conspiracy-fail-maintain-effective-anti-money.

290 DOJ, "Founder of Cryptocurrency Payment Company Charged with Evading Sanctions and Export Controls, Defrauding Financial Institutions, and Violating the Bank Secrecy Act," (June 9, 2025) https://www.justice.gov/opa/pr/founder-cryptocurrency-payment-company-charged-evading-sanctions-and-export-controls.

291 *See, e.g.*, FinCEN, "Consent Order Number 2023-04," (November 2023), p. 34, https://www.fincen.gov/system/files?file=enforcement_action/2023-11-21/FinCEN_Consent_Order_2023-04_FINAL508.pdf.

Additionally, the use of digital asset kiosks in scams has skyrocketed in recent years.[292] In 2024, the IC3 received more than 10,956 complaints reporting the use of digital asset kiosks, with reported victim losses of approximately $246.7 million.[293] This represents a 99 percent increase in the number of complaints and a 31 percent increase in reported victim losses from 2023.[294] This rise in illicit activity may be related to substantial rates of non-compliance with AML/CFT regulatory requirements by kiosk operators.[295] Digital asset kiosks are considered MSBs under the BSA.[296] According to law enforcement, scammers have directed victims to specific digital asset kiosks, sometimes across state lines, likely to avoid digital asset kiosk operators with strong AML/CFT controls.

Special Focus: Increasing Misuse of Stablecoins

Illicit actors are increasingly using stablecoins to facilitate transactions and store proceeds. The U.S. government has identified misuse of stablecoins for sanctions evasion;[297] fraud;[298] terrorist financing;[299] and proliferation financing;[300] among other crimes. The liquidity, relative stability, and rapid settlement of stablecoins appeal to illicit actors in the same way they appeal to licit users for legitimate purposes.[301] Often, illicit actors use stablecoins as one element of a complex laundering process that may include the use of digital asset service providers, switching between stablecoins and other digital assets, and transfers between self-hosted wallets. Illicit actors may also use stablecoins in the last phase of their transaction as they convert their illicit digital assets into fiat currency, which is often required to buy goods and services. Some facilitators involved in exchanging illicit proceeds in digital assets for fiat currency, including over-the-counter digital asset brokers, may request stablecoins instead of other digital assets considering the characteristics noted above.

Certain stablecoin issuers develop and maintain the underlying smart contract supporting the stablecoin. In some cases, issuers build in functionality that allows them to maintain control over and alter the use of their tokens. This can include the ability to ban specific wallet addresses from interacting with the stablecoin smart contracts, effectively "freezing" the stablecoin funds held at those addresses. Issuers may also be able to permanently remove stablecoins from circulation. Law enforcement has worked with stablecoin issuers to seize hundreds of millions of

292 FTC, "Bitcoin ATMs: A payment portal for scammers," (September 3, 2024) https://www.ftc.gov/news-events/data-visualizations/data-spotlight/2024/09/bitcoin-atms-payment-portal-scammers.

293 IC3, "Internet Crime Report 2024," (April 23, 2025), p. 36, https://www.ic3.gov/AnnualReport/Reports/2024_IC3Report.pdf.

294 Ibid.

295 FinCEN, "FinCEN Notice on the Use of Convertible Virtual Currency Kiosks for Scam Payments and Other Illicit Activity," (August 4, 2025) https://www.fincen.gov/system/files/2025-08/FinCEN-Notice-CVCKIOSK.pdf.

296 As an MSB, any non-exempt person engaged in money transmission must register with FinCEN within 180 days of starting to engage in money transmission. See 31 C.F.R. § 1022.380. Money transmitters must also comply with the recordkeeping, reporting, and transaction monitoring obligations set forth in parts 1010 and 1022 of 31 CFR chapter X. Examples of such requirements include the filing of Currency Transaction Reports (31 C.F.R. § 1022.310) and Suspicious Activity Reports (31 C.F.R. § 1022.320), as well as general recordkeeping obligations (31 C.F.R. § 1010.410).

297 *See, e.g.*, Treasury, "Treasury Exposes Money Laundering Network Using Digital Assets to Evade Sanctions," (December 4, 2024) https://home.treasury.gov/news/press-releases/jy2735

298 *See, e.g.*, DOJ, "Largest Ever Seizure of Funds Related to Crypto Confidence Scams," (June 18, 2025) https://www.justice.gov/usao-dc/pr/largest-ever-seizure-funds-related-crypto-confidence-scams.

299 *See, e.g.*, DOJ, " Justice Department Disrupts Hamas Terrorist Financing Scheme Through Seizure of Cryptocurrency," (March 27, 2025) https://www.justice.gov/usao-dc/pr/justice-department-disrupts-hamas-terrorist-financing-scheme-through-seizure; DOJ, " United States Unseals Civil Action Filed Against Approximately $2M in Digital Currency Involved in Hamas Fundraising," (July 22, 2025) https://www.justice.gov/opa/pr/united-states-unseals-civil-action-filed-against-approximately-2m-digital-currency-involved.

300 *See, e.g.*, DOJ, "Justice Department Announces Nationwide Actions to Combat Illicit North Korean Government Revenue Generation," (November 14, 2025) https://www.justice.gov/opa/pr/justice-department-announces-nationwide-actions-combat-illicit-north-korean-government.

301 *See, e.g.*, Treasury, "National Terrorist Financing Risk Assessment," (February 2024) https://home.treasury.gov/system/files/136/2024-National-Terrorist-Financing-Risk-Assessment.pdf; UN Security Council, "Final report of the Panel of Experts submitted pursuant to resolution 2680," (March 2024) https://documents.un.org/doc/undoc/gen/n24/032/68/pdf/n2403268.pdf; UNODC, "Casinos, Money Laundering, and Transnational Organized Crime in East and Southeast Asia : A Hidden and Accelerating Threat," (January 2024) https://www.unodc.org/roseap/uploads/documents/Publications/2024/Casino_Underground_Banking_Report_2024.pdf, .

dollars' worth of stablecoins involved in illicit activity by leveraging this capability.[302]

Jurisdictional Arbitrage

As highlighted in previous NMLRAs, uneven and often inadequate regulation and supervision across jurisdictions allows digital asset service providers and illicit actors to engage in regulatory arbitrage. This issue is of particular concern with digital asset service providers given the ability to transfer virtual assets across borders nearly instantaneously compared to other financial transfers, the fact that many digital asset service providers operate or have architecture in several jurisdictions, and the breadth of gaps in implementing international AML/CFT standards set forth by the Financial Action Task Force (FATF).

In 2019, the FATF clarified how its global standards on AML/CFT apply to digital assets and digital asset service providers.[303] While many countries have made progress in developing AML/CFT frameworks for digital asset service providers, a FATF survey identified that as of mid-2025, nearly 30 countries had not determined their AML/CFT approach to digital asset service providers.[304] Additionally, many countries with AML/CFT frameworks for digital asset service providers have not yet operationalized them. Law enforcement has observed illicit actors take advantage of these gaps, using foreign digital asset service providers to conceal the ownership and location of illicit proceeds as part of their laundering process.[305] In doing so, these actors may seek out service providers that do not require, among other things, customers to provide personal identifying information or identity documents.

In one case, the DOJ filed a civil action seeking the forfeiture of digital assets valued at approximately $7.1 million, which were seized in the investigation of an oil- and gas-related investment fraud scheme. According to the forfeiture filing and other records in the case, from at least August 2022 through August 2024, the co-schemers convinced victims to send money to what was represented as escrow accounts to purchase oil tank storage in either Rotterdam, Netherlands, or Houston. The money was quickly moved to one or more of at least 81 different accounts at financial institutions, moved offshore, or moved to one or more of at least 19 different accounts, where it was used for the purchase of digital assets, including Bitcoin, Tether, USD Coin, and Ether . Many of the digital assets were transferred to accounts at the digital asset service provider Binance. Some of the digital assets purchased with victims' funds were also sent to digital asset service providers in Russia and Nigeria, at least one of which is alleged to have facilitated money laundering for TCOs—including terrorist organizations and organizations that violate international trade sanctions.[306]

Obfuscation Tools and Methods

Criminals commonly use obfuscation tools, services, and methods that introduce challenges for investigators attempting to trace illicit digital assets. These tools and services include mixers, anonymity-enhancing cryptocurrencies (AECs), and money laundering services through darknet markets. In addition to selling illicit drugs and other contraband, darknet markets often offer money laundering services, mixing digital assets used for purchases of goods and services from the market. In some instances, illicit actors may deposit funds and subsequently withdraw them from darknet markets without making a purchase as a laundering technique.[307]

Illicit actors also use methods designed to obfuscate the traceability of transactions on public blockchains, which can frustrate law enforcement investigations as well as digital asset service providers attempting to detect whether

302 *See, e.g.*, DOJ, "Department of Justice Agents Seize $8.5 Million in Cryptocurrency and Disrupt Investment Fraud Scheme," (December 18, 2025) https://www.justice.gov/usao-ednc/pr/department-justice-agents-seize-85-million-cryptocurrency-and-disrupt-investment-fraud.

303 The FATF uses the terms "virtual assets" and "virtual asset service providers (VASPs)." See FATF, "Virtual Assets," https://www.fatf-gafi.org/en/topics/virtual-assets.html.

304 FATF, "Targeted Update on Implementation of the FATF Standards on Virtual Assets and Virtual Asset Service Providers," (June 2025) https://www.fatf-gafi.org/content/dam/fatf-gafi/recommendations/2025-Targeted-Upate-VA-VASPs.pdf.coredownload.pdf.

305 See the Digital Asset Investment Scams section for additional examples.

306 DOJ, "U.S. commences civil action to forfeit $7.1 million in cryptocurrency tied to oil and gas storage fraud scheme," (July 22, 2025) https://www.justice.gov/usao-wdwa/pr/us-commences-civil-action-forfeit-71-million-cryptocurrency-tied-oil-and-gas-storage.

