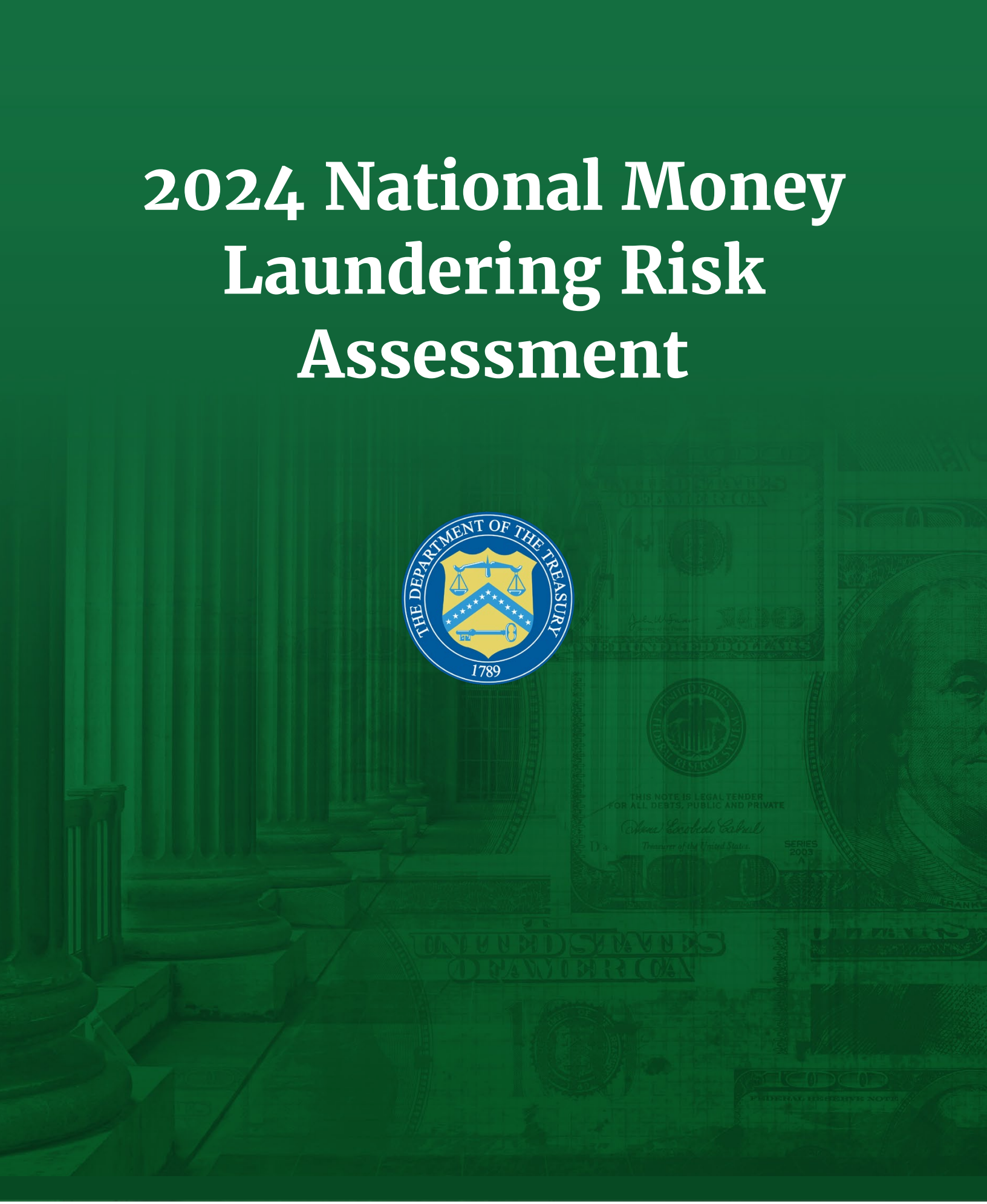
2024 National Money Laundering Risk Assessment



February 2024

Department of the Treasury

National Money Laundering Risk Assessment (NMLRA)

Table of Contents

EXECUTIVE SUMMARY

Money laundering enables criminal activity and is necessary to disguise ill-gotten gains. It facilitates crime, distorts markets, and has a devastating economic and social impact on citizens. It also threatens U.S. national security as money laundering allows drug traffickers, fraudsters, human trafficking organizations, and corrupt officials, to operate and expand their criminal enterprises.

The 2024 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 governmental and private sector actors, strengthen risk mitigation strategies of financial institutions, and enhance policy deliberations by the U.S. government. As this NMLRA discusses, criminals constantly develop and adopt new ways to launder illicit funds. Thus, there is a need to constantly track and address evolving money laundering trends and methodologies.

This risk assessment reflects an evolving understanding of the key money laundering threats, including crimes that generate illicit proceeds and criminal actors involved in the laundering process. The 2024 NMLRA highlights how both old and relatively new schemes and threat actors are adapting to maximize profit from their criminal activities, including those related to check fraud, unlawful campaign finance, tax crime and Russian money laundering. For example, criminals have employed novel means, such as using telemedicine platforms and virtual asset investment scams, to carry out fraud schemes on a larger scale. Further, Russian money laundering organizations use a vast global network of shell companies, bank accounts, and trusts to launder funds or evade sanctions on behalf of others.

This evolution in coverage and understanding extends to long-standing and new money laundering vulnerabilities, to include gaps and weaknesses in regulation and policy. Shell companies and the lack of timely access to beneficial ownership information and, transparency for certain non-financed real estate transactions, are distinct vulnerabilities in the U.S. anti-money laundering/ countering the financing of terrorism (AML/CFT) system. The United States worked expeditiously to close these long-standing gaps. The establishment of a beneficial ownership information registry housed at Treasury's Financial Crimes Enforcement Network (FinCEN) on January 1, 2024 will fundamentally enhance corporate transparency and address the United States' most significant and longstanding gap in its AML/CFT regime. Additionally, FinCEN is drafting regulations to address money laundering vulnerabilities in the residential real estate sector.

Another concerning money laundering vulnerability is the lack of comprehensive AML/CFT regulations for certain financial intermediaries, such as investment advisers, that may not be directly subject to comprehensive AML/CFT regulations or generally examined for AML/CFT compliance. Treasury plans to issue in the first quarter of 2024 an updated NPRM that would propose applying AML/CFT requirements pursuant to the Bank Secrecy Act, including suspicious activity reporting obligations, to certain investment advisers. Additionally, the 2024 NMLRA highlights a number of new financial services that criminals seek to exploit, such as so-called "decentralized finance" (DeFi) and online gaming. Illicit actors, including ransomware cybercriminals, thieves, scammers, and the Democratic People's Republic of Korea (DPRK) cyber actors, are now using DeFi services to transfer and launder their illicit proceeds. In recent years, legal and technological developments have led to substantial growth in online gaming activity in the United States. The anonymity afforded by online gaming and the size and rapid growth of this sector now present unique money laundering risks.

Over the last 50 years the United States has built a robust AML/CFT framework to address illicit finance risk. The United States Department of the Treasury and its interagency partners continue to ensure that the U.S. AML/CFT regime stays ahead of criminals who use existing and emerging techniques to launder the profits of their crimes.

This risk assessment, along with the 2024 National Terrorist Financing and Proliferation Financing Risk Assessments, serves as a prologue to the 2024 National Strategy to Combat Terrorist and Other Illicit Financing (2024 Strategy). The 2024 Strategy provides a detailed roadmap of the actions that the United States should take to further strengthen its AML/CFT regime and address both novel and lingering illicit finance vulnerabilities.

INTRODUCTION

This report identifies the most significant money laundering threats, vulnerabilities, and risks the United States faces. With a gross domestic product (GDP) of 25 trillion dollars, the United States is the world's largest economy and is particularly susceptible to the laundering of illicit proceeds. This risk is also due to the value, stability, and the centrality of the U.S. dollar in the global economy's payment infrastructure.

Like 2022, this year's risk assessment identifies the most significant money laundering crimes in the United States are linked to fraud, drug trafficking, cybercrime, human trafficking, human smuggling, and corruption. In addition, this report includes a "special focus" on risks that were not identified or fully addressed in previous risk assessments.

Fraud remains the largest and most significant proceed-generating crime for which funds are laundered in or through the United States. Criminals make billions of dollars annually by deceiving U.S. government programs, private companies, and individuals into sending funds via a variety of methods where those funds are ultimately unaccounted for, diverted, or stolen.[1] Investment fraud and healthcare fraud remain the most prevalent proceeds-generating crimes.

The gravity of the illicit drug problem, particularly the use of fentanyl, represents a crisis for U.S. public health and national security. Proceeds from illicit drug sales remain one of the main proceed-generating offenses. Mexican drug trafficking organizations (DTOs), particularly the Sinaloa Cartel and the Cartel Jalisco Nueva Generación (CJNG), remain the most predominant and sophisticated DTOs active in the United States, with consolidated control over drug corridors from Mexico and are heavily involved in the trafficking of fentanyl, methamphetamine, cocaine, heroin, and marijuana.

Corrupt officials, both foreign and domestic, steal U.S. and foreign public funds and misappropriate wealth from U.S. citizens and others. They generate illicit proceeds in the form of bribes, kickbacks, and embezzled assets and launder them in the United States.

With respect to cybercrime, ransomware actors have increased the potency of their attacks over the last few years and have exerted greater pressure on victims to extract payments. Further, cybercrime groups linked to or receiving safe haven from Russia and the Democratic People's Republic of Korea (DPRK) have been responsible for an overwhelming share of recently identified ransomware-related incidents and openly attacked U.S. organizations.

The prevalence of professional money laundering—by individuals, organizations, and networks that launder for a fee or commission—continues to grow as a threat to the U.S. financial system. Chinese Money Laundering Organizations (CMLOs) are now one of the key actors in professionally laundering money within the United States and around the globe. Money mules are also a constant feature in the movement of fraud or other illicitly earned proceeds.

While the United States has many legal, supervisory, and enforcement mitigation measures in place to prevent, detect and stop money laundering, criminals seek to identify and exploit gaps these measures.

1 The potential loss from fraudulent scams and cyberattacks reported to the FBI in 2022 equaled $10.3 billion, which is assumed to underrepresent actual loss based upon the voluntary nature of reporting to the FBI Internet Crime Center (IC3). See Federal Bureau of Investigation (FBI), "2022 Internet Crime Report," FBI Internet Crime Complaint Center, https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3Report.pdf. See Figure 12.

Some regulated financial institutions remain a money laundering vulnerability despite many having adequate AML/CFT programs. Analysis of these vulnerabilities, including occasional AML/CFT compliance deficiencies, is a key feature of this report.

Criminals and transnational criminal organizations (TCOs) continue to use cash to launder illicit proceeds because it provides anonymity, stability, and is widely accepted. While bulk cash smuggling and the use of cash-intensive businesses are historically favored laundering methods for many DTOs, criminals have expanded the way they transport currency, including using new cities as cash consolidation points to convert bills more expeditiously. They also charter private aircraft to smuggle cash via less monitored routes.

While the use of virtual assets for money laundering remains far below that of fiat currency, this assessment provides a comprehensive update on existing and evolving trends in AML/CFT risks associated with virtual assets, including inconsistent compliance with domestic laws and international AML/CFT obligations, obfuscation tools and methods, mixing, disintermediation, and other aspects of purported decentralized finance (DeFi).

This Report was prepared pursuant to Sections 261 and Section 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 2024 NMLRA primarily relies on open-source reporting from the Department of Justice (DOJ), the use of publicly available court documentation[2], and consultations with law enforcement agencies (LEAs).[3] The NMLRA also utilizes 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. (See Annex on Methodology for further information.)

2 The charges contained in an indictment are merely allegations. All defendants are presumed innocent until proven guilty beyond a reasonable doubt in a court of law. Case examples will cite names of those only found guilty.

3 Information from LEAs will be cited as "according to law enforcement sources."

SECTION I. THREATS

In the context of the NMLRA, money laundering threats[4] are the predicate crimes that generate illicit proceeds for laundering in, from, or through the United States. Money laundering threats also represent criminal actors such as those engaged in professional money laundering (PML), and TCOs, including DTOs.[5] Where reliable data exists, this section also discusses the proceeds of crimes generated abroad (*e.g.,* corruption) that are laundered through or in the United States. The findings related to money laundering threats within this risk assessment align with the 2021 AML/CFT National Priorities issued by the FinCEN.[6]

This report identifies the top money laundering threats as fraud; drug trafficking; cybercrime; corruption; human trafficking; human smuggling; and professional money laundering. This report also includes special focus sections on the increased risk identified during the reporting period for check fraud; tax crime; unlawful campaign finance; and Russian money laundering. The report also highlights a range of relatively novel schemes. including call center fraud; virtual currency investment scams (more commonly known as pig-butchering scams);[7] prescription drug diversion; and schemes involving electronic goods. The report also provides an update on wildlife trafficking and other nature crimes.