307 *See, e.g.*, DOJ, "Bitfinex Hacker Sentenced in Money Laundering Conspiracy Involving Billions in Stolen Cryptocurrency," (November 14, 2024) https://www.justice.gov/archives/opa/pr/bitfinex-hacker-sentenced-money-laundering-conspiracy-involving-billions-stolen.

incoming funds are tied to illicit activity. Actors can chain-hop by exchanging digital assets on one blockchain for digital assets on another, including by using cross-chain bridges. Other obfuscation methods include exchanging assets using DeFi services to conduct hundreds of thousands of rapid transactions across a large network of addresses, creating a complex web of transactions.[308] While many of the addresses in such webs are often self-hosted wallets, they may also be accounts at digital asset service providers that operate off-chain.[309] Illicit actors may use false customer identification information to open accounts at these providers as part of their laundering process.[310]

Use of Digital Assets Outside Regulated Institutions

Many digital assets can be self-custodied and transferred without the involvement of an intermediary financial institution. These P2P transactions can limit authorities' collection of and access to customer and transaction information. While the BSA framework covers many digital asset service providers in the United States, the current legislative framework does not clearly account for fully decentralized protocols, where the governance or decision-making is distributed across communities of users and the protocols may be immutable. The president's Working Group on Digital Asset Markets report from July 2025 noted that to provide clarity to industry and allow tailored solutions to mitigate illicit finance risks, Congress should consider a principled approach to defining various actors in the DeFi ecosystem. Relatedly, some DeFi services may fall outside of the AML/CFT framework in the United States and, as such, may not implement measures to mitigate illicit finance risk.[311] Such instances can present a vulnerability, although these transactions may occur on public blockchains providing some transparency.[312]

XI. Financial Products and Services

Financial institutions and other entities offer a wide range of financial products and services that can allow their customers to transfer and store value. The money laundering risks of these products and services vary depending on several factors, including the level of adoption, the speed of payments, the amount of value transferred, the product's or service's level of integration with the broader financial system, and the providers' AML/CFT obligations. Although the availability and uptake of newer products and services like P2P payments and digital assets are growing, legacy products and services such as credit cards and ACH payments have also been growing in recent years, surpassing pre-pandemic levels. According to a survey conducted by the FRB, credit and debit card payments represented nearly two-thirds of all consumer payments in 2024, followed by cash (14 percent), ACH (13 percent), other (five percent), check (three percent), and mobile payment apps (less than one percent).[313]

Newer technologies, like network analysis tools that reveal hidden connections, bots to strengthen customer identification efforts, and generative AI for onboarding and transaction monitoring, have allowed providers to mitigate some risk by improving the detection and prevention of illicit activity. But illicit actors have also sought to use these tools to exploit vulnerable products and services. Financial institutions are obligated to assess the risks of products and services, especially as new ones are introduced, and the effectiveness of these ongoing efforts

308 DOJ, "Canadian Man Charged in $65M Cryptocurrency Hacking Schemes," (February 3, 2025) https://www.justice.gov/opa/pr/canadian-man-charged-65m-cryptocurrency-hacking-schemes; Indictment, United States of America v. Andean Medjedovic, No. 1:24-cr-00529-NGG (E.D.N.Y. December 30, 2024) ¶ 49 https://www.justice.gov/opa/media/1388021/dl.

309 Indictment, United States of America v. Andean Medjedovic, No. 1:24-cr-00529-NGG (E.D.N.Y. December 30, 2024) ¶ 56-57, 81 https://www.justice.gov/opa/media/1388021/dl. .

310 Ibid, ¶ 55-66.

311 The White House, "Strengthening American Leadership in Digital Financial Technology," (July 2025) p. 106-7 https://www.whitehouse.gov/wp-content/uploads/2025/07/Digital-Assets-Report-EO14178.pdf. Whether an entity operating in the DeFi space is a covered financial institution under the BSA depends on specific facts and circumstances surrounding its financial activities.

312 *See, e.g.*, DOJ, "Justice Department Seeks Forfeiture of Over $5 Million in Bitcoin Stolen in SIM Swapping Scams," (September 9, 2025) https://www.justice.gov/usao-dc/pr/justice-department-seeks-forfeiture-over-5-million-bitcoin-stolen-sim-swapping-scams.

313 Federal Reserve Financial Services, "2025 Findings from the Diary of Consumer Payment Choice," (May 2025), p. 5, https://www.frbservices.org/binaries/content/assets/crsocms/news/research/2025-diary-of-consumer-payment-choice.pdf. "Other" payments include prepaid access, account-to-account transfers, income deductions, money orders, and other methods that did not fall into the existing categories.

is a critical component of ensuring that financial products and services, new and old, do not become vectors for financial crime.

Credit Cards and Prepaid Access

Credit cards, debit cards, and prepaid access present varying illicit finance vulnerabilities. Criminals exploit cards for money laundering, fraud, and other illicit finance schemes, taking advantage of cards' high liquidity, and seamless integration into legitimate commerce. Payment cards are widely accepted and easily converted to cash or goods, which allow illicit proceeds to be moved quickly through routine transactions. Operators of credit card systems are subject to AML/CFT program, reporting, and recordkeeping requirements.[314] Furthermore, under the BSA, certain providers and sellers of prepaid access are considered MSBs and are also subject to the AML/CFT program, reporting, and recordkeeping requirements.[315]

Money laundering typologies often vary by card type, with criminals exploiting the specific vulnerabilities of each. For instance, prepaid and gift cards are a popular choice for laundering illicit funds due to their anonymity, transferability, and the fact that no account is generally needed; credit and debit cards do require an account, so schemes involving these cards often rely on stolen identities; and lax requirements on the use of EMV chips in electronic benefit transfer (EBT) cards makes them a popular target for "skimming" card information from a card's magnetic strip.

Prepaid access, including gift cards, deserves special scrutiny for both fraud and money laundering. General-purpose prepaid cards, also called open-loop gift cards, which operate on major card networks, are valuable to criminals because funds can be loaded via cash or transfer and can be withdrawn at ATMs or used for purchases, allowing movement of illicit money with less oversight than traditional wire transfers. A common scam involves a fraudster contacting a victim and telling the victim that they owe money (for instance, to pay back taxes or arrears on a life insurance policy). The victim is instructed to purchase prepaid cards and provide the criminal with the card number. Closed-loop prepaid access (i.e., store-branded cards or gift cards) are also widely used in fraud schemes and money laundering.[316]

Another common gift card scheme involves "card draining," in which criminals steal gift cards from retail displays and record the information, reseal the cards in their original packaging, and place the gift cards back onto store shelves. Once a customer purchases the gift card and loads funds onto it, the criminal has access to the funds without the customer's knowledge.[317] Such schemes have been tied to Chinese organized crime groups, and Homeland Security Investigations (HSI) estimates that card draining operations range from the hundreds of millions of dollars.[318] Gift cards are also often used as a step in the money laundering lifecycle due to their anonymity, portability (both physically and by transferring the code), and ability to easily be converted to goods. Criminals may purchase gift cards with the proceeds of crime, sometimes selling them to others at a discount, and other times using them to purchase high-value goods, which they then re-sell.[319]

Other typologies involving cards specifically target credit and debit cards, which are account-based. Similar to checks, credit and debit cards stolen in mail theft schemes can be used to purchase goods for resale or personal

314 31 CFR Chapter X, Part 1028: Rules for Operators of Credit Card Systems.

315 31 CFR Chapter X, Part 1022: Rules for MSBs.

316 FTC, "Avoiding and Reporting Gift Card Scams," (July 2023) https://consumer.ftc.gov/articles/avoiding-and-reporting-gift-card-scams.

317 *See, e.g.*, DOJ, "Chinese National Sentenced To Federal Prison For Access Device Fraud," (April 3, 2025), https://www.justice.gov/usao-mdfl/pr/chinese-national-sentenced-federal-prison-access-device-fraud.

318 HSI, "Tackling the Rise in Gift Card Fraud," (updated August 15, 2025) https://www.ice.gov/about-ice/hsi/news/hsi-insider/tackling-gift-card-fraud.

319 *See, e.g.*, DOJ, " Three Los Angeles County Men Sentenced to Federal Prison for Laundering Gift Cards Purchased by Victims of Telephone Scams," (March 26, 2024) https://www.justice.gov/usao-cdca/pr/three-los-angeles-county-men-sentenced-federal-prison-laundering-gift-cards-purchased.

use.[320] Credit and debit cards are also targeted via card skimming devices and through "bust-out" schemes, in which criminals defraud banks by opening card accounts, often with stolen identities and then "bust out" by making large purchases. In one case, a dual U.S. and Greek national was charged in connection with a multi-million-dollar bank fraud conspiracy. According to documents filed in the case and statements made in court, the man and co-conspirators would create shell companies and open bank accounts in those companies' names. They would then fund those accounts with nominal funds. Then, after a few months with no activity, they would fund the accounts via transfers from external sources, including accounts they controlled. Several weeks later, they would make very large debit purchases over the course of several days from those accounts, causing those accounts to accrue significantly negative balances. They executed this scheme numerous times at six victim financial institutions between July 2022 and July 2023, causing those institutions approximately $2.8 million in losses.[321]

Card skimming, in which criminals install skimmer devices on ATMs, gas pumps, or point-of-sale terminals to steal card data and PINs, also targets the inherent vulnerability of card payments. Specifically, EBT cards are an appealing target for illicit actors because they are largely not chip-enabled, making them far easier to compromise and cash out.[322] According to the U.S. Secret Service (USSS), it is estimated that EBT skimming alone costs financial institutions and consumers more than $1 billion each year.[323] The USDA encourages chip functionality but leaves adoption up to states; California began issuing chip-enabled EBT cards in January 2025, with adoption planned in a few other states.[324] In August 2025, an illegal alien from Romania was sentenced to 120 months in federal prison for skimming tens of thousands of EBT cards in California and New York. The man entered the U.S. on a tourist visa in 2020 but overstayed his visa. He travelled across Los Angeles and the Inland Empire installing sophisticated skimming devices in ATMs and point-of-sale terminals to record the account information of individuals who used those devices. He worked with multiple members of a TCO from Romania to carry out this scheme. A search warrant for the residence of one of his accomplices revealed that he had sent them more than 36,000 stolen EBT card numbers over three years.[325]

Peer-to-Peer Payments

Peer-to-peer (P2P) payment platforms, such as Zelle, Venmo, PayPal, Cash App, and Apple Pay, have become widely used in the United States over the past decade. These services allow instant, low-cost transfers between individuals, and while convenient for consumers, they also present vulnerabilities that illicit actors can exploit. Criminals can exploit P2P platforms for money laundering, fraud schemes, the sale of illegal goods, and other illicit finance purposes, by taking advantage of the speed and scale of these systems. P2P payment platforms may meet the MSB definition and be subject to AML/CFT program, reporting, and recordkeeping requirements.[326]

P2P payments are fast, widely adopted, and often irrevocable, making them ideal for moving and disguising illicit funds. In 2024, the U.S. domestic network, Zelle, alone processed over $1 trillion across 3.6 billion transfers[327]—an enormous volume into which criminals can try to blend. Many P2P platforms charge no fees and operate 24/7,

320 *See, e.g.*, DOJ, "Carson Woman and Former U.S. Postal Service Employee Sentenced to More Than 5 Years in Federal Prison for Stealing Checks and Credit Cards from Mail," (December 8, 2025) https://www.justice.gov/usao-cdca/pr/carson-woman-and-former-us-postal-service-employee-sentenced-more-5-years-federal.

321 DOJ, "Dual U.S. and Greek National Arrested for Multimillion-Dollar Bank Fraud Conspiracy," (March 6, 2024) https://www.justice.gov/usao-nj/pr/dual-us-and-greek-national-arrested-multimillion-dollar-bank-fraud-conspiracy.

322 FBI, "Skimming," (updated November 18, 2025) https://www.fbi.gov/how-we-can-help-you/scams-and-safety/common-frauds-and-scams/skimming.

323 USSS, "Law Enforcement Agencies Conduct EBT Fraud and Card Skimming Outreach," (January 31, 2025) https://www.secretservice.gov/newsroom/releases/2025/01/law-enforcement-agencies-conduct-ebt-fraud-and-card-skimming-outreach.

324 USDA, "SNAP EBT Modernization," (updated December 7, 2025) https://www.fns.usda.gov/snap/ebt/modernization.

325 DOJ, "Romanian Man Sentenced to 10 Years in Federal Prison for Skimming Tens of Thousands of Welfare Cards at ATMs," (August 4, 2025), https://www.justice.gov/usao-cdca/pr/romanian-man-sentenced-10-years-federal-prison-skimming-tens-thousands-welfare-cards.