Fraud

Fraud,[8] both in the private sector and in government benefits and payments, continues to be the largest driver of money laundering activity in terms of the scope of activity and volume of illicit proceeds, generating billions of dollars annually. Fraud is a broad criminal activity that can be categorized in a variety of ways: (1) by entity exploited (*e.g.,* financial institution, government programs, or insurance companies); (2) by victim (*e.g.,* elders, investors, or taxpayers); or (3) by how it is perpetrated (*e.g.,* identity theft/fraud, business email compromise (BEC), account takeover, check fraud, loan fraud, wire fraud, credit/debit card fraud, securities fraud, or cyber-enabled fraud).[9] There can be significant overlap in these classifications and with other money laundering typologies such as the use of professional money laundering organizations and money mules, which are addressed later in this report.

Investment scams and healthcare fraud continue to represent the highest proceeds-generating offenses. This year's report also highlights check fraud, which has seen a major rise in the last few years, as well as new types of fraud involving the use of technology, such as telemedicine and virtual asset investment scams.

Fraud groups are often well-organized, sophisticated, and can be cyber-enabled. They can use social media, darknet forums, and encrypted messaging apps for communication, coordination, sales, and recruitment of new criminal actors. The Fraud Section is designed not to focus on the predicate offense

4 See ANNEX on METHODOLOGY.

5 TCOs, to include DTOs, are identified as AML/CFT National Priorities.

6 FinCEN, "Anti-Money Laundering and Countering the Financing of Terrorism National Priorities", (June 30, 2021), https://www.fincen.gov/sites/default/files/shared/AML_CFT%20Priorities%20(June%2030%2C%202021).pdf.

7 FinCEN Alert, FIN-2023-Alert005, September 8, 2023

8 Fraud is identified as an AML/CFT National Priority.

9 The 2024 NMLRA has used recent work by the Financial Action Task Force to help classify cyber-enabled fraud. See: FATF, "Illicit financial flows from Cyber-enabled Fraud", (November 9, 2023), https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Illicit-financial-flows-cyber-enabled-fraud.pdf.coredownload.inline.pdf.

but to highlight how fraudsters target U.S. citizens and companies and abuse the U.S. financial sector to launder illicit proceeds.

1. Investment Fraud

For the first time, investment schemes represented the highest aggregate reported dollar loss to victims, replacing BEC as the costliest scheme reported to the Federal Bureau of Investigation's (FBI's) Internet Crime Complaint Center (IC3). Based on an analysis by IC3, cyber-enabled investment fraud cost U.S. citizens a staggering $3.3 billion in 2022 alone, representing a 127 percent surge from the previous year.[10] For 2022, the number of investment fraud complaints received ranked 6th when compared to other crime types; however, investment fraud complaints represented the highest reported dollar loss by crime type. Investment fraud complaints replaced BEC complaints as the highest aggregate reported dollar loss. BEC had been the highest aggregate dollar loss since at least 2014.

Investment fraud refers to schemes where criminals provide false information so that the victim will invest or transfer control of assets to the perpetrator.[11] This illicit activity includes types of securities fraud. Once the perpetrator has control of the assets in investment fraud schemes, they divert funds out of the investment vehicle. For the first time, investment schemes reported the highest financial loss to victims, as measured by aggregate dollar value.[12] An estimated 10 percent of investors will become victims of an investment fraud scheme at some point.[13]

Although the increase in investment fraud is often attributed to the recent growth in the number of retail traders and price appreciation for securities and virtual assets from 2020 through 2022, the number of reported schemes and average dollar amount lost per victim have both been increasing since at least 2018.[14] Social media influencers have contributed to and have facilitated investment fraud by using their large audiences and fans' rapport to solicit funds for investment fraud schemes.[15] One case involved the unregistered offer and sale of crypto asset securities, the fraudulent manipulation of the secondary market, and the orchestration of a scheme to pay celebrities to tout crypto asset securities without disclosing their compensation.[16] More traditional types of investment fraud, including through real estate, have remained stable over the years. In contrast, investment fraud involving virtual assets has rapidly increased in both the number of victims and losses, rising 183 percent between 2021 and 2022.[3]

Just as certain professions lend themselves to being used to facilitate certain types of schemes, each scheme type targets a certain demographic, based on investment fraud typology from the FBI and

10 FBI, "Internet Crime Complaint Center Releases 2022 Statistics", (March 22, 2023), https://www.fbi.gov/contact-us/field-offices/springfield/news/internet-crime-complaint-center-releases-2022-statistics.

11 FBI, "Securities Fraud Awareness & Prevention Tips", https://www.fbi.gov/stats-services/publications/securities-fraud.

12 FBI, "Internet Crime Report 2022" (March 2023), https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3Report.pdf.

13 Pension Research Council, "Understanding and Combating Investment Fraud", (2016), https://pensionresearchcouncil.wharton.upenn.edu/wp-content/uploads/2017/02/WP2016-19-Kieffer-and-Mottola.pdf.

14 FBI, "Internet Crime Report 2020", (March 2021), https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf.

15 SEC, "Investor Alerts and Bulletins Social Media and Investment Fraud – Investor Alert," (August 29, 2022), https://www.sec.gov/oiea/investor-alerts-and-bulletins/social-media-and-investment-fraud-investor-alert.

16 SEC, "SEC Charges Crypto Entrepreneur Justin Sun and his Companies for Fraud and Other Securities Law Violations", (March 22, 2023), https://www.sec.gov/news/press-release/2023-59.

Securities and Exchange Commission (SEC).[17] For example, high-yield investment schemes primarily target elderly victims, age 65 or older, due to the victims' larger investable assets and increased reliance on investment income.[18] Criminals also often target religious or ethnic communities, leveraging the built-in trust found in these communities.[19]

Once the criminal has identified a target or vulnerable population, initial contact typically involves advertising potentially high rates of returns with minimal risk via an investment vehicle or strategy that investors can only access through the criminal.[20] Once the funds have been transferred into the investment vehicle controlled by the criminal, the criminals misappropriate the funds by transferring them to personal or otherwise undisclosed bank accounts. After they divert the funds out of the investment vehicle, the criminal typically uses them for purposes other than what they represented to the investor, such as for personal uses or luxury purchases.[21]

a) Ponzi Schemes

A Ponzi scheme is an investment fraud that pays existing investors with funds collected from new investors. Ponzi scheme organizers often promise to invest your money and generate high returns with little or no risk. But in many Ponzi schemes, the fraudsters do not invest the money. Instead, they use it to pay those who invested earlier and may keep some for themselves. With little or no legitimate earnings, Ponzi schemes require a constant flow of new money to survive. When it becomes hard to recruit new investors, or when large numbers of existing investors cash out, these schemes tend to collapse. Ponzi schemes are named after Charles Ponzi, who duped investors in the 1920s with a postage stamp speculation scheme.[22]

If not identified early, losses to investors can expand exponentially as more individuals contribute money to the pool of funds under the perpetrator's control.[23] Ponzi schemes are not immediately apparent to victims, allowing the schemes to operate for months or even years. Like most types of frauds, Ponzi schemes have different variations and may exploit different types of investment, such as foreign exchange trading. In one such scheme, a fraudster persuaded at least 700 victims to invest through promissory notes and other means, causing victim losses exceeding $80 million.[24] Investigators are now seeing the use of DeFi technology involving smart contracts to carry out traditional Ponzi and pyramid schemes. Criminals will develop and deploy smart contracts that employ Ponzi-pyramid techniques.

17 FBI's typology refers to the breakdown and subdivision of investment fraud as reported in "Internet Crime Report 2022". SEC's typology refers to that provided on Investors.Gov.

18 SEC, "High Yield Investment Programs", (March 2023), https://www.investor.gov/protect-your-investments/fraud/types-fraud/high-yield-investment-programs.

19 SEC, "Affinity Frauds", (June 2014), https://www.sec.gov/files/ia_affinityfraud.pdf.

20 DOJ, "Dearborn Resident Sentenced in Investment Fraud Scheme", (May 4, 2022), https://www.justice.gov/usao-edmi/pr/dearborn-resident-sentenced-investment-fraud-scheme#:~:text=DETROIT%20%2D%20Dearborn%20resident%20Ali%20Rameh,Ison..

21 Investment frauds differ greatly by scheme used. Based on analysis of DOJ cases, the most common narrative is what has been reflected and discussed.

22 SEC, Types of Fraud, "Ponzi Scheme," https://www.investor.gov/protect-your-investments/fraud/types-fraud/ponzi-scheme.

23 DOJ, "DC Solar Owner Sentenced to Over 11 Years in Prison for Billion Dollar Ponzi Scheme" (June 28, 2022), https://www.justice.gov/usao-edca/pr/dc-solar-owner-sentenced-over-11-years-prison-billion-dollar-ponzi-scheme#:~:text=—%20U.S.%20District%20Judge%20John%20A,Talbert%20announced.

24 DOJ, "Jury Finds Sarasota Man Guilty Of Running $80 Million "Oasis" Forex Ponzi Scheme", (May 5, 2022), https://www.justice.gov/usao-mdfl/pr/jury-finds-sarasota-man-guilty-running-80-million-oasis-forex-ponzi-scheme.

As soon as an investor places virtual assets into a smart contract, the smart contract automatically diverts the investor's funds to other investors, such that earlier investors are paid with funds from later investors.[25]

b) Virtual Asset Investment Schemes

Virtual asset investment schemes (VAIS) include a variety of traditional fraud fact patterns based on misrepresentations concerning potential investment opportunities in virtual assets. Recently, U.S. law enforcement is seeing a growing number of instances of fraud that are initiated when fraudsters contact victims on social media, dating platforms, or text messages purportedly sent to the wrong number. Scammers often portray outreach as an "innocent" connection when it is a scripted, calculated attempt designed to build rapport and gain trust with the victim. Eventually, these conversations lead to discussions of investment opportunities, wherein victims are lured into investing virtual assets using fake websites or applications that allow the scammers to manufacture fraudulent data about the investment. The deception becomes apparent when victims attempt to cash out their investments, or when the fraudster terminates communication with the victim. Unlike schemes involving wire transfers, where some restoration of financial losses may occur if it is quickly reported, victims of VAIS are less likely to recover their virtual asset losses because of the ability to rapidly transfer virtual assets across borders, potential challenges in identifying virtual asset service providers (VASPs) involved in transfers and relevant points of contact, and the fact that virtual asset transfers are typically irreversible.[26]

Losses from VAIS accounted for nearly 75 percent of all internet-enabled investment fraud in 2022.[27] VAIS often target a younger demographic, with victims having a median age of between 30 and 49. Common schemes of this type include pig butchering (see snapshot below) and some Ponzi scheme variations (see above). While many of the methods used by these scammers are similar to those used by traditional fraudsters, they often take advantage of the publicity around virtual assets to victimize investors.

Pig Butchering

Pig butchering scams are investment scams involving virtual currency fraud. In "pig butchering" schemes, the perpetrator develops an online relationship, sometimes romantic, with the victim. The perpetrator entices the victim to "fatten" an account by transferring virtual assets into a virtual asset wallet, usually on a fake virtual asset platform controlled by the perpetrator. Then, metaphorically, "butcher" the victim or their accounts by taking the victim's funds.[28]

After gaining their victim's trust – sometimes as soon as over a few days or as long as a few months – scammers eventually introduce the idea of investing in virtual assets. The scammers then direct victims

25 DOJ, "Forsage Founders Indicted in $340M DeFi Crypto Scheme", (February 22, 2023), https://www.justice.gov/opa/pr/forsage-founders-indicted-340m-defi-crypto-scheme#:~:text=A percent20federal percent20grand percent20jury percent20in, percent24340 percent20million percent20from percent20victim percent2Dinvestors.

26 FBI, "Consumers Intending to Invest with Cryptocurrency: Be Aware, Be Cautious and Be Educated", (March 9, 2023), https://www.fbi.gov/contact-us/field-offices/richmond/news/consumers-intending-to-invest-with-cryptocurrency-be-aware-be-cautious-and-be-educated.

27 The VA amount for 2022 ($2.57 billion) was divided by the total for investment fraud claims for 2022 ($3.31 billion) to get 77.6 percent, see FBI, "2022 IC3 Report," p.12. https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3Report.pdf.

28 DOJ, "Middlesex County Man Charged with Laundering $2.1 Million Obtained from Internet-Related Frauds", (October 11, 2022), https://www.justice.gov/usao-nj/pr/middlesex-county-man-charged-laundering-21-million-obtained-internet-related-frauds#:~:text=Okuonghae percent20laundered percent20at percent20least percent20 percent242.1,the percent20transfer percent2C percent20whichever percent20is percent20greater.

to fake virtual asset investment platforms, controlled by the scammer or co-conspirators posing as investment advisers or customer service representatives. Once victims make an initial "investment," the fake platforms are manipulated to show substantial gains. Sometimes, victims are allowed to withdraw some of these initial "funds" to further engender trust in the scheme. It is not until a large investment is made that victims find that they are unable to withdraw their funds. Even when a victim is denied access to their funds, the fraud is often not yet over. Scammers request additional payments for purported taxes or fees, promising these payments will allow victims access to their accounts. Scammers often continue to steal from their victims and do not stop until they have deprived victims of any remaining savings. In some cases, the criminals prompt victims to liquidate holdings in tax-advantaged accounts or take out home equity lines of credit and second mortgages on their homes to fund purported investments.[29]

Law enforcement has observed scammers then laundering the funds through several unhosted wallet addresses or by exchanging virtual assets on different blockchains through cross-chain bridges, referred to as chain hopping, before sending the funds to foreign-located VASPs. In some cases, these are nested VASPs, smaller financial institutions that offer services to their customers through accounts and sub-accounts at larger VASPs to benefit from the greater liquidity in larger VASPs. Scammers have also been observed using VASPs in Southeast Asia to exchange virtual assets from victims for fiat currency. In April 2023, the DOJ seized virtual assets worth an estimated $112 million linked to accounts that were allegedly used to launder the proceeds of various virtual asset confidence scams.[30] Law enforcement also identified cases in which VASPs identified and halted victim transfers; in such instances, the scammers directed victims to send funds via wire transfers to foreign bank accounts associated with shell companies or held by money mules associated with the scammers.

Some of the perpetrators of these scams may themselves be victims of separate crimes, including human trafficking. Pig butchering schemes are often run by criminal networks, which often place fake job advertisements to attract young English-speaking people from Asian countries. These individuals are then held, against their will, in secure compounds, generally in Asia, where they are forced (often under threat of violence) to scam people throughout the globe.[31]

2. Healthcare Fraud

Healthcare fraud continues to generate significant proceeds and victimize government programs as well as private entities. In fiscal year 2022, health care fraud remained a leading source of False Claims Act settlements and judgments.[32] Accordingly, the DOJ and federal law enforcement agencies devote significant resources to combating this type of fraud, including through the development of a "strike force" model of investigative and prosecutorial resources. In Fiscal Year (FY) 2022, the U.S. Sentencing Commission received 431 cases of healthcare fraud, and 90 percent of all healthcare offenders were U.S. citizens.[33] Schemes often involve hundreds of millions, if not billions, of dollars generated through

29 FinCEN, "FinCEN Alert on Prevalent Virtual Currency Investment Scam Commonly Known as "Pig Butchering" (FIN-2023-Alert005)", (September 8, 2023), https://www.fincen.gov/sites/default/files/shared/FinCEN_Alert_Pig_Butchering_FINAL_508c.pdf.

30 DOJ, "Justice Department Seizes Over $112M in Funds Linked to Cryptocurrency Investment Schemes", (April 3, 2023), https://www.justice.gov/opa/pr/justice-department-seizes-over-112m-funds-linked-cryptocurrency-investment-schemes.

31 HSI, "Special Edition Cornerstone Newsletter, HSI and ACAMS Alert: "Pig Butchering", (April 2023), https://www.ice.gov/doclib/cornerstone/pdf/cornerstoneACAMS_SpecialIssue40_Apr21_2023.pdf.

32 DOJ "False Claims Act Settlements and Judgments Exceed $2 Billion in Fiscal Year 2022", (February 7, 2023), https://www.justice.gov/opa/pr/false-claims-act-settlements-and-judgments-exceed-2-billion-fiscal-year-2022.

33 USSC, "Health Care Fraud", (August 2023), https://www.ussc.gov/sites/default/files/pdf/research-and-publications/quick-facts/Health_Care_Fraud_FY22.pdf.

fraudulent activity and run the gamut from corporate fraud, bribery, and kickbacks, to activity resulting in the illicit distribution and diversion of narcotics. These large-scale fraud schemes increase healthcare costs, waste limited resources, and cause an increased risk of mortality.[34] Investigators and prosecutors have employed innovative methods to target particularly egregious activity, given the complexity of these schemes.[35]

One of the most common types of fraud perpetrated against Medicare, Medicaid, and other Federal healthcare programs involves filing false claims for reimbursement.[36] Groups ranging from large networks to small groups are actively filing false claims to generate funds. One recent case saw Francisco Patino, M.D., convicted of fraud and money laundering, among other charges, for his role in running a scheme that required patients to receive unnecessary medical treatment and prescriptions of dangerous and unnecessary addictive opioids. Patino and a handful of co-conspirators submitted over $250 million in false and fraudulent claims to Medicare,[37] Medicaid,[38] and other health insurance programs for unnecessary medical treatment.[39] Another example of healthcare fraud includes the use of fake medical supply companies to fraudulently bill Medicare, Medicaid, and private healthcare insurers to generate hundreds of thousands of dollars in illicit proceeds.[40]

Fraudsters are often repeat money laundering offenders. For example, Carlos Alberto Padron pleaded guilty to money laundering involving two separate money laundering conspiracies while on supervised release from a prior federal prison sentence. During 2022, Padron laundered $249,901 in Medicare fraud proceeds related to two fraudulent durable medical equipment (DME)[41] companies. Padron and his co-conspirator picked up nearly $229,920 in cash in parking lots after they laundered the money. During 2021, Pardon also laundered $2,185,392 in Medicare fraud proceeds related to two other DME companies. Padron was involved in managing the nominee owner of those two companies and received some of the approximately $260,000 in withdrawals of Medicare fraud proceeds from the nominee owner.[42]

34 CMS, "Exploring Fraud, Waste, and Abuse within Telehealth", https://www.cms.gov/files/document/hfpp-white-paper-exploring-fraud-waste-abuse-within-telehealth.pdf-0.

35 DOJ, Health Care Fraud Unit Website (accessed 11/1/23), https://www.justice.gov/criminal-fraud/health-care-fraud-unit.

36 HHS, "Semiannual Report to Congress", (Spring 2023), https://oig.hhs.gov/reports-and-publications/semiannual/index.asp.

37 Medicare is Government health insurance for people 65 or older. See *What is Medicare,* https://www.medicare.gov/what-medicare-covers/your-medicare-coverage-choices/whats-medicare.

38 All states, the District of Columbia, and the U.S. territories have Medicaid programs designed to provide health coverage for low-income people. Although the Federal government establishes certain parameters for all states to follow, each state administers their Medicaid program differently, resulting in variations in Medicaid coverage across the country. See *Medicaid Program History*, https://www.medicaid.gov/about-us/program-history/index.html.

39 DOJ, "Doctor Sentenced for Role in Illegally Distributing 6.6 Million Opioid Pills and Submitting $250 Million in False Billings", (January 1, 2023), https://www.justice.gov/opa/pr/doctor-sentenced-role-illegally-distributing-66-million-opioid-pills-and-submitting-250.

40 DOJ, "Woman Convicted of Laundering Over $750,000 from Health Care Fraud Scheme", (May 13, 2022,) https://www.justice.gov/opa/pr/woman-convicted-laundering-over-750000-health-care-fraud-scheme#:~:text=According percent20to percent20court percent20documents percent20and, percent2C percent20to percent20her percent20co percent2Dconspirators.

41 Durable medical equipment (DME) is defined as equipment and supplies ordered by a health care provider for everyday or extended use. Coverage for DME may include oxygen equipment, wheelchairs, crutches or blood testing strips for diabetics.

42 DOJ, "Repeat Offender Sentenced to a total of 90 Months in Prison for Money Laundering of Medicare Fraud Proceeds", (September 20, 2023), https://www.justice.gov/usao-sdfl/pr/repeat-offender-sentenced-total-90-months-prison-money-laundering-medicare-fraud.

a) Telemedicine Fraud

Recent adjudicated law enforcement cases and court documentation indicate an increase in fraudulent activity related to telemedicine. For example, a 2023 Nationwide Healthcare Fraud Enforcement Action resulted in criminal charges against telemedicine platform owners, laboratory owners, DME providers, hospice operators, and pharmacists, with losses totaling approximately 1.1 billion U.S. dollars (USD).[43] This corresponds to the increase in telemedicine visits due to the COVID-19 pandemic when many patients stopped in-person visits with medical providers. One indictment demonstrates how one doctor allegedly signed prescriptions and order forms via telemedicine services for DME that were not medically necessary. The defendant based the submission of the claims based solely on short telephone conversations with beneficiaries they had not physically examined and evaluated and that were induced, in part, by the payments of bribes and kickbacks the doctor received from telemedicine companies. The doctor and others submitted or caused the submission of approximately $10 million in false and fraudulent claims to Medicare, resulting in the payout of more than $4 million.[44]

In another case, an individual was criminally charged for their role in a scheme in which they invested in a pharmacy. The defendant operated a call center where telemarketers persuaded Medicare beneficiaries to accept prescriptions for expensive medications that the beneficiaries neither needed nor wanted. The individual allegedly obtained signed prescriptions by paying kickbacks to two telemedicine companies. Through two companies the individual controlled, the individual was paid kickbacks from the pharmacy he invested in and other pharmacies In the network in exchange for supplying signed prescriptions for the medications.[45]

3. Update on COVID-19-Related Fraud

As indicated in the 2022 NMLRA, the COVID-19 pandemic accelerated online financial activity, leading to increased fraud risk for online financial services and an overall spike in activity related to healthcare, bank, elder, and government benefit fraud schemes with a connection to COVID-19. Since March 2020, Congress provided over $4.6 trillion to help the nation respond to and recover from the COVID-19 pandemic. The public health crisis, economic instability, and increased flow of federal funds associated with the pandemic increased pressures on federal agency operations and presented opportunities for individuals to commit fraud. The COVID-19 pandemic saw an increase in the number of fraud-related charges, including schemes by individuals and large, complex syndicates. Many individuals and entities facing fraud-related charges in cases involving COVID-19 relief programs have already been found guilty of criminal violations or were found liable for civil violations. For example, the DOJ has brought federal fraud-related charges against at least 2,191 individuals or entities in cases involving federal COVID-19 relief programs, consumer scams, and other types of fraud as of June 30, 2023.[46]

43 DOJ, "National Enforcement Action Results in 78 Individuals Charged for $2.5B in Health Care Fraud," (June 28, 2023), https://www.justice.gov/opa/pr/national-enforcement-action-results-78-individuals-charged-25b-health-care-fraud.

44 DOJ, "Physician Indicted in $10 Million Telemedicine Health Care Fraud Scheme", (April 21, 2022), https://www.justice.gov/usao-edny/pr/physician-indicted-10-million-telemedicine-health-care-fraud-scheme.

45 DOJ, "DOJ Announces Nationwide Coordinated Law Enforcement Action to Combat Health Care Fraud and Opioid Abuse", case summaries, January 28, 2023, https://www.justice.gov/criminal-fraud/health-care-fraud-unit/2023-national-hcf-case-summaries.

46 Government Accounting Office (GAO), "COVID-19: Insights from Fraud Schemes and Federal Response Efforts", GAO-24-106353, (November 2023), https://www.gao.gov/assets/d106353.pdf.

While in-person healthcare and financial activity has resumed, a significant amount of healthcare and commerce is still conducted virtually, leaving ample opportunity for online criminal activity. The number of individuals or entities facing fraud charges related to COVID-19 relief programs has grown since March 2020 and will likely continue to increase as these cases take time to develop. For example, an individual charged in an indictment in 2022 may not receive a trial until 2023, and if found guilty, the sentencing may occur in 2024 or later. As of August 2022, the statute of limitations has been extended to 10 years to prosecute individuals who committed Paycheck Protection Program (PPP) and Economic Injury Disaster Loan (EIDL)-related fraud. Many of these cases continue to demonstrate the magnitude of proceeds generated from COVID-related fraud.