326 31 CFR Chapter X, Part 1022: Rules for MSBs.

327 Zelle, "Zelle Shatters Records with $1 Trillion Sent in a Single Year," (February 12, 2025) https://www.zellepay.com/press-releases/zelle-shatters-records-1-trillion-sent-single-year.

whereas bank transfers might take days and can be comparatively expensive. This convenience also means that fraudulent or illegal transfers can happen quickly and be hard to reverse, leaving victims and financial institutions little time to detect or claw back illicit payments. Moreover, P2P platforms often integrate with users' bank accounts, debit cards, or credit cards, allowing criminals to move funds through multiple institutions rapidly.

Money launderers use P2P platforms to layer and integrate illicit proceeds from predicate crimes. Drug trafficking, fraud, and other criminal enterprises have utilized P2P transfers extensively to move dirty money into and through the banking system. In one case, a woman pleaded guilty to conspiracy to distribute controlled substances and money laundering. A review of the woman's bank records revealed she received and spent more than $2 million from 2017 to 2023. Agents traced her drug transactions through P2P applications such as Zelle and Cash App.[328] P2P platforms can also be just one component of complex money laundering schemes relying on several methods to disguise origin and ownership. In June 2025, the DOJ unsealed an indictment charging two men with bank fraud and aggravated identity theft. According to court documents, one man took over multiple bank accounts belonging to two elderly victims at two separate banks. The two men funneled the stolen money through pass-through accounts created in the victims' names. They then ultimately disbursed the money to themselves using ATM cash withdrawals, personal checks, Western Union transactions, Zelle transactions, payments to credit cards, online gambling, and the purchase of a Mercedes.[329]

Fraud schemes targeting consumers increasingly leverage P2P platforms to steal funds, as scammers exploit the speed and finality of these transactions. According to the FTC, reported losses from fraud on payment apps have grown an average of 47 percent year-over-year for the past four years, reaching $390 million in 2024. This likely represents only a fraction of total fraud.[330] Scams involving P2P payments often begin with the scammer contacting their victims via email and phone calls and end with the scammer directing the victim to send money through a P2P platform to "reverse" a fictional fraudulent transaction by making a P2P payment to what they believe is their own account, but is, in fact, an account controlled by the fraudsters.[331]

Beyond fraud and money laundering, P2P platforms are often used to facilitate payments for illegal goods and services, ranging from drug sales to unlicensed gambling or even human smuggling fees. These efforts can be facilitated by P2P platforms that fail to meet their AML/CFT obligations. In January 2025, Block, Inc. (Block) paid an $80 million penalty to 48 states and the District of Columbia and agreed to undertake corrective action for violations of the BSA and AML laws in connection with its mobile payment service, Cash App.[332] State regulators found Block was not in compliance with certain requirements, creating the potential that its services could be used to support money laundering, terrorism financing, or other illegal activities.[333]

---

328 DOJ, "Rosedale Woman Pleads Guilty to Conspiracy to Distribute Controlled Substances and Money Laundering," (June 4, 2025), https://www.justice.gov/usao-md/pr/rosedale-woman-pleads-guilty-conspiracy-distribute-controlled-substances-and-money.

329 DOJ, "Brothers-in-Law Indicted for Bank Takeover Scheme and Aggravated Identity Theft," (June 17, 2025) https://www.justice.gov/usao-edca/pr/brothers-law-indicted-bank-takeover-scheme-and-aggravated-identity-theft.

330 Reported losses were $87.3 million in 2020, $129.3 million in 2021, $163.5 million in 2022, $209.9 million in 2023, and $391 million in 2024. See FTC, Tableau public dashboard, https://public.tableau.com/app/profile/federal.trade.commission/viz/FraudReports/PaymentContactMethods.

331 FTC, "Do you use payment apps like Venmo, CashApp, or Zelle? Read this," (August 14, 2023) https://consumer.ftc.gov/consumer-alerts/2023/08/do-you-use-payment-apps-venmo-cashapp-or-zelle-read; *see, e.g.*, DOJ, "Florida Man Admits Defrauding Zelle Users," (May 21, 2024), https://www.justice.gov/usao-ct/pr/florida-man-admits-defrauding-zelle-users.

332 Conference of State Bank Supervisors (CSBS), "State Regulators Issue $80 Million Penalty to Block, Inc., Cash App for BSA/AML Violations," (January 15, 2025) https://www.csbs.org/newsroom/state-regulators-issue-80-million-penalty-block-inc-cash-app-bsaaml-violations.

333 Separately, in April 2025, Block, Inc. paid a $40 million penalty to the New York Department of Financial Services (NY DFS) for significant failures in its BSA/AML compliance program. The NY DFS investigation revealed critical gaps in Block's BSA/AML program, including inadequate CDD, failure to implement sufficient risk-based controls designed to prevent money laundering and illicit activity, and failure to effectively and timely monitor transactions. Notably, Block's lax treatment of high-risk Bitcoin transactions allowed largely anonymous transactions to proceed without proper scrutiny. Additionally, Block's rapid growth between 2019 and 2020 contributed to a severe transaction alert backlog, which Block left unaddressed for a significant period of time. NY DFS, "Superintendent Adrienne A. Harris Secures $40 Million Settlement with Block, Inc. for Inadequate Anti-Money Laundering Program and Virtual Currency Compliance Failures on Cash App Platform," (April 10, 2025) https://www.dfs.ny.gov/reports_and_publications/press_releases/pr202504101.

Money Orders

A money order is a prepaid monetary instrument that a payee can negotiate just as they would a check. Money orders are typically marketed to un- or under-banked consumers sold at post offices and agents of MSBs, like Western Union and MoneyGram, in addition to banks. Unlike with personal checks, the purchaser of a money order is not required to maintain a bank account. Money orders cannot bounce because the sender has paid the full amount at the time of purchase, and they are typically issued with a maximum individual value of up to $1,000.

Money orders continue to be exploited to launder the proceeds of a wide range of crimes. They may be attractive to criminals for several reasons: money orders offer a way to convert illicit funds into a monetary instrument that is not inherently suspicious because the value is paid upfront and guaranteed, making them as good as cash for many purposes; they can be purchased anonymously at thousands of agent locations across the country; they can be purchased with bulk cash in consecutively numbered strings of money orders aggregating below $3,000; they do not expire; and they can be physically lighter than an equivalent value in cash. The number of SARs filed by financial institutions in connection with money orders has fallen nearly 30 percent between 2021 and 2024, suggesting a possible decline in their use for illicit finance.[334]

The risks associated with money orders are partially mitigated by issuers or sellers of money orders being subject to BSA requirements. Issuers or sellers of money orders are classified as MSBs if they sell or issue money orders in an amount greater than $1,000 to any person on any day in one or more transactions.[335] As MSBs, issuers and sellers are subject to certain recordkeeping, registration, AML program, and reporting requirements pursuant to the BSA and its implementing regulations, including filing SARs and CTRs.[336] For currency purchases of $3,000 or more (including multiple purchases of individual money orders that aggregate to $3,000 or more), issuers and sellers must verify and record the purchaser's identity; however, that information is not necessarily validated instantaneously or retroactively, which illicit actors exploit by using fake or synthetic identification.[337]

A review of law enforcement cases over the last two years reveals that money orders are sometimes used to launder illicit or fraudulently obtained funds, such as the proceeds of cybercrime or drug trafficking. Money orders are used by criminals for structuring to circumvent recordkeeping and reporting thresholds as part of laundering illicit proceeds.[338] After purchasing money orders with illicit funds, criminals deposit the funds into their own accounts or those of accomplices, sometimes using bank accounts opened using stolen identities.[339] Once placed in the financial system the proceeds of money orders can be further transferred to other bank accounts, used to purchase luxury items, or reinvested back into the criminal enterprise.

Insurance

Insurance products pose a lower risk of money laundering than other financial products because the products are generally held for extended time periods and are not sufficiently flexible for laundering illicit proceeds.[340] Insurance companies that offer covered insurance products, such as certain annuities and life insurance products, are subject to the BSA and undergo regular AML/CFT examinations and have SAR-filing obligations, further mitigating money

334 Financial institutions filed 478,568 and 336,832 SARs in connection with money orders in 2021 and 2024, respectively. As of November 30, 2025, they have filed 271,558 SARs, continuing a declining trend. FinCEN, "Suspicious Activity Report Statistics (SAR Stats)," https://www.fincen.gov/reports/sar-stats.

335 31 C.F.R. § 1010.100(ff)(3).

336 31 C.F.R. § 1022.210, 1010.311, 1022.320.

337 31 C.F.R. § 1010.415

338 *See, e.g.*, DOJ, "Raymore Man Sentenced for Drug Trafficking, Illegal Firearms," (December 13, 2024) https://www.justice.gov/usao-wdmo/pr/raymore-man-sentenced-drug-trafficking-illegal-firearms.

339 *See, e.g.*, DOJ, "Wyoming County Man and Raleigh County Woman Sentenced for Evading Financial Reporting Requirements," (October 21, 2024) https://www.justice.gov/usao-sdwv/pr/wyoming-county-man-and-raleigh-county-woman-sentenced-evading-financial-reporting.

340 See FATF, "Guidance for a Risk-based Approach: Life Insurance Sector," (2018), p. 9, https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/RBA-Life-Insurance.pdf.coredownload.pdf.

laundering risk. In 2024, insurance companies and depository institutions filed just over 1,000 SARs related to suspicious activity involving covered insurance products.[341]

When covered insurance products are used to launder illicit proceeds, the predicate crime is often fraud, sometimes related to the covered product itself. For example, in July 2025 a husband and wife were sentenced to 12 and four years in prison, respectively, after their convictions for a scheme to commit insurance fraud. According to court documents and evidence presented at trial, the couple conspired to defraud insurance companies by obtaining over 40 life insurance policies for applicants by misrepresenting their health, wealth, and existing life insurance coverage. The total death benefits from these policies exceeded $20 million. To conceal the fraud, the couple transferred the money they made from the fraud through multiple bank accounts, including accounts in the name of trusts.[342]

XII. Legal Entities and Arrangements

Illicit actors frequently misuse legal entities and arrangements to launder illicit proceeds, though the sophistication of individual schemes varies widely depending on the predicate crime, the location of the perpetrators, the location of the legal entity or arrangement, and the degree to which perpetrators seek to disguise their identities.

Shell Companies

Shell companies[343] are legal business entities that have no physical presence, have few or no employees, and generate little to no independent economic value. They are generally organized as limited liability companies (LLCs) or corporations because those entities are easy and inexpensive to form and administer. Most shell companies in the United States are legitimate and are used because they can limit liability, facilitate mergers and acquisitions, aid in tax planning, and provide privacy. Like most U.S. companies, shell companies are generally incorporated under state law.

Shell companies are used in money laundering schemes because they can allow illicit actors to portray illicit transfers as legitimate business activity and obscure their identities when owned by money mules or nominees. This can make it harder for financial institutions to prevent illicit actors from misusing their products and services and for law enforcement to identify the perpetrators of illicit activity. During the assessment period, shell companies were used to facilitate several different types of financial crime, including evading sanctions, paying and receiving bribes, defrauding healthcare programs, and laundering the proceeds of drug trafficking, cybercrime, and fraud schemes, among other crimes.

Domestic shell companies are used in third-party money laundering schemes, such as those involving money mules and CMLNs, because criminals believe they may be able to move more funds through a financial institution when the transactions are disguised as business payments. Financial institutions are generally adept at identifying and reporting on money laundering activity involving shell companies, however, and law enforcement can use those reports to unravel the schemes. In one case, six members of a prolific CMLN, including four Chinese nationals, pleaded guilty to money laundering charges involving drug trafficking proceeds. According to court documents, the CMLN laundered over $92 million in illicit funds. The organizer directed a group of couriers to pick up bulk cash proceeds from unlawful activities, including narcotics trafficking, from individuals throughout the United States. The couriers then deposited these illicit funds, which generally exceeded $10,000, into shell company bank accounts

341 Insurance companies and depository institutions, respectively, filed 696 and 372 SARs related to insurance products in 2024. FinCEN, "Suspicious Activity Report Statistics (SAR Stats)," https://www.fincen.gov/reports/sar-stats.

342 DOJ, "Maryland Couple Sentenced for $20M Insurance Fraud Scheme," (July 8, 2025) https://www.justice.gov/opa/pr/maryland-couple-sentenced-20m-insurance-fraud-scheme.

343 Shelf companies are a type of shell company created with no immediate purpose and put on the "shelf" to age. Legitimate actors may purchase shelf companies to avoid having to create their own or gain access to business activity in a certain jurisdiction. Illicit actors may also purchase shelf companies to make their activity appear more legitimate.

controlled by the CMLN in order to conceal the nature of the illicit funds.[344]

Foreign shell companies present heightened national security and illicit finance risks because they are often used by threat actors operating from sanctioned jurisdictions, such as Iran, and because their use may allow illicit actors to expatriate illicit proceeds beyond the reach of U.S. law enforcement.[345] U.S. law enforcement has a broad range of tools they can employ to identify the beneficial owners of U.S. legal entities, such as through state-level registries, IRS data, commercial databases, and records held by financial institutions or other companies, but identifying the beneficial owners of foreign-based or foreign-owned shell companies through mutual legal assistance requests can take years or even be prohibited by a foreign country's data privacy laws. Under FinCEN regulations, certain foreign legal entities are required to report beneficial ownership information (BOI).[346]

The following cases demonstrate how illicit actors use foreign shell companies to perpetrate several types of financial crimes, including proliferation financing, fraud, and bribery:

- **Proliferation Financing:** In April 2025, a complaint was unsealed charging two Iranian nationals and an Iranian company with conspiring to procure U.S. parts for Iranian Unmanned Aerial Vehicles (UAVs, also known as drones), conspiring to provide material support to the Islamic Revolutionary Guard Corps (IRGC)—a designated FTO—and conspiring to commit money laundering. According to court documents, the defendants used various front or shell companies to pay for UAV parts and to obfuscate the true end destination and the true identities of the sanctioned end users, including the IRGC, which were acquiring U.S.-made parts through the Iranian company. The men used at least three shell companies, which were all based in the UAE, to pay a PRC-based company that sent invoices to the Iranian company for the sale of motors. Those payments were processed through U.S.-based correspondent bank accounts. The men also used two of these shell companies to pay a separate PRC-based company for the sale of pneumatic masts—a drone operation component.[347]

- **Digital Asset Investment Scams:** In September 2025, a California man was sentenced to 51 months in federal prison for his role in laundering more than $36.9 million from victims in an international digital asset investment scam conspiracy that was carried out from scam centers in Cambodia. According to court documents, the man co-owned the Bahamas-based company Axis Digital Limited. More than $36.9 million in victim funds were transferred from U.S. bank accounts controlled by the co-conspirators to a single account at Deltec Bank in the Bahamas, opened in the name of Axis Digital Limited. The man and other co-conspirators directed Deltec Bank to convert victim funds to stablecoins and to transfer the converted funds to a digital asset wallet controlled by individuals in Cambodia.[348]

344 DOJ, "Final Three Members Charged in Prolific Chinese Money Laundering Scheme Plead Guilty to Laundering Tens of Millions in Drug Proceeds," (July 7, 2025) https://www.justice.gov/opa/pr/final-three-members-charged-prolific-chinese-money-laundering-scheme-plead-guilty-laundering.

345 As noted regarding domestic shell companies, many foreign shell companies are legitimate and are used because they can limit liability, facilitate mergers and acquisitions, aid in tax planning, and provide privacy. For example, it is common for private fund structures to have an offshore fund vehicle that facilitates tax-efficient investments by U.S. tax-exempt investors.

346 FinCEN, "Beneficial Ownership Information Reporting Requirement Revision and Deadline Extension," (Interim Final Rule, 90 FR 13688, 13697 (March 26, 2025) https://www.federalregister.gov/documents/2025/03/26/2025-05199/beneficial-ownership-information-reporting-requirement-revision-and-deadline-extension.

347 DOJ, "Iranian Company and Two Iranian Nationals Charged with Conspiring to Provide Material Support to Islamic Revolutionary Guard Corps (IRGC) and for Scheme to Procure U.S. Technology for Iranian Attack Drones," (April 1, 2025) https://www.justice.gov/opa/pr/iranian-company-and-two-iranian-nationals-charged-conspiring-provide-material-support. *See also*, Treasury, "The Departments of Treasury and Justice Take Action Against Iranian Weapons Procurement Network," (April 1, 2025) https://home.treasury.gov/news/press-releases/sb0066.

348 DOJ, "California Man Sentenced for Role in Global Digital Asset Investment Scam Conspiracy Resulting in Theft of More than $36.9M from Victims," (September 8, 2025) https://www.justice.gov/opa/pr/california-man-sentenced-role-global-digital-asset-investment-scam-conspiracy-resulting.

- **Paying Bribes:** In March 2024, Gunvor S.A. (Gunvor), a part of the Gunvor Group, one of the largest commodities trading firms in the world, pleaded guilty to one count of conspiracy to violate the Foreign Corrupt Practices Act (FCPA). According to the company's admissions and court documents, between 2012 and 2020, Gunvor and its co-conspirators paid more than $97 million to intermediaries understanding that some of the money would be used to bribe numerous Ecuadorian officials. The bribe payments were routed through banks in the United States using shell companies in Panama and the British Virgin Islands controlled by Gunvor's co-conspirators. In exchange for these bribe payments, high-level Ecuadorian officials helped Gunvor win contracts to provide a series of oil-backed loans to Petroecuador. In total, Gunvor earned more than $384 million in profits from the business it corruptly obtained related to Petroecuador.[349]

- **Government Benefits Fraud:** In November 2025, a man was sentenced to 10 years in prison for his role in the $300 million Feeding Our Future case in Minnesota, the largest COVID-19 fraud scheme in the United States. As demonstrated at trial, the man and his codefendants stole more than $47 million in program funds by claiming to serve 18 million meals to kids at more than 30 food distribution sites. The man and his co-conspirators engaged in a conspiracy to launder the proceeds of their fraud scheme using a series of shell companies both in the United States and Kenya. The man helped distribute millions of dollars in fraudulent proceeds among their money laundering entities. The man also set up his own shell company that he used to receive and launder his share of the fraud proceeds by disguising them as "consulting" and similar payments. In all, the man used his shell company to receive more than $900,000 in fraud proceeds.[350]

Treasury also continues to monitor foreign partners' efforts to collect BOI and effectively use that data to investigate and prosecute cases involving shell companies. Some countries, for example, have established more comprehensive BOI registries and collection requirements, but this may not thoroughly mitigate risk, since vast databases of user-submitted information may contain fraudulent, inaccurate, vague, or repeatedly used registration data.

Domestically, FinCEN's CDD Rule and the tailored implementation of the Corporate Transparency Act (CTA) have improved the ability to access BOI and identify and stop criminal activity. The CDD rule took effect in 2018 and requires certain financial institutions to identify and verify the identities of the beneficial owners when a legal entity customer first opens an account with the institution. Law enforcement can access this information in certain circumstances, leading to prompter investigations of financial crimes. Enacted as part of the Anti-Money Laundering Act of 2020 (AML Act), the CTA requires specified "reporting companies" to provide BOI to FinCEN, including at the point of creation or registration. FinCEN stores this data in a secure database, which certain law enforcement agencies can access to facilitate investigations. In March 2025, FinCEN issued an interim final rule that defines reporting companies as entities formed under the law of a foreign country and registered to do business in the United States.[351] This revision reflected FinCEN's findings about the heightened national security and illicit finance risks posed by foreign illicit actors, as demonstrated by the above case examples. These reporting companies were required to submit BOI to FinCEN effective April 25, 2025.

Regulating legal entities to combat money laundering requires balance between protecting the financial system from illicit activity and avoiding an undue burden on legitimate businesses, especially for smaller businesses. Despite the misuse of domestic and foreign shell companies by illicit actors who likely would be undeterred by

349 DOJ, "Gunvor S.A. Pleads Guilty to Scheme to Bribe Ecuadorian Officials and Ordered to Pay Over $600 Million in Criminal Penalties," (March 1, 2024) https://www.justice.gov/usao-edny/pr/gunvor-sa-pleads-guilty-scheme-bribe-ecuadorian-officials-and-ordered-pay-over-600.

350 DOJ, "Feeding Our Future Defendant Sentenced to 10 Years in Prison," (November 24, 2025) https://www.justice.gov/usao-mn/pr/feeding-our-future-defendant-sentenced-10-years-prison.

351 FinCEN, "Beneficial Ownership Information Reporting Requirement Revision and Deadline Extension," (Interim Final Rule, 90 FR 13688, 13697 (March 26, 2025) https://www.federalregister.gov/documents/2025/03/26/2025-05199/beneficial-ownership-information-reporting-requirement-revision-and-deadline-extension.

even the strictest of regulatory regimes, U.S. law enforcement in its follow-the-money approach has been, and will continue to be, the global leader in unraveling nominee ownership including in cross-border cases for money laundering.

Front Companies

In the context of illicit finance, front companies are legal entities that provide legitimate goods or services and use that economic activity as a "front" to disguise illicit activity. As previously described, shell companies have several legitimate uses, whereas front companies, by definition, are always involved in illicit activity. Financial institutions and auditors are generally capable of identifying anomalous transactions indicative of money laundering in front companies, forcing money launderers to fabricate documents or make false statements to explain the transactions. Under FinCEN regulations implementing the CTA, front companies that meet the definition of a reporting company would be required to report BOI. Front companies can be used to evade sanctions and launder the illicit proceeds of fraud and drug trafficking, among other crimes.[352]

In one case, according to the allegations contained in the indictment, the CFO of a multinational media company conspired with others to participate in a sprawling, transnational scheme to launder at least approximately $67 million of illegally obtained funds to bank accounts in the names of the media company and related entities (collectively, the "Media Entities"). Scheme participants used digital assets to knowingly purchase tens of millions of dollars in crime proceeds, including proceeds of fraudulently obtained unemployment insurance benefits, that had been loaded onto tens of thousands of prepaid debit cards. Once the crime proceeds were purchased, participants in the scheme used stolen PII to open accounts, including prepaid debit card accounts, digital asset accounts, and bank accounts, that were used to transfer the crime proceeds into bank accounts associated with the Media Entities. When banks, including two U.S.-based banks, asked the CFO about the increase in transactions entering the bank accounts of the Media Entities, the CFO lied, claiming that the increase in funds came from donations.[353]

Trusts

Trusts are relationships in which one person holds the title to property and is subject to an obligation to keep or use the property for the benefit of another.[354] Trusts are formed under state law, and are widely used for legitimate purposes, particularly estate and tax planning. They allow families and businesses to manage assets discreetly, safeguard the interests of minors or financially inexperienced beneficiaries, and, in the case of inheritances, avoid probate and, in some circumstances, reduce tax liabilities.