FinCEN has issued a number of COVID-19-Related Advisories and Alerts during 2020-2023.[47] For example, in November 2023, FinCEN and IRS-CI issued a joint alert regarding the Employee Retention Credit (ERC) to highlight its significance (323 investigations involving more than $2.8 billion of potentially fraudulent ERC claims in 2020-2023) and the existence of "ERC mills" that are perpetrating the fraud.[48]

A wide array of COVID-19-related fraud cases demonstrate money laundering schemes. The leader of one such scheme, Seattle-Paradise Williams, pleaded guilty to wire fraud and money laundering charges. Williams personally received more than $2 million in fraudulent proceeds and spent the money on extravagant expenses such as luxury cars, lavish trips, cosmetic surgery, jewelry, and designer goods. Upon receipt of the illegal funds, Williams and her associates methodically laundered the funds through cash withdrawals, wire transfers, and expensive personal purchases. Williams also received more than $1.2 million in kickback payments from her associates for facilitating the fraudulent submissions.[49] In another case, a real estate broker, Chad Wade, pleaded guilty to wire fraud and money laundering and bankruptcy fraud, and entered into a $4 million civil settlement for submitting false information to obtain COVID-19 loans and using those proceeds to purchase high-end real estate and luxury items.[50]

4. Elder Financial Exploitation

Elder financial exploitation (EFE) —also referred to as elder fraud—is a growing money laundering threat linked to more than $3 billion of reported financial losses annually, with victims on average losing $35,000.[51] EFE is defined as the illegal or improper use of an older adult's funds, property, or assets.[52] Elder abuse, a broader category of illegal activity that includes EFE as well as physical and emotional abuse, affects at least 10 percent of those age 65 or older in the United States according to the DOJ.[53] Several of FinCEN's recent alerts and advisories, including a 2022 advisory on EFE, highlight that an

47 FinCEN, https://fincen.gov/coronavirus.

48 FinCEN, "FinCEN Alert on COVID-19 Employee Retention Credit Fraud," FIN-2023-Alert007, (November 22, 2023), https://fincen.gov/sites/default/files/shared/FinCEN_ERC_Fraud_Alert_FINAL508.pdf.

49 DOJ, "Leader of $6.8 Million Pandemic Fraud Scheme Pleads Guilty to Wire Fraud and Money Laundering Charges," (December 11, 2023), https://www.justice.gov/usao-wdwa/pr/leader-68-million-pandemic-fraud-scheme-pleads-guilty-wire-fraud-and-money-laundering.

50 DOJ, "Florida Real Estate Broker Agrees To Pay Over $4 Million To Resolve False Claims Act Allegations Relating To Fraudulent Cares Act Loans", (August 16, 2023), https://www.justice.gov/usao-ndfl/pr/florida-real-estate-broker-agrees-pay-over-4-million-resolve-false-claims-act.

51 FBI, "Elder Fraud Report," (2022), https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3ElderFraudReport.pdf.

52 CFPB and FinCEN, "Memorandum on EFE," (August 30, 2017), https://www.fincen.gov/sites/default/files/2017-08/8-25-2017_FINAL_CFPB percent2BTreasury percent2BFinCEN percent20Joint percent20Memo.pdf.

53 For more information on EFE, *see* DOJ, "About Elder Abuse," https://www.justice.gov/elderjustice/about-elder-abuse.

increasing number of these schemes are now cyber-enabled.[54] According to the FBI, virtual asset-related losses reported by older adults increased by 350 percent from 2021 to 2022.[55]

Targets of EFE schemes are often victimized after having accumulated life savings in conjunction with perceived or actual declining cognitive or physical abilities, decreased social interactions, increased reliance on others for financial management and physical well-being, and potential unfamiliarity with different technology.[56,57] Victims may be exploited for an extended period, are often re-victimized, and are subject to potential further loss due to compromised personally identifiable information (PII), which may be sold on darknet marketplaces.

EFE schemes consist of two types of fraud: elder theft and elder scams. With elder theft, the perpetrator typically has a preexisting relationship with the victim that the perpetrator exploits to steal assets, funds, or income. According to the FinCEN Advisory on Elder Financial Exploitation, 46 percent of elder theft cases are perpetrated by a family member.[58] Exploitation of legal guardianships, power of attorney arrangements, and Ponzi schemes targeting older adults are common examples of elder theft schemes. In elder scams, the perpetrator is often unknown to the victim.[59] These perpetrators are frequently located outside of the United States and use cyber-enabled techniques. Scammers often impersonate government officials, law enforcement officers, customer support representatives (*e.g.,* computer repair), social media connections, and even family, friends, and other known persons to induce victims to send money. Perpetrators attempt to create high-pressure situations to create urgency and take advantage of their victim's trust, emotions, or fear to solicit payments. Some elder scams involve online dating; these are broadly referred to as "romance scams."[60]

Cases involving EFE often utilize traditional money laundering techniques such as in-person cash pickups from victims,[61] receiving cash or checks via the mail, use of shell and front companies, wire transfers,

54 FinCEN, "Advisory on Elder Financial Exploitation), (June 15, 2022), https://www.fincen.gov/sites/default/files/advisory/2022-06-15/FinCEN percent20Advisory percent20Elder percent20Financial percent20Exploitation percent20FINAL percent20508.pdf; FinCEN, "Advisory on Cybercrime and Cyber-Enabled Crime Exploiting the Coronavirus Disease 2019 (COVID-19) Pandemic", (July 30, 2020), https://www.fincen.gov/sites/default/files/advisory/2020-07-30/FinCEN percent20Advisory percent20Covid percent20Cybercrime percent20508 percent20FINAL.pdf.

55 FBI, "Elder Fraud Report," (2022), https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3ElderFraudReport.pdf. In 2022, the FBI's Internet Crime Complaint Center received almost 10,000 complaints from victims over the age of 60 involving the use of some type of virtual asset, such as Bitcoin, Ethereum, Litecoin, or Ripple. Losses incurred by these victims totaled over $1 billion.

56 CFPB and FinCEN, Memorandum on EFE, *supra* Note 1. *See also,* FTC Older Consumers Report, *supra* Note 1.

57 DOJ, "Associate Attorney General Vanita Gupta Delivers Remarks at the Elder Justice Coordinating Council Meeting," (Dec. 7, 2021), https://www.justice.gov/opa/speech/associate-attorney-general-vanita-gupta-delivers-remarks-elder-justice-coordinating; DOJ, "Statement of Attorney General Merrick B. Garland on World Elder Abuse Awareness Day," (Jun. 15, 2021) https://www.justice.gov/opa/pr/statement-attorney-general-merrick-b-garland-world-elder-abuse-awareness-day?utm_medium=email&utm_source=govdelivery.

58 FinCEN, "Advisory on Elder Financial Exploitation", (June 15, 2022), https://www.fincen.gov/sites/default/files/advisory/2022-06-15/FinCEN percent20Advisory percent20Elder percent20Financial percent20Exploitation percent20FINAL percent20508.pdf.

59 These include lottery phone scams, grandparent scams, romance scams, IRS or government imposter scams, and sham business opportunities.

60 DOJ, "Woodbridge Money Launderer Sentenced for his Role in a Romance Fraud Scheme" (Mar. 11 2022) https://www.justice.gov/usao-edva/pr/woodbridge-money-launderer-sentenced-his-role-romance-fraud-scheme#:~:text=Woodbridge percent20Money percent20Launderer percent20Sentenced percent20for percent20his percent20Role percent20in percent20a percent20Romance percent20Fraud percent20Scheme,-Friday percent2C percent20March percent2011&text=ALEXANDRIA percent2C percent20Va.,scheme percent20against percent20mostly percent20elderly percent20victims.

61 DOJ, "Defendant in 'Grandparent Scam' Network Sentenced for RICO Conspiracy Targeting Elderly Americans," (Aug. 17, 2022), https://www.justice.gov/opa/pr/defendant-grandparent-scam-network-sentenced-rico-conspiracy-targeting-elderly-americans.

virtual assets, and laundering funds through multiple bank accounts, often using fake PII, [62] and through the use of money mules.[63]

Call Center Fraud

Illegal call centers defraud thousands of victims each year and are responsible for over $1 billion in losses to victims.[64] Call center fraud encompasses a variety of financial fraud typologies, but generally refers to scams that illicit actors perpetrate over the phone from call centers located overseas. Call center fraud, while not new, has proliferated rapidly in recent years and now includes timeshare fraud (see below). Call center fraud overwhelmingly targets older adults, making it also a form of EFE.[65]

According to the FBI, tech and customer support fraud reports were up 132 percent in 2022. In these scams, fraudsters may pose as customer or tech support representatives from well-known companies and claim that the victim's account or computer has been compromised. They then may ask victims to install desktop software remotely (*e.g.,* "trojan horses" or other types of malware) to allow them to monitor activity, which then gives the fraudster complete control over the victim's computer.[66]

In government impersonation scams, the fraudster impersonates a law enforcement agent, Internal Revenue Service (IRS) representative, or other government official. The scammers may also spoof phone numbers or use fake credentials to appear legitimate. Scammers create various scenarios to elicit payment, including that the victim has missed jury duty and must provide payment immediately to avoid arrest or must provide personal information to renew a driver's license, passport, or medical license.[67] These types of scams frequently emanate from call centers in South Asia, mainly India, and often target Americans.[68] In 2022, with the assistance of U.S. law enforcement, Indian law enforcement accomplished multiple call center raids, disruptions, seizures, and arrests of the individuals alleged to be involved in perpetrating these cyber-enabled financial crimes and global telemarketing frauds.

In recent years, organized crime groups such as CJNG have committed timeshare fraud using call centers in Mexico.[69] The FBI, SEC, and U.S. Embassy in Mexico have all issued warnings in recent years about the increasing prevalence of these types of call center-based scams aimed at Americans who own timeshares

62 DOJ, "Four Individuals Charged with Conspiring to Launder Money Obtained from Romance Scams" (Apr. 13, 2022), https://www.justice.gov/usao-nj/pr/four-individuals-charged-conspiring-launder-money-obtained-romance-scams.

63 DOJ, "Two Californians Indicted in Multi-Million Dollar Tech-Support Scam Targeting Elderly Victims" (May 12, 2022), https://www.justice.gov/usao-wdpa/pr/two-californians-indicted-multi-million-dollar-tech-support-scam-targeting-elderly.

64 FBI Annual Internet Crime Report 2022, https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3Report.pdf, p. 16.

65 Id.

66 FBI, "FBI Warns Public to Beware of Tech Support Scammers Targeting Financial Accounts Using Remote Desktop Software", (October 18, 2023), https://www.fbi.gov/contact-us/field-offices/boston/news/press-releases/fbi-warns-public-to-beware-of-tech-support-scammers-targeting-financial-accounts-using-remote-desktop-software.https://www.fbi.gov/contact-us/field-offices/boston/news/press-releases/fbi-warns-public-to-beware-of-tech-support-scammers-targeting-financial-accounts-using-remote-desktop-software

67 IC3, "FBI Warns of the Impersonation of Law Enforcement and Government Officials" (March 07, 2022), https://www.ic3.gov/Media/Y2022/PSA220307.

68 DOJ, "Multiple India-based call centers and their directors indicted for perpetuating phone scams affecting thousands of Americans", (February 3, 2022), https://www.justice.gov/usao-ndga/pr/multiple-india-based-call-centers-and-their-directors-indicted-perpetuating-phone-scams.

69 Treasury, "Treasury Sanctions Fugitive, Others Linked to CJNG Timeshare Fraud Network," (April 27, 2023), https://home.treasury.gov/news/press-releases/jy1443.

in Mexico.[70] In these schemes, fraudsters may pose as travel or real estate agents, sales representatives, or brokerage firms, and make unsolicited offers to owners of timeshare properties. If the timeshare owner agrees, the scammer tells the victim to pay an "upfront fee" to facilitate or expedite the sale of the property. Once this fee is paid, all communication by the scammer may cease, or they may demand additional fees from the victim. Some victims reported that they were contacted by a fake "timeshare fraud recovery company" that promised to assist victims in recovering their money and then asked for additional fees for this service. [71] As with the prior call center fraud typologies noted, this kind of fraud overwhelmingly affects retirees and older Americans.

5. Special Focus: Check Fraud

While the use of checks in the financial system has declined, check fraud over the last few years has boomed due to the limited capability of financial institutions to verify the legitimacy of checks in a timely manner, the lack of self-verification systems built into checks, the prevalence of remote capture technology,[72] and the ability to directly access all funds within a specified account through a single check.[73]

The U.S. government continues to use checks, in addition to other payment options, to issue federal payments, including for Medicare and Medicaid reimbursement and income tax refunds. However, the use of paper checks by the U.S. government is declining overall both in terms of number of payments and total value moved. However, checks remain a major monetary instrument, with check payments worth $27.23 trillion in 2021, according to the 2022 Federal Reserve Payments Study.[74] For example, the average dollar value per commercial check has been trending upward in recent years.[75]

Check fraud refers to the illicit use of either paper or digital checks[76] to unlawfully gain money. Some examples of check fraud include check washing,[77] counterfeit checks or "check kiting" (checks presented based on fraudulent identification or are false checks drawn on valid account), and fraudulent checks (either as a signature or endorsement). BSA reporting by financial institutions has documented the rapid growth of check fraud.[78] The number of SARs relating to check fraud increased by 94 percent between 2021 and 2022 and 23 percent between 2020 and 2021.

70 U.S. Embassy Mexico, "Real Estates and Time Shares - Fraud Typology", (May 3, 2023), https://mx.usembassy.gov/real-estate-and-time-shares-fraud-typology/.

71 Id.

72 FDIC, "Remote Deposit Capture: A Primer," (Updated: June 6, 2023), https://www.fdic.gov/regulations/examinations/supervisory/insights/sisum09/sisummer2009-article02.html#:~:text=RDC percent20allows percent20financial percent20institution percent20customers,instant percent20credit percent20to percent20their percent20account.

73 Federal Reserve Board (FRB) "The Federal Reserve Payments Study: 2022 Triennial Initial Data Release", (Updated July 27, 2023), https://www.federalreserve.gov/paymentsystems/fr-payments-study.htm.

74 Id.

75 FRB, "Commercial Checks Collected through the Federal Reserve--Quarterly Data," (update November 17, 2023), https://www.federalreserve.gov/paymentsystems/check_commcheckcolqtr.htm.

76 Investopedia, "Check: What It Is, How Bank Checks Work, and How to Write One," (Updated June 2, 2023), https://www.investopedia.com/terms/c/check.asp.

77 USPIS, "Check Washing," (Updated October 13, 2023), https://www.uspis.gov/news/scam-article/check-washing.

78 FinCEN, "FinCEN Alert on Nationwide Surge in Mail Theft-Related Check Fraud Schemes Targeting the U.S. Mail," FIN-2023-Alert003, (February 27, 2023), https://www.fincen.gov/sites/default/files/shared/FinCEN%20Alert%20Mail%20Theft-Related%20Check%20Fraud%20FINAL%20508.pdf.

U.S. law enforcement has also observed an increase in check fraud activity, with fraudsters targeting checks from businesses and checks with large dollar amounts due to a perception that the accounts the checks draw from are well funded and the checks will not bounce, leading to large losses and unpaid bills for victims.

There have been several criminal cases demonstrating money laundering activity involving check fraud. A 2022 case related to a nationwide check kiting "bust out" scheme where bank accounts were opened using a fake passport to receive checks from accounts with insufficient funds. Fraudsters then withdrew those funds before the checks cleared.[79]

Mail Theft-Related Check Fraud

Mail theft-related check fraud refers to the fraudulent negotiation of checks stolen from the U.S. Mail.[80] According to discussions with U.S. law enforcement, there has been a notable spike in mail theft in 2023, as evidenced by a 139 percent increase in reports of high-volume mail theft from mail receptacles over the past four fiscal years. Due to a nationwide surge in mail theft-related check fraud targeting the U.S. Mail, FinCEN issued an alert in collaboration with the United States Postal Inspection Service (USPIS) in February 2023 that identified trends, risks, typologies, and red flags of these schemes.[81] By issuing the mail theft-related check fraud alert, FinCEN sought to ensure that SARs filed by financial institutions appropriately identify and report suspected check fraud schemes that may be linked to mail theft in the United States.

According to FinCEN's alert, after a check is stolen from the mail, criminals will often "wash" the checks, which is altering them using acetone chemicals to remove the original ink applied by the check issuer.[82] The criminal then replaces the payee information with their own, a fraudulent identity (or that of a money mule), or fraudulent business they control. They also frequently increase the dollar amount of the check. Similarly, criminals engaged in mail theft-related check fraud will often take the information found on the original victim's check, such as routing and account numbers, and use those numbers to generate additional checks. Criminal actors involved in mail theft can also sell checks or PII stolen from the mail over darknet marketplaces or on encrypted social media platforms such as Telegram.[83]

Once the altered or counterfeit check has been deposited, criminals quickly withdraw cash or transfer the funds via wire transfers to alternative accounts to obfuscate the individuals involved or the destination of

79 DOJ, "Korean National Sentenced to 7 Years and 9 Months in Prison for "Bust Out" Bank Fraud Scheme in Sacramento Area and Elsewhere", (November 10, 2022), https://www.justice.gov/usao-edca/pr/korean-national-sentenced-7-years-and-9-months-prison-bust-out-bank-fraud-scheme#:~:text= percentE2 percent80 percent94 percent20Kyung percent20Min percent20Kong percent2C percent2055 percent2C,Talbert percent20announced; DOJ, "Colorado Man Pleads Guilty to "Bust Out" Bank Fraud Scheme in Sacramento Area and Elsewhere", (July 14, 2022), https://www.justice.gov/usao-edca/pr/colorado-man-pleads-guilty-bust-out-bank-fraud-scheme-sacramento-area-and-elsewhere#:~:text=Area percent20and percent20Elsewhere-,Colorado percent20Man percent20Pleads percent20Guilty percent20to percent20 percentE2 percent80 percent9CBust percent20Out percentE2 percent80 percent9D percent20Bank percent20Fraud percent20Scheme,in percent20Sacramento percent20Area percent20and percent20Elsewhere&text=SACRAMENTO percent2C percent20Calif.,Talbert percent20announced.

80 Business checks may be more valuable because business accounts typically hold higher account balances, and these victims take longer notice the fraud on average.

81 FinCEN, "FinCEN Alert on Nationwide Surge in Mail Theft-Related Check Fraud Schemes Targeting the U.S. Mail", (February 7, 2023), https://www.fincen.gov/sites/default/files/shared/FinCEN percent20Alert percent20Mail percent20Theft-Related percent20Check percent20Fraud percent20FINAL percent20508.pdf.

82 USPIS, "Check Washing" (updated October 13, 2023), https://www.uspis.gov/news/scam-article/check-washing.

83 For more information regarding Telegram, see SEC, "Telegram to Return $1.2 Billion to Investors and Pay $18.5 Million Penalty to Settle SEC Charges," (June 26, 2020), https://www.sec.gov/news/press-release/2020-146.

the funds. Additionally, the criminal may use the victim's PII to continue to engage in check fraud, open new bank accounts, or perpetrate credit card fraud.

For example, in October 2023, Ishmael Benreuben pleaded guilty to a conspiracy to deposit approximately $760,000 in fraudulent checks into bank accounts across New York, New Jersey, and Washington, D.C., and to fraudulently withdraw approximately $115,000. Between 2021 and 2022, Benreuben stole checks from the mail, forged and altered them, deposited them into various bank accounts, and then quickly withdrew the funds before the banks could void the checks or close the accounts. Benreuben worked alongside 26 others who owned the bank accounts and received a portion of the fraudulent funds.[84]

To facilitate mail theft-related fraud, criminals will often use money mules, individuals who receive and move criminal proceeds. Criminals can recruit mules in person or over social media. (See Section on Money Mule Networks) Some criminals will offer the money mule a fee (*e.g.,* a portion of a check's value) in exchange for using their bank account to clear the check.[85] The funds are then quickly transferred out of the account before the checks are returned or flagged. Once this occurs, the mule who deposited the checks is responsible for the stolen funds, and the financial institution will hold them accountable for the missing or stolen funds.

Check fraud actors will also pay mules for access to their banking information, including debit card, bank pin, and password. After receiving the information, the check fraud actor will access the mule accounts to deposit checks and withdraw proceeds. Criminal actors prefer using these already established bank accounts with demonstrated regular banking activity as said accounts generally have fewer checking restrictions placed on them by financial institutions, allowing for a larger percent of the checks' value to be accessed immediately upon deposit.

6. Business Email Compromise (BEC)

In 2022, the FBI received 21,832 BEC complaints with adjusted losses totaling more than $2.7 billion, which makes it a top money laundering threat in the United States. BEC is a scam that elicits fraudulent payments or sensitive identifying information using compromised email accounts. Scammers may take over a legitimate email address and use it to contact victims or create their own email address that is nearly identical to a legitimate one and then contact victims.

These scams often target businesses or individuals who regularly perform wire transfer payments to send funds. The fraudsters may also compromise or spoof other forms of communication, such as phone numbers and virtual meeting applications, social engineering, or other computer intrusion techniques. These schemes aim to induce targets to transfer funds to bank accounts thought to belong to trusted partners.[86]

Further, in 2022, the FBI saw a slight increase in instances whereby criminal actors targeted victims' investment accounts rather than traditional banking accounts. Additionally, the FBI noted increased

84 DOJ, "Mount Vernon Man Pleads Guilty To Elaborate Check Fraud Scheme", (October 10, 2023), https://www.justice.gov/usao-sdny/pr/mount-vernon-man-pleads-guilty-elaborate-check-fraud-scheme.

85 USPIS, "Check Fraud", (updated May 1, 2019), https://www.uspis.gov/news/scam-article/check-fraud.

86 FinCEN, "Updated Advisory on Email Compromise Fraud Schemes Targeting Vulnerable Business Processes", (July 16, 2019), https://www.fincen.gov/sites/default/files/advisory/2019-07-16/Updated percent20BEC percent20Advisory percent20FINAL percent20508.pdf.

instances where BEC perpetrators spoof legitimate business phone numbers to confirm fraudulent banking details with victims.[87] Over the last several years, methodologies have evolved and now involve the impersonation of more entities with greater levels of detail (e.g., vendors, lawyers, requests for seeming legitimate paperwork like W-2 information), diverting payroll funds, targeting real estate payments, and requests for large amounts of gift cards.[88] As noted in the 2022 NMLRA, BEC in the real estate sector has become more prevalent, with individual homebuyers suffering disproportionately from these incidents.

In March 2023, FinCEN issued a Financial Trends Analysis on patterns and trends identified in BSA data relating to BEC in the real estate sector in 2020 and 2021.[89] FinCEN found that the sector remains a target for BEC attacks exploiting the high monetary values generally associated with real estate transactions and the various communications between entities involved in the real estate closing process (e.g., title companies, title agents, closing agents, and escrow companies, and other individuals and entities involved in the title and closing processes). Perpetrators of BEC in the real estate sector may obtain unauthorized access to networks and systems to misappropriate confidential and proprietary information to increase the likelihood that their scam is successful.

Those involved in BEC scams often use several traditional ML techniques to launder their illicit funds. For example, fraudsters may establish a fake business whose name closely resembles that of a legitimate company and then use unwitting money mules to establish bank accounts that will be used for the layering process. Once a victim has sent the funds to a fake business, the manager of the fraud group will work with others to transfer the funds from the mule accounts before they ultimately end up in accounts under the group's control. In other cases, the fraudsters may simply withdraw funds as cash or negotiable instruments such as cashier's checks or have mules make withdrawals on their behalf.[90]

Drug Trafficking

The trafficking of illicit drugs, and related money laundering remains a significant threat to U.S. public health and national and economic security. TCOs, primarily based in Mexico but operating a global illicit supply chain, engage in the trafficking of a variety of drugs, including counterfeits, into the United States. Since at least 2017, illicit fentanyl has been the largest driver of overdose deaths and the number one counter-narcotics priority for the U.S. government. Illicit fentanyl is often mixed with other illicit drugs or pressed and sold as counterfeit versions of other substances (such as prescriptions or veterinary medication).

Consistent with the 2022 NMLRA, criminal actors in the drug trade embrace several methods to launder proceeds, including bulk cash smuggling (BCS), funnel accounts, structured money transfers, trade-based money laundering (TBML), purchase of real estate and luxury items, and virtual assets. While the laundering of drug trafficking proceeds is predominantly cash-based, the use of virtual assets is

87 FBI, "2022 Internet Crime Report", https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3Report.pdf.

88 FBI, "2022 Congressional Report on BEC and Real Estate Wire Fraud", https://www.fbi.gov/file-repository/fy-2022-fbi-congressional-report-business-email-compromise-and-real-estate-wire-fraud-111422.pdf/view.