Foreign-established trusts (foreign trusts) that connect to the U.S. financial system, particularly those used to hold assets like real estate, represent the greater money laundering risk. Foreign trusts often limit law enforcement access to beneficial ownership and related information, heightening their vulnerability to sanctions evasion and allowing the laundering of illicit proceeds of a predicate crime with a foreign nexus, such as corruption or fraud.[355] While law enforcement has identified some misuse of trusts established in the United States (domestic trusts) related to fraud

352 *See, e.g.*, DOJ, "Venezuelan National and U.S. Citizen Arrested for Sanctions Evasion and Smuggling in Scheme to Supply Venezuela's State-Owned Steel Industry," (June 16, 2025) https://www.justice.gov/opa/pr/venezuelan-national-and-us-citizen-arrested-sanctions-evasion-and-smuggling-scheme-supply; DOJ, "Michigan Business Owner Sentenced to Three Years in Prison for Money Laundering and Obstructing the IRS," (March 4, 2024) https://www.justice.gov/archives/opa/pr/michigan-business-owner-sentenced-three-years-prison-money-laundering-and-obstructing-irs; DOJ, " Mexican National Sentenced to More Than Five Years in Prison for Conspiring to Traffic Cocaine and Money Laundering," (September 4, 2025) https://www.justice.gov/usao-ma/pr/mexican-national-sentenced-more-five-years-prison-conspiring-traffic-cocaine-and-money.

353 DOJ, "Chief Financial Officer Of Multinational Media Company Charged With Participating In Scheme To Launder At Least $67 Million In Fraud Proceeds," (June 3, 2024) https://www.justice.gov/usao-sdny/pr/chief-financial-officer-multinational-media-company-charged-participating-scheme;

354 IRS, "Definition of a trust," (updated January 30, 2025) https://www.irs.gov/charities-non-profits/definition-of-a-trust.

355 *See, e.g.*, DOJ, "Federal Courts Authorize IRS 'John Doe' Summonses to Trident Trust Entities," (January 30, 2025) https://www.justice.gov/opa/pr/federal-courts-authorize-irs-john-doe-summonses-trident-trust-entities.

against a beneficiary or tax-related offenses, domestic trusts have an overall lower risk profile for money laundering and sanctions evasion as they require specialized knowledge to establish and administer. Illicit finance actors are more likely to choose less complex and time-consuming methods as trusts often involve multiple parties, such as the settlor, trustee, and beneficiaries. Unlike foreign trusts, law enforcement can seek information about domestic trusts, such as information about settlors or beneficiaries, through judicial or administrative channels.

Moreover, due to the CDD Rule, covered financial institutions are required to have risk-based CDD policies and procedures that consider trusts and trustees. For example, trustees are generally expected to inform covered financial institutions of their status as trustees during the account opening process. Additionally, regardless of where a trust is formed, if there are U.S. persons who may be settlors or beneficiaries, or who conduct transactions with both U.S.-source and certain foreign-source income, the trust could remain subject to federal tax filing obligations with the IRS.[356] These requirements create additional transparency for any trust with a U.S. nexus. Trust administration also remains subject to state or territorial statutes and court supervision. Many states also require tax filings or probate disclosures for trusts with local ties. Common law fiduciary obligations, such as the duties of loyalty, prudence, impartiality, recordkeeping, and disclosure, apply to trustees. These legal obligations provide recourse against abuse and enhance accountability. Treasury's rule on non-financed residential real estate transfers by trusts or legal entities, which takes effect on March 1, 2026, will require reporting of beneficial ownership information in most non-financed residential real estate transactions across the United States.[357] The rule significantly reduces the ability of illicit actors to launder proceeds through U.S. real estate held in trust structures.

The creation and administration of trusts is often connected to gatekeepers described in the next section. For example, in December 2025, a natural U.S. person agreed to pay $1,092,000 to settle potential civil liability to OFAC for apparent violations of Ukraine-/Russia-related sanctions. The person is an attorney and former U.S. government official. The conduct giving rise to the apparent violations took place between 2018 and 2022 when the person served as the fiduciary of the family trust of a sanctioned Russian oligarch. Over the course of the person's time as fiduciary, they authorized the transfer of trust assets, paid various service providers on behalf of the trust, and authorized various substantive actions taken by the trust, which resulted in a total of 122 apparent violations of the Ukraine-/Russia-Related Sanctions Regulations.[358]

XIII. Gatekeepers

Gatekeepers are trusted professionals and entities that can help their clients access the financial system. Although these entities may have some federal or state AML/CFT obligations, they are not subject to comprehensive AML/CFT requirements and may be exploited by illicit actors in money laundering schemes, inadvertently or willingly. Certain gatekeepers face a wide range of money laundering risks that are influenced by their customer base, services offered, and geographic footprint, among several other factors. This risk assessment looks at the risk posed by four of the largest gatekeeper sectors in the United States that may be exploited for financial crime.[359]

356 Generally, the fiduciary of the domestic non-grantor trust is required to file Form 1041 (U.S. Income Tax Return for Estates and Trusts) to report trust income, if any. Specific tax forms that identify the trust's beneficiaries and report their share of income are required for a tax year if distributions are made. The trustee of a foreign non-grantor trust generally is required to file Form 1040-NR (U.S. Nonresident Alien Income Tax Return) to report U.S.-source and certain foreign-source income, if any. A foreign trust with a U.S. owner also must file Form 3520-A (Annual Information Return of Foreign Trust with a U.S. Owner).

357 FinCEN, "Residential Real Estate Rule Frequently Asked Questions," (updated December 18, 2025) https://www.fincen.gov/rre-faqs.

358 OFAC, "OFAC Settles with an Individual for $1,092,000 Related to Apparent Violations of Ukraine-/Russia-Related Sanctions," (December 9, 2025) https://ofac.treasury.gov/media/934806/download?inline.

359 FATF's July 2024 "Horizontal Review of Gatekeepers' Technical Compliance Related to Corruption" report defines gatekeepers by sector, specifically 1) lawyers, notaries and other independent legal professionals, 2) accountants, 3) trust and company service providers, and 4) real estate agents, which are specific designated non-financial businesses and professions that can perform specific financial tasks for clients (See "The FATF Recommendations," (updated October 2025), pp. 19-21, https://www.fatf-gafi.org/content/dam/fatf-gafi/recommendations/FATF%20Recommendations%202012.pdf.coredownload.inline.pdf).

Attorneys

Attorneys in the United States can pose a money laundering risk when they serve as an intermediary between clients and the financial system, such as by managing client funds; creating, operating, or managing client legal entities; or buying and selling real estate. In performing these services, attorneys may help clients launder money by obscuring the origin of illicit proceeds. Compared to other professionals that offer similar services, attorneys may facilitate this laundering more easily due to the opacity afforded by attorney-client privilege and an attorney's duty of confidentiality. While the furtherance of criminal acts by attorneys is not covered under this privilege (the "crime-fraud exception"), this limitation is narrowly applied by courts and the existence of the exception does not, by itself, result in the disclosure of instances of illicit finance facilitated by attorneys to law enforcement.

While attorneys in the United States are not subject to comprehensive AML/CFT regulations, they are bound to certain ethics practices meant to deter illicit finance in the legal sector, and due to the reliance on the highly regulated financial services sector to conduct transactions, there are measures in place, such as CDD and suspicious activity reporting, at covered financial institutions that help to mitigate illicit finance risks in the legal sector. In particular, the American Bar Association (ABA)—which is a voluntary organization led by its members—maintains a series of Model Rules of Professional Conduct (the Model Rules). Many state bar associations model their rules of professional conduct on the Model Rules. As discussed in the 2024 NMLRA, in 2023, the Model Rules were amended to include money laundering risks among the factors an attorney must consider in determining whether to decline or withdraw from a client representation. In August 2024, the ABA issued its first guidance on the 2023 amendments, noting an implicit "obligation to conduct a *reasonable* risk-based inquiry, not a perfunctory one and not one that involves a dragnet-style operation to uncover every fact about every client."[360]

One particular area of risk is "Interest on Lawyers' Trust Accounts" (IOLTAs),[361] which are interest-bearing, pooled accounts held by an attorney on behalf of their clients. Attorneys and law firms use IOLTAs, which are required by most state laws and professional responsibility rules, to manage client trust funds. Financial institutions that hold IOLTAs typically only know the identity of the lawyer in whose name the IOLTA is titled and do not know the identity of the underlying clients who are the actual owners of the funds. Given banks' limited visibility into the actual owner and source of the funds, an attorney who allows clients to use their account to move illicit proceeds may avoid or delay raising red flags at the bank.

In one case, an attorney was sentenced to nine months in federal prison for knowingly transferring, and aiding and abetting the transfer of, $3 million to prevent the lawful seizure of the funds. Evidence obtained in the investigation revealed that the attorney directed and aided and abetted the transfer of $3 million for his clients following the execution of federal search and seizure warrants in California. The attorney directed the transfer from an account in the Bahamas to his trust account, thereafter, combining the funds for his personal use.[362]

Although state bar association rules govern IOLTAs, the rules are generally meant to protect clients and impose obligations on lawyers not to misuse the funds in the IOLTA. Notwithstanding these rules of professional conduct, some attorneys have abused IOLTAs to defraud their clients. For example, in March 2025, an attorney was sentenced to more than five years in federal prison for money laundering and wire fraud. According to the guilty plea, the defendant served as an attorney licensed to practice law in New York, Pennsylvania, and New Jersey, and was a named partner at a law firm. Over several years, the defendant led clients to believe that they had immediate access to the money in two law firm IOLTA accounts, but the attorney was directing employees to transfer the clients' money into other accounts that he controlled. The scheme caused more than $2.4 million in losses to the law firm's clients. The attorney used the stolen funds to pay for personal expenses.[363]

360 ABA, "Formal Opinion 513: Duty to Inquire Into and Assess the Facts and Circumstances of Each Representation," (August 23, 2024), p. 7, https://www.americanbar.org/content/dam/aba/administrative/professional_responsibility/ethics-opinions/aba-formal-opinion-513.pdf. Emphasis in original.

361 See ABA, "IOLTA Overview," (accessed December 17, 2025) https://www.americanbar.org/groups/interest_lawyers_trust_accounts/overview/.

362 DOJ, "Hilton Head Lawyer Sentenced for Knowingly Transferring $3M to Prevent the Lawful Seizure of the Funds," (February 21, 2025) https://www.justice.gov/usao-sc/pr/hilton-head-lawyer-sentenced-knowingly-transferring-3m-prevent-lawful-seizure-funds.

363 DOJ, "California Lawyer Sentenced to More Than Five Years in Federal Prison for Wire Fraud and Money Laundering," (March 7, 2025) https://www.justice.gov/usao-md/pr/california-lawyer-sentenced-more-five-years-federal-prison-wire-fraud-and-money.