89 FinCEN, "FinCEN Analysis of Business Email Compromise in the Real Estate Sector Reveals Threat Patterns and Trends," (March 30, 2023), https://www.fincen.gov/news/news-releases/fincen-analysis-business-email-compromise-real-estate-sector-reveals-threat.

90 DOJ, "Carson Man Sentenced to More Than 11 Years in Prison for Role in International Conspiracy to Launder Money Taken from Fraud Victims," (February 27, 2023), https://www.justice.gov/usao-cdca/pr/carson-man-sentenced-more-11-years-prison-role-international-conspiracy-launder-money.

a growing concern for U.S. law enforcement. Drug traffickers are also turning to professional money launderers to launder their ill-gotten proceeds. In particular, drug traffickers use Chinese Money Laundering Organizations (CMLOs),[91] which employ an informal value transfer system (IVTS) to move value across borders without needing to use the U.S. financial system. CMLOs have come to dominate money laundering services for some DTOs.

This section focuses on the major money laundering threats involving proceeds generated from the trafficking of illicit synthetic opioids, given that is the biggest narcotics-related challenge currently facing the United States. The section also highlights prescription drug diversion and addresses the priority DTO threat actors.

1. Illicit Synthetic Opioids (including Fentanyl) and Heroin

According to the Drug Enforcement Administration (DEA), the availability of fentanyl throughout the United States has reached "unprecedented heights."[92] Since 2019, Mexican TCOs predominately import fentanyl precursor chemicals and related manufacturing equipment[93] by air and marine shipping from the People's Republic of China (PRC). This diversion of fentanyl precursor chemicals and manufacturing equipment can also be facilitated by a loose network of brokers who identify buyers and sellers. Once the precursor chemicals and manufacturing equipment are diverted to Mexico, cooks and chemists associated with the TCOs fabricate illicit fentanyl into pill and powder form, sometimes mixed with other illicit drugs or as counterfeit versions of pharmaceuticals (such as Vicodin).

In 2022, the DEA seized more than 58 million counterfeit pills containing fentanyl, and 13,000 pounds of fentanyl powder, equating to nearly 400 million deadly doses of fentanyl.[94] Data from the Centers for Disease Control and Prevention consistently cite that about 75 percent of all overdose deaths are attributed to illicit synthetic opioids, particularly fentanyl and its analogues.[95]

Given the global nature of DTOs, the proceeds of fentanyl sales in the United States will intersect many jurisdictions. A January 2024 case denotes this reality. This case involved a Utah-based company that was allegedly the laundering hub for multiple drug trafficking organizations which laundered more than $20 million of dollars via wire transfers from Utah to Mexico and Honduras. According to court documents, the company served as a money-remitting business for fentanyl and other drug proceeds, which the defendants then used to falsify wire transfer information to avoid detection.[96]

91 See Section on CMLOs.

92 DEA, "Statement of Anne Milgram Administrator DEA, DOJ At a Hearing Entitled "Drug Enforcement Administration Oversight" Before the House Subcommittee on Crime and Federal Government Surveillance", (July 27, 2023, https://www.dea.gov/sites/default/files/2023-07/Administrator percent20Written percent20SFR percent20July percent202023 percent20 percent28Final percent29.pdf.

93 To include pill presses, encapsulating machines, and die molds.

94 DEA, "Statement of Anne Milgram Administrator DEA, DOJ At a Hearing Entitled "Drug Enforcement Administration Oversight" Before the House Subcommittee on Crime and Federal Government Surveillance", (July 27, 2023, https://www.dea.gov/sites/default/files/2023-07/Administrator percent20Written percent20SFR percent20July percent202023 percent20 percent28Final percent29.pdf.

95 CDC, "Drug Overdose Deaths Remained High in 2021" (update August 22, 2023), https://www.cdc.gov/drugoverdose/deaths/index.html#:~:text=Opioids percent20were percent20involved percent20in percent2080 percent2C411,and percent20without percent20synthetic percent20opioid percent20involvement.

96 DOJ, "24 Defendants, including a Utah Business Owner, Accused of Running a Drug and Money Laundering Operation from Utah to Mexico and Honduras," (January 8, 2024), https://www.justice.gov/usao-ut/pr/24-defendants-including-utah-business-owner-accused-running-drug-and-money-laundering.

In the first criminal charges against China-based chemical manufacturing companies and nationals of the PRC for trafficking fentanyl precursor chemicals into the United States, the DOJ announced the arrest of two individuals and the unsealing of three indictments charging China-based companies and their employees with crimes related to fentanyl production, distribution, and sales resulting from precursor chemicals. One of the indictments also charges defendants with money laundering offenses.[97] According to the allegations contained in the indictment and other court filings, a chemical manufacturer based in the city of Wuhan, China, exported vast quantities of the precursor chemicals used to manufacture fentanyl and its analogues. This manufacturer has openly advertised online its shipment of fentanyl precursor chemicals to the United States and to Mexico, where drug cartels operate clandestine laboratories, synthesize finished fentanyl at scale, and distribute the deadly fentanyl into and throughout the United States. According to court documents, the defendants took payment for the shipments in virtual assets.[98]

In May 2023, the DOJ's Joint Criminal Opioid and Darknet Enforcement team and international partners announced the results of Operation SpecTor, which included 288 arrests.[99] One investigation that was part of Operation SpecTor resulted in a May 2022 indictment of two defendants charging them with conspiracy to distribute and possess with intent to distribute fentanyl and methamphetamine and with conspiracy to launder money.[100] According to court documents, the defendants operated vendor accounts on darknet marketplaces, through which they sold tens of thousands of counterfeit oxycodone pills containing fentanyl in exchange for virtual assets. One defendant deposited into his wallet at a virtual asset exchange[101] approximately $800,000 worth of bitcoin that originated from purchases made on his and the co-defendant's darknet vendor accounts. One defendant converted some part of those bitcoin holdings into fiat currency.

In October 2023, the DOJ unsealed a series of indictments against another set of PRC-based chemical companies similarly engaged in the illicit shipment of precursor chemicals.[102] In addition to accepting virtual assets as payment, according to the charging documents, the defendants also used wire transfers and a U.S.-based money services business (MSB) to process transactions.

97 DOJ, "Justice Department Announces Charges Against China-Based Chemical Manufacturing Companies and Arrests of Executives in Fentanyl Manufacturing", (June 23, 2023), https://www.justice.gov/opa/pr/justice-department-announces-charges-against-china-based-chemical-manufacturing-companies.

98 DOJ, SDNY, U.S. v. Hubei Amarvel, case 23 cr 302, https://www.justice.gov/d9/2023-06/sdny_unsealed_2023.06.22_amarvel_biotech_indictment_stamped_redacted.pdf.

99 DOJ, "Largest International Operation Against Darknet Trafficking of Fentanyl and Opioids Results in Record Arrests and Seizures", (May 2, 2023), https://www.justice.gov/opa/pr/largest-international-operation-against-darknet-trafficking-fentanyl-and-opioids-results.

100 DOJ, "Sacramento Grand Jury Indicts Riverside County Man and Woman for Fentanyl Distribution and Money Laundering Conspiracy", (May 12, 2022), https://www.justice.gov/usao-edca/pr/sacramento-grand-jury-indicts-riverside-county-man-and-woman-fentanyl-distribution-and.

101 The use of the term "exchange" in this assessment does not indicate registration as such or any legal status of any such platform. This definition is for the purpose of the risk assessment and should not be interpreted as a regulatory definition under the BSA or other relevant regulatory regimes.

102 DOJ, "Justice Department Announces Eight Indictments Against China-Based Chemical Manufacturing Companies and Employees," (October 3, 2023), https://www.justice.gov/opa/pr/justice-department-announces-eight-indictments-against-china-based-chemical-manufacturing.

SNAPSHOT: Prescription Drug Diversion

While illicit production of synthetic opioids remains a significant concern, U.S. law enforcement also prioritizes the investigation of medical professionals (or those representing themselves as such) who divert controlled substances from legitimate medical supply. Many of these offenses are associated with other predicates for money laundering, such as healthcare fraud.

In March 2023, 14 defendants were sentenced for their respective roles in a variety of crimes stemming from a wide-ranging racketeering conspiracy involving diversion of prescription drugs, money laundering, mail and wire fraud, and additional crimes.[103] According to the government's filings, prescription drugs were procured illicitly at below-market value and then were resold and re-introduced into the market as legitimate drugs at near-market prices. Illicit procurement can involve stealing drugs from manufacturers; buying drugs from patients with prescriptions at below-market prices (the patients' costs are offset or reduced by insurance, including Medicare); buying drugs using false prescriptions and straw patients, usually with the aid of a corrupt doctor (again, with the costs offset or reduced by insurance); and purchasing drugs from a manufacturer at a discounted price through fraud (*e.g.,* falsely claiming a charitable or similar discount).

2. Priority DTO Threat Actors

The illicit financial activities of DTOs pose risks to banks, money services businesses, and other entities, such as real estate agents and attorneys. DTOs have also made use of VASPs.[104]

a) Sinaloa and CJNG (Mexico)

According to its 2023 Annual Threat Assessment, the U.S. intelligence community cited Mexico-based TCOs as the dominant producers and suppliers of various illicit drugs destined for the domestic U.S. market.[105] Mexican TCOs, particularly the Sinaloa Cartel and the CJNG remain the most predominant and sophisticated groups overseeing the transportation and distribution routes from Mexico to the United States. According to the DEA, these two cartels, as well as their associates, facilitators, and brokers, operate in all 50 U.S. states and over 50 countries around the world. Both groups have consolidated control over drug corridors from Mexico and are heavily involved in the trafficking of fentanyl, methamphetamine, cocaine, heroin, and marijuana. Both have a history of establishing drug trafficking hubs, strong criminal partnerships, and using violence and corruption to gain control over the territory where they operate.[106]

According to the DOJ, the Sinaloa Cartel operates as an affiliation of drug traffickers and money launderers who obtain precursor chemicals, mainly from suppliers in China, for the manufacture of

103 DOJ, "Judgment Entered Against Fourteen Defendants In Case Dismantling Nationwide Racketeering Conspiracy", (March 30, 2023), https://www.justice.gov/usao-ndca/pr/judgment-entered-against-fourteen-defendants-case-dismantling-nationwide-racketeering.

104 DTO Activity as a national AML/CFT priority.

105 DNI, "Annual Threat Assessment of the U.S. Intelligence Community", (February 6, 2023), https://www.dni.gov/files/ODNI/documents/assessments/ATA-2023-Unclassified-Report.pdf.

106 Europol-DEA, "Complexities and Convenances in the International Drug Trade: The involvement of Mexican criminal actors in the EU drug market", (December 5, 2022), https://www.dea.gov/sites/default/files/2022-12/Europol_DEA_Joint_Report_Final.pdf, pg. 3.

synthetic drugs in Mexico. The Sinaloa Cartel will then traffic those drugs into the United States and collect, launder, and transfer the illicit proceeds back to Mexico. Once led by Joaquin Guzman Loera, aka El Chapo, and Ismael Zambada Garcia, aka El Mayo, the Sinaloa Cartel's members and associates, allegedly including the sons of Guzman Loera (collectively known as Los Chapitos), smuggled significant quantities of illicit drugs through Mexico and into the United States.[107]

In April 2023, the DOJ announced charges against several leaders of the Sinaloa Cartel, including the sons of incarcerated former Sinaloa leader Guzman Loera.[108] According to court documents, Los Chapitos leveraged several methods for laundering proceeds from fentanyl and other illicit drug sales, using various methods long used by the Sinaloa cartel and similar Mexican TCOs such as BCS, domestic and offshore bank accounts, shell companies, real estate, TBML, and virtual assets.[109]

As explained further in the Los Chapitos indictment, two of the defendants allegedly conspired to repatriate the value of drug proceeds through smuggling mobile phones as part of a TBML scheme. As part of the scheme, one defendant allegedly purchased U.S. dollars in bulk from Mexico-based Sinaloa Cartel traffickers at a discount in exchange for Mexican pesos, which represents the proceeds of cartel-linked fentanyl sales in the United States. The defendant directed U.S.-based couriers to collect drug proceeds in specific U.S. cities, which they then used to purchase cellphones in bulk. The defendant then smuggled the phones into Mexico to sell at an inflated price. (*See CMLO section for further information on schemes involving electronics*).