Accountants

U.S. accountants present a low level of money laundering risk because, unlike in other jurisdictions, they generally provide financial record keeping or advice services rather than managing or holding client funds, purchasing real estate, or establishing companies or trusts.[364] Although accountants could facilitate illicit financial schemes due to their knowledge of the financial system, accountants do not retain any special ability to register companies, open bank accounts, or authorize financial transactions not available to ordinary citizens. In the past ten years, accountants have rarely been implicated in cases in which they used their professional skills to provide third-party money laundering services. When accountants are charged with money laundering, it is most often in conjunction with fraud or embezzlement perpetrated against a client or the government.[365]

Third-Party Payment Processors

Payment processors, also known as third-party payment processors, serve as intermediaries in non-cash transactions—such as credit and debit card, ACH, and mobile wallet transactions—enabling merchants to accept payments from customers online and in person without needing their own merchant account with a bank. Payment processors are customers of banks. They operate between merchants and financial institutions and facilitate the transmission of transaction data, authorization, and settlement, and often provide additional services such as fraud detection and chargeback management, encryption and security, and data analytics. Given the rise in smaller e-commerce merchants, especially since the COVID-19 pandemic; the growth in credit card, debit card, and digital wallet transactions; and the emergence of new payment schemes such as "buy now, pay later," the payment processor market has been growing and is expected to continue to grow rapidly over the next several years.[366]

Under the BSA and FinCEN's implementing regulations, payment processors may be exempt from meeting the MSB definition if they meet certain criteria.[367] In a 2013 FinCEN administrative ruling describing the regulatory exemptions from the definition of a MSB (i.e., not a money transmitter), a payment processor can avail itself of the "payment processor exemption" and not be subject to the BSA where: (a) the entity must facilitate the purchase of goods or services, or the payment of bills for goods or services (not money transmission itself); (b) the entity operates through clearing and settlement systems that admit only BSA-regulated financial institutions; (c) the entity provides payment services pursuant to a formal agreement; and (d) the entity has a contract at minimum with the merchant or creditor receiving the funds.[368] An entity that satisfies all four conditions is not treated as a money transmitter under BSA rules and thus is generally not required to register as an MSB or implement a full AML/CFT program. This regulatory carve-out recognizes that such processors operate within the banking system's oversight;

364 See FATF, "Accounting Profession: Guidance for a Risk-based Approach," (June 2019), p. 11, https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/RBA-Accounting-Profession.pdf.coredownload.pdf.

365 *See, e.g.*, DOJ, "California Certified Public Accountant Indicted for Filing False Tax Returns and Mail Fraud Scheme," (July 24, 2025) https://www.justice.gov/opa/pr/california-certified-public-accountant-indicted-filing-false-tax-returns-and-mail-fraud; DOJ, "Two Businessmen, a Certified Public Accountant, and Four Puerto Rico-Based Businesses Indicted on Charges of Fraud, Bribery, and Money Laundering" (April 3, 2025) https://www.justice.gov/usao-pr/pr/two-businessmen-certified-public-accountant-and-four-puerto-rico-based-businesses.

366 See FRB Financial Services, "Federal Reserve Payments Insights Brief: Consumer Payments Study," (2024) https://fedpaymentsimprovement.org/wp-content/uploads/2024-consumer-payments-study.pdf.

367 31 C.F.R. 1010.100(ff)(5)(ii)(B).

368 FinCEN, "FIN-2013-R002: Whether a Company that Offers a Payment Mechanism Based on Payable-Through Drafts to its Commercial Customers is a Money Transmitter," (November 13, 2013), p. 3, https://www.fincen.gov/system/files/administrative_ruling/FIN-2013-R002.pdf. *See also*, FinCEN, "Application of Money Services Business Regulations to a Company Acting as an Independent Sales Organization and Payment Processor," (August 27, 2024), p. 2, https://www.fincen.gov/system/files/administrative_ruling/FIN-2014-R009.pdf.

however, it may also create a vulnerability in the AML/CFT regime.[369]

Payment processors serve a gatekeeping role for the funds they process into the financial system because merchants are presumed to have met the strict requirements set by card networks and any additional due diligence requirements set by acquiring banks. Because many payment processors fall outside direct BSA regulation, they can be an attractive avenue for illicit finance. This can increase risk for banks that provide accounts for payment processors because they do not have direct relationships with the merchants and therefore rely on the processor to conduct due diligence and verify the merchant's identity and business practices.[370] Payment processors outside the scope of the BSA have no legal obligation to conduct customer due diligence or file SARs; as a result, some payment processors may lack robust controls to vet the merchants or transactions they handle. Higher-risk merchants that cannot easily obtain direct bank merchant accounts may turn to third-party processors, and fraudulent merchants may use third-party processors due to perceived lower controls.

One of the ways criminals use payment processors for illicit activity is through "transaction laundering," whereby criminals misrepresent themselves as legitimate merchants in order to process illegal transactions through the payment system. In a typical transaction laundering scheme, illicit payments (e.g., payments for counterfeit goods, illegal drugs, gambling, etc.) are disguised as ordinary sales by routing them through a seemingly legitimate merchant account. Sometimes fraudulent merchants create shell companies with seemingly legitimate websites to establish their own merchant account at a payment processor; other schemes involve a legitimate merchant with an existing account at a payment processor processing transactions on behalf of a fraudulent merchant. In transaction laundering schemes, it is often the case that both the consumers and merchants are complicit in defrauding the payment processors, card networks, and banks.

In one case, a man was sentenced to 10 years in prison for defrauding internet users through scam virus alerts and distributing controlled substances online. The man and his co-conspirators facilitated online sales from multiple foreign drug suppliers and received controlled substances from abroad before repackaging and distributing them throughout the United States. To conceal the nature of the transactions, the man and his co-conspirators used PayPal and merchant accounts that purported to belong to nonexistent consulting companies, health supplement stores, auto parts suppliers and travel agencies. In some instances, the man and his co-conspirators created fake travel itineraries and receipts to deceive credit card processors in the United States in order to keep the drug business from being detected.[371]

Complicit payment processors can also abuse their positions as gatekeepers and either independently conduct illicit activity or collude with their merchant clients to commit fraud against the consumer, as well as the card network and banks involved. There are numerous permutations of fraudulent schemes involving payment processors, which are often complicated by the number of entities in the payments landscape. As one example, in June 2025, a U.K.-based payment processor agreed to pay $5 million and be permanently banned from processing payments for tech-support telemarketers to settle an FTC action. The FTC action alleged that the payment processor abused the U.S. credit-card system and enabled deceptive foreign operators to access it, costing consumers millions of dollars. The complaint charged that the payment processor opened merchant accounts claiming to be a "merchant of record"

369 Digital asset payment processors do not qualify for the payment processor exemption because they are generally unable to satisfy the second condition since they do not operate, either in whole or in part, through clearing and settlement systems that only admit BSA-regulated financial institutions as members. See FinCEN, "FIN-2019-G001: Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies," (May 9, 2019), pp. 21-23, https://www.fincen.gov/system/files/2019-05/FinCEN%20Guidance%20CVC%20FINAL%20508.pdf.

370 In June 2023, the FRB, FDIC, and OCC issued guidance for supervised banks regarding the risks of third-party relationships, including those with payment processors. The guidance noted that a bank's use of third parties does not diminish its responsibility to meet its regulatory requirements, and that the use of third parties can reduce a bank's direct control over activities and may introduce new risks or increase existing risks. Interagency Guidance on Third-Party Relationships: Risk Management, 88 Fed. Reg. 37920 (June 9, 2023) https://www.occ.gov/news-issuances/federal-register/2023/88fr37920.pdf.

371 DOJ, "Michigan Man Who Orchestrated International Computer Fraud and Online Drug Distribution Schemes Sentenced to Decade in Prison," (June 18, 2024), https://www.justice.gov/usao-ma/pr/michigan-man-who-orchestrated-international-computer-fraud-and-online-drug-distribution.

or software "reseller," then used these accounts to process card payments on behalf of numerous, unrelated third-party merchants, and enabled overseas schemes to access the credit card system and collect payments from U.S. consumers, and to evade detection by merchant banks and card networks.[372]

XIV. High-Value Goods and Property

Criminals purchase high-value goods and property to launder illicit proceeds because the items can easily be resold around the world in high volumes due to their transportability and value retention. These types of goods and property include precious metals, stones, and jewels (PMSJ), watches and other jewelry, handbags and other fine leather goods, designer clothing items, art, automobiles, and electronics, among others. Although BSA obligations apply to PMSJ dealers as described below, most other merchants dealing in high-value goods and property are only required to file a Form 8300 when they receive more than $10,000 in cash in a single transaction or in related transactions.[373] Many criminals purchase high-value goods and property for their own personal enjoyment, but professional money launderers, including CMLNs, also use these items to facilitate cross-border money laundering operations. Criminals have also targeted the real estate sector to launder illicit proceeds, particularly through all-cash purchases made by legal entities. Treasury's finalized real estate rule that imposes reporting and recordkeeping requirements on a narrow category of higher-risk transfers of residential real estate will allow law enforcement to more easily investigate these transfers.

Precious Metals, Stones, and Jewels (PMSJ)

The PMSJ sector has a high inherent risk for money laundering and other illicit activities, due to the value and fungibility of these goods, the size and structure of the sector, and the often-informal nature of these businesses and transactions. These materials' value density makes them a highly attractive and effective vehicle for criminals seeking to move or transfer large sums, while their opaque and international supply chains result in significant upstream risks related to sanctions and tariff evasion, forced labor and human rights abuse, and transnational organized crime. The sector, which comprises more than 20,000 dealers, has large cashflow that can be misused to conceal illicit activities, and its predominantly small, family-run businesses have varying levels of experience with AML/CFT and customer due diligence practices.[374] The BSA obligations that apply to dealers in precious metals, stones, and jewels (PMSJ dealers)[375] address proven risks by requiring certain PMSJ dealers to establish and maintain risk-based AML/CFT programs and report certain currency transactions that exceed $10,000 using Form 8300.[376] These BSA obligations address inherent risks that are not otherwise mitigated, but the sector remains vulnerable based on its structure and the goods that flow through it.

In the past two years, there have been several types of illicit finance activities—including fraud, money laundering, and theft—associated with the PMSJ sector, its operators, and its customers. These cases frequently involve individuals selling or pawning illicit goods (including stolen jewelry), at times with the business' full knowledge of the goods' illicit nature;[377] individuals laundering illicit proceeds through gold bars or other precious metals;[378]and

372 FTC, "Paddle Will Pay $5 Million to Settle FTC Allegations of Unfair Payment-Processing Practices and Facilitation of Deceptive Tech-Support Schemes," (June16, 2025) https://www.ftc.gov/news-events/news/press-releases/2025/06/paddle-will-pay-5-million-settle-ftc-allegations-unfair-payment-processing-practices-facilitation.

373 IRS, "Form 8300 and reporting cash payments of over $10,000," (updated July 24, 2025) https://www.irs.gov/businesses/small-businesses-self-employed/form-8300-and-reporting-cash-payments-of-over-10000.

374 See RIN 1506-AA58 31 CFR 103 70 FR 33702

375 See 31 CFR 1027.

376 The BSA obligates PMSJ dealers to report transactions exceeding a $10,000, which is lower than the FATF $15,000 cash transaction reporting threshold for PMSJ dealers.