A two-year Organized Crime Drug Enforcement Task Forces (OCDETF) investigation dismantled a sophisticated money laundering organization linked to the Sinaloa Cartel. The investigation led to the indictment of 12 people, the seizure of over $17 million in cash and bank accounts, and the rescue of two extortion victims. The organization allegedly used shell companies incorporated in Wyoming to launder millions of dollars in cash belonging to the cartel. The leader of the organization was Enrique Daan Esparragoza Rosas, a Mexican national based in Sinaloa, who received requests from top cartel leaders like Ismael "El Mayo" Zambada and Joaquin "Chapo" Guzman. One of the defendants, Cristian Amaya Nava, admitted that he extorted two victims to repay a drug debt and laundered over $2.4 million for the cartel. Amaya Nava was sentenced to 60 months in prison.[110]

b) Clan del Golfo (Colombia)

During the assessment period, Clan del Golfo (CDG), a Colombia-based TCO and paramilitary organization, remained a significant producer and trafficker of cocaine destined for U.S. drug markets and earned a significant amount of proceeds in U.S. dollars. According to the DOJ, CDG is one of the most violent and powerful criminal organizations in Colombia, and it is one of the largest distributors of cocaine in the world. With as many as 6,000 members, the CDG exercises military control over vast amounts of territory in the Urabá region of Antioquia, Colombia, one of the most lucrative drug trafficking areas within Colombia due to its proximity to the Colombia-Panama border and the Caribbean and Pacific coasts.

107 DOJ, "Justice Department Announces Charges Against Sinaloa Cartel's Global Operation", (April 14, 2023,) https://www.justice.gov/opa/pr/justice-department-announces-charges-against-sinaloa-cartel-s-global-operation.

108 Ibid.

109 DOJ, SDNY, USA v. Ivan Archivaldo Guzman, case we CR 203, https://www.justice.gov/d9/press-releases/attachments/2023/04/14/u.s._v._salazar_et_al_indictment_2.pdf.

110 DOJ, "Sophisticated Sinaloa Cartel Money Laundering Organization Dismantled", April 11, 2023, https://www.justice.gov/usao-sdca/pr/sophisticated-sinaloa-cartel-money-laundering-organization-dismantled.

The CDG funds its operations primarily through drug trafficking. It imposes a so-called "tax" on any drug traffickers operating in territories under its control, charging fees for every kilogram of cocaine manufactured, stored, or transported through areas controlled by the organization. The CDG also directly exports cocaine and coordinates the production, purchase, and transfer of weekly and bi-weekly multi-ton shipments of cocaine from Colombia into Central America and Mexico for ultimate importation to the United States.

Cybercrime

For this report, Cybercrime[111] is defined as criminal activity that targets or uses computers under one network for the purpose of harm, often putting critical infrastructure at risk. It is distinct from cyber-enabled fraud, such as BEC.

1. Ransomware

Ransomware criminals and related payments continue to pose a potent threat to U.S. national security, our infrastructure, and our economy according to FBI reporting.[112] The number of ransomware attacks and the amount paid in ransoms is estimated to have decreased in 2022 before rebounding in 2023. For example, FinCEN identified 1,215 ransomware-related incidents reporting approximately $655.98 million in ransomware-related payments during 2022, compared to 1,410 ransomware-related incidents reporting roughly $1.12 billion in payments during 2021.

Ransomware actors have increased the potency of their attacks and exerted greater pressure on victims to pay. These actors also share resources or form partnerships with other cybercriminals to enhance the effectiveness of their attacks. Some ransomware groups use a "ransomware-as-a-service" model. This is a subscription-based model where administrators create an easy-to-use interface and then recruit affiliates to deploy attacks. Affiliates of these groups identify targets and deploy malicious software, and then share a percentage of each ransom payment. Affiliates often use specialized teams for various steps in the ransomware process, including the laundering process. In other cases, affiliates can purchase data from other cyber criminals on darknet markets to gain unauthorized access to a victim's system.

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 or a family member to pay a ransom, for example, by stealing confidential data and threatening to publish the data. However, law enforcement identified that ransomware groups have learned that they can extract ransoms by only stealing data and forgoing encryption, which is often the first step of traditional ransomware attacks.

Ransomware criminals mainly demand payments in virtual assets and direct victims to send ransom payments to specified virtual asset wallet addresses. [113] These addresses can be held at a VASP.[114] Ransomware criminals may also use accounts belonging to money mules[115] or unhosted wallets.

111 Cybercrime is identified as an AML/CFT National Priority.

112 FBI, "Internet Crime Report", (March 2022), https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3Report.pdf.

113 FATF, "Countering Ransomware Financing", (March 14, 2023), https://www.fatf-gafi.org/en/publications/Methodsandtrends/countering-ransomware-financing.html.

114 See Virtual Assets Section.

115 See Money Mule Networks Section.

Ransomware criminals use various tools and methods, such as mixers or chain hopping, to hinder the ability of financial institutions or competent authorities to trace or attribute transactions. These criminals will use VASPs with weak AML/CFT controls, to exchange their illicit proceeds for fiat currency.[116] For example, in January 2023, under section 9714(a) of the Combating Russian Money Laundering Act, as amended by section 6106(b) of the NDAA for Fiscal Year 2022, FinCEN identified the VASP Bitzlato Limited (Bitzlato) as a "primary money laundering concern" in connection with Russian illicit finance, in part for its facilitation of illicit transactions for Russian ransomware actors. This order prohibits certain transmittals of funds involving Bitzlato by any covered financial institution.[117]

According to the DOJ, which concurrently announced charges against a Bitzlato senior executive for operating an unlicensed money transmitting business, Bitzlato allegedly received more than $15 million in ransomware proceeds.[118] Bitzlato allegedly became a haven for criminal proceeds and funds intended for use in criminal activity because of deficient AML/CFT controls. In other instances, ransomware proceeds have been converted into Chinese Renminbi (RMB) or sent to China-based money launderers.[119]

Ransomware attacks continue to frequently stem from jurisdictions with elevated sanctions risk or with ties to sanctioned persons, including Russia, the DPRK, and Iran.[120] Russia is a haven for ransomware actors, enabling cybercriminals to engage openly in ransomware attacks against U.S. organizations.[121] According to FinCEN analysis, 75 percent of ransomware-related incidents reported between July and December 2021 were linked to Russia, its proxies, or persons acting on its behalf. Additionally, the FBI reports that DPRK state-sponsored actors have deployed Maui ransomware against healthcare organizations to disrupt access to electronic health records.[122] The Office of Foreign Assets Control (OFAC) has also designated several entities responsible for perpetrating ransomware attacks, VASPs responsible for laundering ransomware payments, and cybercriminal groups responsible for developing and distributing ransomware, such as Evil Corp.[123]

The DOJ has also worked to prosecute individuals guilty of laundering the proceeds of ransomware attacks, including Bitzlato referenced above. Additionally, in February 2023, Denis Mihaqlovic Dubnikov,

116 See Virtual Assets Section, jurisdictional arbitrage.

117 FinCEN, "FinCEN Identifies Virtual Currency Exchange Bitzlato as a "Primary Money Laundering Concern" in Connection with Russian Illicit Finance", (January 18, 2023), https://www.fincen.gov/news/news-releases/fincen-identifies-virtual-currency-exchange-bitzlato-primary-money-laundering.

118 DOJ, "Founder and Majority Owner of Bitzlato, a Cryptocurrency Exchange, Charged with Unlicensed Money Transmitting", (January 18, 2023), https://www.justice.gov/usao-edny/pr/founder-and-majority-owner-bitzlato-cryptocurrency-exchange-charged-unlicensed-money.

119 DOJ, "Justice Department Seizes and Forfeits Approximately $500,000 from North Korean Ransomware Actors and their Conspirators", (July 19, 2022), https://www.justice.gov/opa/pr/justice-department-seizes-and-forfeits-approximately-500000-north-korean-ransomware-actors.

120 Treasury, "Treasury Sanctions IRGC-Affiliated Cyber Actors for Roles in Ransomware Activity," (September 14, 2022), https://home.treasury.gov/news/press-releases/jy0948; DOJ, "Three Iranian Nationals Charged With Engaging In Computer Intrusions And Ransomware-Style Extortion Against U.S. Critical Infrastructure Providers," (September 14, 2022), https://www.justice.gov/usao-nj/pr/three-iranian-nationals-charged-engaging-computer-intrusions-and-ransomware-style.

121 Treasury, "Treasury Sanctions Russian Ransomware Actor Complicit in Attacks on Police and U.S. Critical Infrastructure", (May 16, 2023), https://home.treasury.gov/news/press-releases/jy1486.

122 CISA, "North Korean State-Sponsored Cyber Actors Use Maui Ransomware to Target the Healthcare and Public Health Sector", (July 7, 2022), https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-187a.

123 Treasury, "Treasury Sanctions Evil Corp, the Russia-Based Cybercriminal Group Behind Dridex Malware", (December 5, 2019), https://home.treasury.gov/news/press-releases/sm845.

a Russian virtual asset money launderer, pleaded guilty to one count of conspiracy to commit money laundering. Dubnikov and his co-conspirators laundered the proceeds of Ryuk ransomware attacks on individuals and organizations throughout the United States and abroad. After receiving ransom payments, Ryuk actors, including Dubnikov, engaged in international financial transactions to conceal the nature, source, location, ownership, and control of the ransom proceeds.[124]

2. Malware

Ransomware actors and other cybercriminals often use malware to commit their crimes. Malware refers to software or code intended to damage or disable a computer or computer systems or destroy data. Malware can enable criminals' computer access to steal credentials, alter account information, and conduct fraudulent transactions. Criminals often deliver malware to victims through phishing emails, malicious websites and downloads (*e.g.,* via illicit streaming and digital privacy sites), domain name system hijacking, and fraudulent mobile applications. Law enforcement identified that cybercriminal groups using malware often take advantage of highly specialized, repurposing tools already installed on a victim's environment to gain access to their system for malicious purposes. Because these existing programs and tools can be used by a victim's legitimate network administrator, the malicious use of the tools can be more difficult to detect than traditional malware.

Cybercriminal groups continue to develop and sell malware via darknet markets and online forums, while others use the malware to harvest and monetize financial data and other PII on an industrial scale. Criminals can traffic the harvested data, such as banking passwords and login credentials, through marketplaces that specialize in the sale of compromised or stolen personal, financial, and banking information. Malicious actors can use this data to initiate unauthorized transfers from compromised bank accounts or to preform social engineering attacks against victims whose data was stolen.

Law enforcement has observed that cybercriminal groups using malware often launder funds using similar methods as ransomware actors. For example, in April 2023, the FBI announced a coordinated international operation against Genesis Market, a criminal online marketplace that advertised and sold packages of account access credentials that had been stolen from malware and infected computers around the world.[125] Since its inception in March 2018, Genesis Market has offered access to data stolen from over 1.5 million compromised computers worldwide containing over 80 million account access credentials. Genesis Market sold device "fingerprints," unique combinations of device identifiers and browser cookies that may be used to circumvent anti-fraud detection systems used by many websites. The combination of stolen access credentials, fingerprints, and cookies allowed purchasers to assume the victim's identity by tricking third-party websites into thinking the Genesis Market user was the actual owner of the account. OFAC concurrently designated Genesis Market as a specially designated national (SDN) under its cyber-related sanctions program.[126]

Additionally, in March 2023, the DOJ charged the founder of BreachForums for creating and administering

124 DOJ, "Russian Cryptocurrency Money Launderer Pleads Guilty", (February 7, 2023), https://www.justice.gov/usao-or/pr/russian-cryptocurrency-money-launderer-pleads-guilty.

125 DOJ, "Criminal Marketplace Disrupted in International Cyber Operation", (April 5, 2023), https://www.justice.gov/opa/pr/criminal-marketplace-disrupted-international-cyber-operation.

126 Treasury, "Treasury Sanctions Illicit Marketplace Genesis Market", (April 5, 2023), https://home.treasury.gov/news/press-releases/jy1388.

a major hacking forum and marketplace for cybercriminals.[127] The founder allegedly operated BreachForums as a marketplace for cybercriminals to buy, sell, and trade hacked or stolen data, harming millions of U.S. citizens and hundreds of U.S. and foreign companies, organizations, and government agencies. According to the complaint, the platform offered stolen data such as bank account information, social security numbers, other PII, hacking tools, breached databases, and account login information for compromised online accounts with service providers and merchants.

Professional Money Laundering

Professional money laundering encompasses individuals, organizations, and networks involved in third-party laundering for a fee or commission.[128] Although typically associated with laundering narcotics proceeds, many money laundering organizations (MLOs) do not discriminate among sources of the dirty money, laundering the proceeds from a variety of crimes, sometimes concurrently. This topic was first included in the 2022 NMLRA and we are continuing to focus on this key threat enabler, exploring in more depth those MLOs not previously covered. Therefore, this section will address new and emerging actors including PML services used by kleptocrats when trying to extract assets from the United States, the connected predicate offenses, and common methodologies.