377 *See, e.g.*, DOJ, " Diamond District Fence Pleads Guilty in Connection with Large Scale Stolen Property Operation," (July 18, 2025) https://www.justice.gov/usao-edny/pr/diamond-district-fence-pleads-guilty-connection-large-scale-stolen-property-operation.

378 *See, e.g.*, DOJ, "Two Indian Nationals Charged in Elder Fraud Gold Bar Courier Scam," (February 23, 2024) https://www.justice.gov/usao-ndoh/pr/two-indian-nationals-charged-elder-fraud-gold-bar-courier-scam.

business owners or employees defrauding their customers or suppliers,[379] or stealing from their own businesses.[380] In one notable case, the owner of a precious metals depository was sentenced to the statutory maximum of 65 years in prison following his conviction on mail fraud, wire fraud, and income tax evasion charges. Evidence presented at trial and in sentencing proceedings revealed that the man stole at least $76 million from his customers and that over 1,000 customer accounts were missing precious metals. Industry sources have characterized the fraudulent scheme as the largest theft from a precious metals depository in U.S. history.[381]

As mentioned in the Illicit Trade section, illicit actors also exploit the PMSJ sector to violate or evade U.S. sanctions, tariffs, or other import duties. These risks are exacerbated by the opacity of the supply chains for these goods. One typology involves jewelry importers deliberately mislabeling or transshipping goods to bypass import, financial, or trade restrictions. Another notable risk typology involves the misuse of jewelry businesses as fronts to conduct illegal financial transactions for customers, including converting cash to checks or wire transfers in exchange for substantial fees without registering as money transmitting businesses with FinCEN or other authorities. One case exemplifies both typologies. In January 2025, an India- and New Jersey-based man who operated jewelry companies in New York City's Diamond District was sentenced to 30 months' incarceration for spearheading a scheme to illegally evade customs duties for more than $13.5 million of jewelry imports into the United States and for illegally processing more than $10.3 million through an unlicensed money transmitting business.[382] Law enforcement has also reported similar illicit trade schemes in connection with the import of diamonds from Russia, Wagner Group-linked mining companies in Africa, and other human rights-abusing diamond mines, in violation of U.S. import bans and/or financial sanctions.[383]

Art

The high-value art market presents a low residual money laundering risk to the U.S. financial system. While the market's inherent structure and vulnerabilities create a moderate money laundering risk environment, such as by presenting opportunities for fraudsters to generate and launder illicit proceeds, and for sanctioned actors to evade restrictions, this activity remains limited. Several qualities inherent to high-value art, the high-value art market, and market participants may make the market attractive to illicit actors for laundering illicit proceeds or evading sanctions. Specifically, the high-dollar values of single transactions, market price volatility and subjectivity, art transportability, the long-standing culture of privacy in the market, the prevalence of private sales and transactions, and the increasing use of art as an investment or financial asset all contribute to the money laundering vulnerabilities of art.[384] But the high-value art market's size and dynamics present several mitigating factors that lower its money laundering risk profile

A recent FATF typologies report on complex sanctions evasion schemes demonstrated that a common tactic of sanctions evaders is to enlist third-party intermediaries and shell companies to obscure a sanctioned person's involvement in an otherwise prohibited transaction.[385] The art market is inherently vulnerable to such complex

379 *See, e.g.*, New York County District Attorney, "D.A. Bragg Announces Guilty Plea In Diamond Swap," (February 28, 2025) https://manhattanda.org/d-a-bragg-announces-guilty-plea-in-diamond-swap/.

380 *See, e.g.*, DOJ, " Supervisor of Luxury Jewelry Company Sentenced for Stealing, Selling Millions of Dollars Worth of Precious Metals," (December 4, 2024) https://www.justice.gov/usao-ma/pr/supervisor-luxury-jewelry-company-sentenced-stealing-selling-millions-dollars-worth.

381 DOJ, "Precious Metals Depository Owner Sentenced to 65 Years in Federal Prison for $76 Million Fraud Scheme," (June 20, 2025) https://www.justice.gov/usao-de/pr/precious-metals-depository-owner-sentenced-65-years-federal-prison-76-million-fraud.

382 DOJ, "India- And New Jersey-Based Jeweler Sentenced To 30 Months Incarceration For Multimillion Dollar International Trade Fraud Scheme And Unlicensed Money Transmitting," (January 23, 2025) https://www.justice.gov/usao-nj/pr/india-and-new-jersey-based-jeweler-sentenced-30-months-incarceration-multimillion-dollar.

383 *See, e.g.*, Treasury, "Treasury Sanctions Wagner Group-linked Companies in the Central African Republic," (May 30, 2024) https://home.treasury.gov/news/press-releases/jy2384.

384 Treasury, "Study of the Facilitation of Money Laundering and Terror Finance Through the Trade in Works of Art" (February 2022) https://home.treasury.gov/system/files/136/Treasury_Study_WoA.pdf.

385 FATF, "Complex Proliferation Financing and Sanctions Evasion Schemes," (June 2025) https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Complex-PF-Sanctions-Evasions-Schemes.pdf.coredownload.inline.pdf.

sanctions evasion schemes because the use of intermediaries, such as advisors or consultants, and shell companies are commonly accepted business practices in the high-value art market, even for legitimate transactions dominated by high-net-worth individuals seeking to keep their dealings shielded from scrutiny for legitimate purposes.

In one case, a woman acting as an intermediary was charged with one count of conspiracy to violate the International Emergency Economic Powers Act (IEEPA, one count of violating the IEEPA, and one count of conspiracy to commit international money laundering. As alleged in the indictment, from at least in or around February 2023 through the present, the woman and others allegedly participated in a scheme to violate IEEPA by purchasing art and antiques for the benefit of sanctioned oligarch from galleries and auction houses in the United States and Europe, and having the items shipped to her residence in Huntly, Virginia, where they were stored for onward shipment to Russia. In return, the woman was reimbursed and received a service fee. The indictment alleges that the woman also engaged in a scheme to commit money laundering, knowing the transactions were intended to conceal the proceeds of IEEPA violations.[386]

While the high-value art market has some qualities that make it vulnerable to abuse by illicit actors, there are several mitigating factors that reduce the residual risk in the sector. First, the relatively small size of the art market when compared to other sectors is not large enough for the most important threat actors to generate or launder significant volumes of illicit proceeds. Second, art market participants have economic incentives to conduct enhanced counterparty and source of funds verifications, such as the reputational risk in an insular, trust-based market or the credit risk of non-payment. Third, art market transactions can take a significant amount of time due to the nature of sourcing, conducting due diligence, and closing procedures. This can make the market an inhospitable environment for criminals seeking to quickly launder large amounts of illicit proceeds.[387]

Luxury Goods and Electronics

Several cases during the assessment period demonstrate how professional money launderers, including CMLNs, continue to purchase luxury goods and electronics to launder illicit proceeds, as was highlighted in the 2024 NMLRA.[388] As with other professional money laundering methods, the source of illicit proceeds can come from different predicate crimes, including drug trafficking, several types of fraud schemes, and cybercrime. Money launderers generally use the illicit proceeds to purchase the goods at retailers (in person or online), consolidate the goods in warehouses, and export the goods to foreign jurisdictions for resale.

In one case, two men were arrested and charged with running a company that exported hundreds of millions of dollars' worth of consumer electronics and gift cards, nearly all derived from criminal activities such as identity theft, credit card theft, and fraud. According to an affidavit filed with the complaint, the men owned and operated a company that used warehouses to aggregate electronics before shipping them out of the United States. Since 2019, the company has exported more than $611 million in electronics from the United States, nearly all of which law enforcement believes to be crime proceeds. The men procured electronics and gift cards from many illicit sources. They also acquired electronics directly themselves through fraud. They bought electronics from Best Buy, The Home Depot, and other retailers using gift cards loaded with fraud proceeds—primarily via stolen credit cards. Those

386 DOJ, "TV Presenter Who Worked for Channel One Russia Charged with Violating U.S. Sanctions Imposed on Russia," (September 5, 2024) https://www.justice.gov/archives/opa/pr/tv-presenter-who-worked-channel-one-russia-charged-violating-us-sanctions-imposed-russia.

387 See Treasury, "Study of the Facilitation of Money Laundering and Terror Finance Through the Trade in Works of Art" (February 2022) https://home.treasury.gov/system/files/136/Treasury_Study_WoA.pdf; FATF, "Money Laundering and Terrorist Financing in the Art and Antiquities Market," (February 2023) https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Money-Laundering-Terrorist-Financing-Art-Antiquities-Market.pdf.coredownload.pdf.

388 *See, e.g.*, DOJ, "Chinese Nationals Sentenced to Federal Prison for Participating in a Fraudulent Gift Card Conspiracy Involving the Purchase and Export of Apple Products to China," (April 22, 2025) https://www.justice.gov/usao-nh/pr/chinese-nationals-sentenced-federal-prison-participating-fraudulent-gift-card-conspiracy; DOJ, "Three Members of an International Money Laundering Organization Charged with Laundering Millions of Dollars in Drug Proceeds," (April 24, 2025) https://www.justice.gov/opa/pr/three-members-international-money-laundering-organization-charged-laundering-millions.

electronics were often shipped directly to the company warehouse or to mailboxes that the men controlled.[389]

As described in FinCEN's August 2025 CMLN Financial Trend Analysis, U.S.-based CMLNs likely recruit witting and unwitting individuals, particularly Chinese national students, in the United States to purchase high-value electronics and luxury goods for export to China and other regions, as part of money laundering schemes. The recruited individuals believe they are working as *daigou* buyers, an informal arrangement where buyers, mainly using messaging platforms popular in China, connect China-based consumers with products from abroad. This can include purchasing items from retailers in store or online using credit cards and obtaining funds from CMLNs via cash, P2P, or ACH to make payments towards account balances.[390]

Real Estate

Most transfers of residential real estate are well-regulated because they are associated with a mortgage loan or other financing provided by covered financial institutions subject to comprehensive AML/CFT program requirements. Non-financed (or "all-cash") transfers of residential real estate, which account for 20 to 30 percent of the market, do not involve such financial institutions and can be exploited to launder illicit proceeds. Treasury has long recognized the illicit finance risks posed by criminals and corrupt officials who abuse opaque legal entities and trusts to launder ill-gotten gains through transfers of residential real estate.[391] This illicit use of the residential real estate market threatens U.S. economic and national security and can disadvantage individuals and small businesses that seek to compete fairly in the U.S. economy.

Illicit actors of all varieties, including those that pose domestic threats, such as persons engaged in fraud or organized crime, and foreign threats, such as international drug cartels, human traffickers, and corrupt political or business figures engage in money laundering through real estate. In one case, a woman pleaded guilty to federal charges of conspiracy to possess with intent to distribute methamphetamine and conspiracy to commit money laundering. As part of the criminal operation, the woman and her associates purchased millions of dollars' worth of real estate, vehicles, and luxury goods—all designed to conceal the illicit source of their wealth. The investigation revealed that the woman purchased five separate residences, including a seven-bedroom waterfront home in Jonesboro, Georgia. Three of these residences were purchased with bulk cash brought directly to the transaction.[392]

In other instances, the U.S. residential real estate sector has been a vehicle for former Venezuelan government officials in the Nicolas Maduro regime and numerous sanctioned Russian individuals to hide their ill-gotten gains from corruption. For example, in January 2025, a Miami real estate broker pleaded guilty to engaging in a scheme to violate U.S. sanctions and launder money by conducting transactions involving blocked properties owned by sanctioned Russian oligarchs. As described in court documents, from in or around January 2018 through in or around March 2023, the broker conspired with others to violate IEEPA and commit money laundering by maintaining, transferring, selling, and leasing several luxury condominiums in the Miami area that the oligarchs owned and by collecting, sharing, and using the proceeds to maintain the properties.[393]

389 DOJ, "Two San Fernando Valley Men Arrested on Federal Complaint Alleging They Exported $611 Million of Electronics Obtained by Fraud," (September 16, 2025) https://www.justice.gov/usao-cdca/pr/two-san-fernando-valley-men-arrested-federal-complaint-alleging-they-exported-611.

390 FinCEN, "Chinese Money Laundering Networks: 2020 – 2024 Threat Pattern & Trend Information," (August 2025), pp. 11-12, https://www.fincen.gov/system/files/2025-08/4000-10-INV-144549-S3F6L-FTA-CMLN-508.pdf.

391 Treasury, "2024 National Money Laundering Risk Assessment," February 2024, pp. 75-78, https://home.treasury.gov/system/files/136/2024-National-Money-Laundering-Risk-Assessment.pdf; Treasury, "2022 National Money Laundering Risk Assessment," February 2024, pp. 57-60, https://home.treasury.gov/system/files/136/2022-National-Money-Laundering-Risk-Assessment.pdf

392 DOJ, "Leader of Multi-Million Dollar International Money Laundering and Drug Trafficking Ring Convicted," (June 16, 2025) https://www.justice.gov/usao-ndga/pr/leader-multi-million-dollar-international-money-laundering-and-drug-trafficking-ring.

393 DOJ, "Miami-Based Real Estate Broker Pleads Guilty to Conspiracy to Violate Russia-Ukraine Sanctions and to Commit Money Laundering," (January 16, 2026) https://www.justice.gov/archives/opa/pr/miami-based-real-estate-broker-pleads-guilty-conspiracy-violate-russia-ukraine-sanctions-and; OFAC, " Family International Realty LLC and its Owner Settle with OFAC for $1,076,923 Related to Apparent Violations of Ukraine-/Russia-Related Sanctions," (January 16, 2025) https://ofac.treasury.gov/media/933941/download?inline.

In August 2024, Treasury finalized a rule that would impose reporting and recordkeeping requirements on a narrow category of higher-risk transfers of residential real estate.[394] The final rule focuses on the less than 20 to 30 percent of transfers that are non-financed and that involve certain legal entities and trusts, and includes multiple significant exceptions for common, low-risk transfers. The final rule will address the risks from numerous money laundering typologies involving the purchase of residential real estate, including the use of domestic and foreign legal entities, legal arrangements, and pooled accounts like IOLTAs; the use of nominees and gatekeepers; the use of all-cash payments to avoid the AML/CFT scrutiny that comes with financing; over or under paying for real estate; and the successive transfer of real estate at a higher value . To be reportable, the transfer must be non-financed (i.e., all-cash) and the new owner of the property must be a legal entity or trust. The final rule was developed based on lessons learned from the highly effective residential real estate Geographic Targeting Orders (GTOs) that have been in place since 2016 and now cover over 66 counties in the United States.[395] These GTOs have required similar reporting of non-financed sales of residential real property to legal entities, on a geographically limited basis.

The final rule will be effective on March 1, 2026. For the first time, the United States will have a uniform, nationwide mechanism for the real estate industry to report on pervasive illicit finance risks associated in equal measure to domestic and foreign legal entities and arrangements in the non-financed U.S. residential real estate market.[396] The reports submitted as per the requirements of the finalized rule will make law enforcement investigations into illicit activity and money laundering through residential real estate less costly, less lengthy, and more effective; reduce the social costs associated with this illicit activity, such as artificially inflated homes prices; create a level playing field for small businesses that operate in the real estate market by ensuring there are uniform nationwide reporting and record keeping requirements; and strengthen U.S. national security and help protect the integrity of the U.S. financial system by ensuring that, illicit actors do not benefit financially by utilizing our real estate market to offshore the proceeds of crime.

Commercial Real Estate

Commercial real estate transactions may serve as conduits for illicit funds—including those tied to drug trafficking and other forms of criminal activity. In January 2023, FinCEN issued an alert highlighting that commercial real estate is exposed to money-laundering risk because it commonly utilizes purpose-built legal entities, indirect ownership chains, multiple types of ownership and financing, and various parties involved in each transaction—factors which can obscure beneficial ownership and source of funds.[397] For example, in April 2024 an eight-count indictment was unsealed charging two men for their roles in facilitating the black-market marijuana industry in Oklahoma. The indictment alleges that the two men, a real estate broker and an attorney, conspired to aid and abet marijuana traffickers in Oklahoma by making false and fraudulent representations on applications for state licenses to operate marijuana farms—all on behalf of their black-market marijuana trafficker clients. The real estate broker was also charged with using his brokerage firm and network of property-management and property-investment companies to service the housing and/or real estate needs of black-market marijuana traffickers by brokering land sales for them across Oklahoma, renting them land on which to operate their black-market marijuana grows, and renting them residences which served as marijuana stash houses and personal residences of the owners of black-market grows.[398] More comprehensive research, data collection, and regulatory scrutiny are needed to determine whether these commercial real estate money-laundering risks are widespread, systemic, or concentrated in specific segments.

394 Anti-Money Laundering Regulations for Residential Real Estate Transfers, 31 CFR Chapter X RIN 1506-AB54 https://www.federalregister.gov/documents/2024/08/29/2024-19198/anti-money-laundering-regulations-for-residential-real-estate-transfers.

395 FinCEN, "FinCEN Renews Residential Real Estate Geographic Targeting Orders," (October 9, 2025), https://www.fincen.gov/news/news-releases/fincen-renews-residential-real-estate-geographic-targeting-orders-0.

396 See Real Estate Report, OMB No. 1506-0080 https://www.fincen.gov/system/files/2025-09/RER-Form-508C.pdf.

397 FinCEN, "FinCEN Alert on Potential U.S. Commercial Real Estate Investments by Sanctioned Russian Elites, Oligarchs, and Their Proxies," (January 2023) https://www.fincen.gov/system/files/shared/FinCEN%20Alert%20Real%20Estate%20FINAL%20508_1-25-23%20FINAL%20FINAL.pdf.

398 DOJ, "Metro Attorney and Metro Real Estate Broker Charged in "Ghost Licensing" Scheme to Facilitate Black-Market Marijuana Operations," (April 10, 2024) https://www.justice.gov/usao-wdok/pr/metro-attorney-and-metro-real-estate-broker-charged-ghost-licensing-scheme-facilitate.

CONCLUSION

The top money laundering threats and vulnerabilities have largely remained consistent over the past decade, but the character and manner by which the U.S. financial system is exploited by illicit actors continues to evolve. Technological advancements in finance and communication have amplified the threats posed by all manner of predicate crimes. While all countries must adapt to these changes, the United States in particular has been increasingly targeted by foreign-based actors due to the size and openness of the U.S. economy. The U.S. public and private sectors must continue to evolve to combat the threat posed by illicit finance while protecting and foster legitimate finance without undue burden.

PARTICIPANTS

- **Department of the Treasury**
  - Internal Revenue Service - Criminal Investigation (IRS-CI)
  - Terrorism and Financial Intelligence (TFI)
    - Financial Crimes Enforcement Network (FinCEN)
    - Office of Foreign Assets Control (OFAC)
    - Office of Intelligence and Analysis (OIA)
    - Office of Terrorist Financing and Financial Crimes (TFFC)
- **Department of Justice (DOJ)**
  - Criminal Division
    - Computer Crime and Intellectual Property Section (CCIPS)
    - Fraud Section
    - Money Laundering, Narcotics and Forfeiture Section (MNF)
  - Executive Office for U.S. Attorneys
  - Drug Enforcement Administration (DEA)
  - Federal Bureau of Investigation (FBI)
- **Department of Homeland Security**
  - Customs and Border Protection (CBP)
  - Homeland Security Investigations (HSI)
  - United States Secret Service (USSS)
- **Department of State**
- **U.S. Postal Inspection Service (USPIS)**
- **Staff of the Federal functional regulators**[399]

399 This includes staff of the Commodity Futures Trading Commission (CFTC), the Federal Deposit Insurance Corporation (FDIC), the Board of Governors of the Federal Reserve System (FRB), the National Credit Union Administration (NCUA), the Office of the Comptroller of the Currency (OCC), and the Securities and Exchange Commission (SEC). The SEC staff also sought input from the staff of the Financial Industry Regulatory Authority (FINRA), which regulates broker-dealer members doing business with the public in the United States.

METHODOLOGY

Treasury's Office of Terrorist Financing and Financial Crimes (TFFC), by statute, is the AML/CFT policy coordinator for Treasury and routinely interacts with our domestic partners. This report is based on a review of federal and state public sector analysis, enforcement actions, guidance, and interviews with U.S. Treasury staff, intelligence analysts, law enforcement agents, and prosecutors. During the research and analysis phase, we shared working drafts of different sections with relevant stakeholders for comment and coordinated input and feedback on three separate drafts of this document.

The NMLRA uses all available information to identify the current money laundering environment within the United States. This initiative includes feedback and input from various private sector participants through formal and informal mechanisms and targeted meetings on illicit finance trends. This action is generally done through outreach following the publication of the previously released NMLRA. Relevant components of agencies, bureaus, and offices of the Treasury, the U.S. Department of Justice (DOJ), the U.S. Department of Homeland Security (DHS), and others listed above, participated in the development of the risk assessment. Data collected is current as of January 15, 2026.

We have identified cases that demonstrate some type of money laundering activity or show how criminal actors have used the U.S. financial system to move, disguise, or hide proceeds of crime. Case examples may involve criminal charges in an indictment, which are merely allegations. All defendants are presumed innocent unless, and until, proven guilty beyond a reasonable doubt in a court of law. We have also utilized qualitative data, often provided by law enforcement, when no public sources are available (e.g., press releases or court documentation). When citing qualitative data, the NMLRA makes clear that certain information is "according to law enforcement."

Treasury will conduct extensive outreach to our public and private sectors to deliver the results of this report. In doing so, we hope to receive valuable feedback on the usefulness of this assessment and how we can continue to improve this process.

TERMINOLOGY

The terminology and methodology of the NMLRA are based in part on the guidance of the FATF, the international standard-setting body for AML/CFT safeguards. The following concepts are used in this risk assessment:

Threats: For purposes of the NMLRA, threats are the predicate crimes that are associated with money laundering. The environment in which predicate offenses are committed, and the proceeds of crime are generated, is relevant to understanding why, in some cases, specific crimes are associated with particular money laundering methods.

Vulnerabilities: Vulnerabilities are what facilitate or create the opportunity for money laundering. They may relate to a specific financial sector or product, or a weakness in law, regulation, supervision, or enforcement.

Consequences: Consequences include harms or costs inflicted upon U.S. citizens and the effect on the U.S. economy, which provide further context on the nature of the threats.

Risk: Risk is a function of threat, vulnerability, and consequence. It represents an overall assessment, considering the effect of mitigating measures, including regulation, supervision, and enforcement.

THE DEPARTMENT OF THE TREASURY
1789