There has been an increased use of professional enablers who facilitate the money laundering process by further obfuscating the source of the funds, such as through a network of shell, front and legitimate companies or the provision of supporting documentation. As noted in the Drug Trafficking Section, PML methods often involve using TBML techniques. For example, in Mexico, professional enablers include "factureros," whose sole job is to create false invoicing and billing for seemingly legitimate services never rendered and used to further obfuscate the money trail. A relevant case involves Ghacham Inc., a clothing wholesaler fined for customs fraud and violating U.S. drug trafficking sanctions. The company pleaded guilty in December 2022 to one count of conspiracy to pass false and fraudulent papers through a customhouse and one count of conspiracy to engage in any transaction or dealing in properties of a specially designated narcotics trafficker. Ghacham Inc. was ordered to pay financial penalties and ordered to create and maintain an AML/CFT compliance and ethics program.[129]

As noted earlier, drug cartels commonly employ MLOs. One 2022 OCDETF investigation involved a Tampa-based MLO responsible for laundering more than $21.5 million in drug proceeds. Spread out over 400 transactions, this MLO received the cash proceeds and then used the cash to purchase cashier's checks, visiting several banks in the same day to avoid suspicion. The couple purchased the cashier's checks themselves, on behalf of businesses they created, and recruited additional individuals to do so as well. According to the DOJ, the checks "were then remitted to various other individual and business accounts to receive, disguise, conceal, and distribute the drug trafficking proceeds." [130]

127 DOJ, "United States v. Conor Brian Fitzpatrick", (March 15, 2023), https://www.justice.gov/usao-edva/united-states-v-conor-brian-fitzpatrick.

128 PML can be categorized as (1) individuals, (2) groups or (3) networks. See FATF, *Professional Money Laundering*, pp. 12-13, (2018), https://www.fatf-gafi.org/en/publications/Methodsandtrends/Professional-money-laundering.html.

129 ICE, "HSI Los Angeles investigation ends with clothing wholesaler fined for customs fraud and violating U.S. drug trafficking sanctions,"(December 13, 2023), https://www.ice.gov/news/releases/hsi-los-angeles-investigation-ends-clothing-wholesaler-fined-customs-fraud-and.

130 DOJ, "Tampa Couple Sentenced In Multimillion Dollar Money Laundering Scheme", (October 24, 2022), https://www.justice.gov/usao-mdfl/pr/tampa-couple-sentenced-multimillion-dollar-money-laundering-scheme.

Another example of a professional launderer is Djonibek Rahmankulov, who was convicted of committing bank fraud as well as laundering the proceeds of fraud and hacking schemes. Rahmankulov was described as "laundering money for a living" for receiving proceeds from hacked bank accounts, COVID fraud, and Medicare and Medicaid fraud. Rahmankulov operated a network of shell companies and bank accounts and funded an unlicensed money transmitting business that illegally moved money to and from multiple countries, including Iran.[131] This reflects a broader trend in which MLOs have established unlicensed Money Service Businesses (MSBs) to facilitate their schemes.

1. Money Mule Networks

The role of money mules in facilitating cyber-enabled frauds and scams have been highlighted in both the 2018 and 2022 NMLRAs and this year's report is placing a special focus on these networks as a category of PMLs. Money mules are recruited by MLOs and are used to transfer value, either by laundering stolen money or physically transporting goods or other merchandise. Money mules may be witting or unwitting participants and are often recruited by criminals via job advertisements for 'transaction managers' or through online social media interactions. Money mule recruiters or directors are referred to as mule herders.[132] Money mules provide critical services to fraud syndicates by receiving money from fraud victims and forwarding the fraud proceeds to the perpetrators (many of whom are based overseas).

Some individuals first interact with herders as victims and may be unaware that their activity is furthering criminal activity. For example, these unwitting mules often have trust in the actual existence of their romance or job position. Other mules continue to operate after they have been warned by bank employees that they were involved in fraudulent activity or even after U.S. law enforcement informs them of their role in the criminal activity. These may be witting mules who are motivated by financial gain or an unwillingness to acknowledge their role. For example, one alleged mule opened 11 bank accounts at seven separate financial institutions and law enforcement informed that person that they were moving fraud proceeds between various bank accounts. Despite this warning, the alleged mule continued to receive more than $1.8 million into various bank accounts. These funds came directly from fraud victims who were deceived into sending the funds to bank accounts controlled by the alleged mule, rather than to the victims' intended recipients. After receiving this money, the alleged mule quickly withdrew or transferred it to various individuals or entities, including converting the funds into virtual assets.[133]

In addition to moving fraudulent proceeds, complicit mules are also used to create shell companies to open business bank accounts that can be used as part of the laundering process.[134] These complicit mules may advertise their services as a money mule (*e.g.,* on darknet marketplaces), to include what actions they offer (*e.g.,* recruiting other mules-see below) and at what prices. These mules are also

131 DOJ, "Queens Man Sentenced To 121 Months In Prison For Laundering Millions Of Dollars Of Fraud And Hacking Schemes And Committing Bank Fraud", (March 17, 2023), https://www.justice.gov/usao-sdny/pr/queens-man-sentenced-121-months-prison-laundering-millions-dollars-fraud-and-hacking#:~:text=Damian percent20Williams percent2C percent20the percent20United percent20States,Business percent20Administration percent20loan percent20fraud percent2C percent20as.

132 FBI, "Money Mules: Don't Be a Mule: Awareness Can Prevent Crime," https://www.fbi.gov/how-we-can-help-you/scams-and-safety/common-scams-and-crimes/money-mules.

133 DOJ, "Westminster Woman Charged in Federal Indictment Alleging She Acted as 'Money Mule' Who Laundered Funds for Cybercriminals", (February 16, 2023), https://www.justice.gov/usao-cdca/pr/westminster-woman-charged-federal-indictment-alleging-she-acted-money-mule-who.

134 DOJ, "Rhode Island Man Arrested and Charged with Laundering More than $35 Million in Fraud Proceeds and Obstruction of Justice", (February 23, 2023), https://www.justice.gov/usao-ma/pr/rhode-island-man-arrested-and-charged-laundering-more-35-million-fraud-proceeds-and.

motivated by financial gain but often are loyal to a known criminal group. Mule networks are also involved in IVTS described in the previous section. The illicit couriers will move the funds that are raised via fraud to a location which will facilitate the sale of the proceeds as part of IVTS transactions.

Managers and recruiters of money mule networks will recruit money mules to provide their PII in connection with the incorporation of sham businesses under the money mules' names. Under the instruction of these herders, money mules open bank accounts under the names of the sham corporations. Mule networks are often used to facilitate BEC scams (*see previous section on BEC scams*) and other on-line scams. For example, when the victims of these scams comply with the fraudulent wiring instructions, the money is quickly debited or transferred out of the bank account created under the mule's name but that the herder ultimately controls. Money is quickly transferred out via in-person and Automatic Teller Machine (ATM) withdrawals, debit card purchases often in thousands of dollars, or via wire from the bogus bank accounts to foreign bank accounts controlled by conspirators.[135]

Some criminal networks also utilize online forums, including online classifieds and Darknet forums, to advertise for and recruit cyber actors to establish sophisticated money laundering networks. For example, herders advertise their cash-out services to cyber actors in online forums and communicate with these actors on various messaging applications. After negotiating a portion of the cyber actors' stolen funds as fee for their services, the herders direct their money mules to transfer funds from victim accounts in the United States to drop accounts domestically and abroad.[136]

These groups use several techniques to recruit new mules to receive and transmit fraud proceeds. Victims may be asked to receive money or checks mailed to them or sent to their bank account for someone they have met over the phone or online. Victims may be asked to open a bank or cryptocurrency account at someone else's direction. Fraudsters will lie to persuade victims to help them. They may falsely tell victims that they are helping them get a lottery prize, initiate a purported romantic relationship, pretend to offer them a job, present an opportunity to invest in a business venture, or offer the chance to help in a charitable effort. In addition, according to law enforcement sources, the use of virtual businesses (*e.g.,* check depositing service) has the potential to be abused by having third-party deposit checks to funnel accounts on behalf of the criminals.

International students are particularly vulnerable to being recruited as money mules for a variety of reasons, including the allure of quick and easy money.[137] Mules are often targeted using social media, including messaging apps such as WeChat. Students may be told that they are providing money transmission services for other students, or that they are servicing unbanked Chinese citizens residing in the United States. They are asked to open bank accounts or tasked with collecting and depositing cash into banks on behalf of the CMLO. Some mules may even be asked to travel into or out of the United States carrying bulk cash or transport high value luxury items to China.

135 DOJ, "Recruiter and Director of Money Mule Sentenced to Two Years in Prison for Participation in Business Email Compromise Scheme", (March 24, 2023), https://www.justice.gov/usao-nj/pr/recruiter-and-director-money-mule-sentenced-two-years-prison-participation-business.

136 DOJ, "Ukrainian Nationals Plead Guilty to Financial Crimes", (July 12, 2022), https://www.justice.gov/usao-ndtx/pr/ukrainian-nationals-plead-guilty-financial-crimes#:~:text=Viktor percent20Vorontsov percent2C percent2040 percent2C percent20and percent20Zlata,wire percent20fraud percent2C percent20and percent20bank percent20fraud.

137 Barclays, "Barclays warns of 23 per cent surge in student money mules," (October 2, 2023), https://home.barclays/news/press-releases/2023/10/barclays-warns-of-23-per-cent-surge-in-student-money-mules/.

2. Chinese Money Laundering Organizations and Networks

CMLOs were addressed as a special focus topic in the 2022 NMLRA.[138] Since that time, law enforcement has reported that CMLOs have become more prevalent and are now one of the key actors laundering money professionally in the United States and around the globe.[139] CMLOs continue to work with other international MLOs, such as Colombian peso brokers, and are able to penetrate their competitor's markets given their lower fees and rapid pay-out options. This capability is due to their effective use of near real-time mirror transactions offsetting transfers of money which can handle large amounts of cash, overcome currency controls, and provide the rapid repatriation of proceeds. In addition, CMLOs have been known to offer to absorb losses due to providing guarantees on any funds delivered. By charging low fees and providing these guarantees, CMLOs are becoming one of the most significant money laundering threat actors facing the U.S. financial system.

CMLOs, like other types of MLOs, are not typically involved in the underlying crimes which generate proceeds (*e.g.,* drugs, human smuggling, and fraud) and operate in a very compartmentalized fashion. However, CMLOs are often associated with larger TCOs engaged in a wide array of criminal activity. Additionally, the CMLO cells will sometimes engage in low-level criminal activity to facilitate funds movement as part of their laundering scheme, including through the use of counterfeit identification or employing insiders to open bank or casino accounts. What makes these CMLOs effective is that they are insular and often decentralized, making them difficult to penetrate. They rely on a variety of interpersonal relationships working together to facilitate different aspects of the laundering cycle. According to law enforcement and open-source reporting, there appear to be a high number of CMLO members who originate from or have close ties to the Fujian Province in China.[140]

While CMLOs provide money laundering services for TCOs, their primary objective is to acquire and subsequently sell USD (and other foreign currencies) using IVTS schemes to Chinese nationals seeking to evade the Chinese government's currency controls.[141] CMLOs operating in the United States increasingly need access to significant amounts of USD to satisfy the demand for IVTS services by Chinese nationals. This is how they make most of their profits, setting them apart from other professional MLOs. Since the use of large sums of cash in the United States is uncommon and raises flags, CMLOs regularly source the USD they need from TCOs operating throughout the United States. This has created a symbiotic relationship between the two with each possessing what the other needs - CMLOs have a supercharged demand for USD, while TCOs need their ill-gotten gains laundered.

For example, CMLOs enable Mexican cartels to seamlessly exchange USD derived from the sale of narcotics for Mexican pesos.[142] Once the CMLO retrieves the criminal cash in the United States, a

138 Treasury, "National Money Laundering Risk Assessment", (February 2022), see pp.23-24.

139 HSI, "HSI, Australian Federal Police and partners, announce takedown of multi-million dollar Chinese money laundering syndicate," (October 26, 2023), https://www.ice.gov/news/releases/hsi-australian-federal-police-and-partners-announce-takedown-multi-million-dollar.

140 ProPublica, "Outlaw Alliance: How China and Chinese Mafias Overseas Protect Each Other's Interests", (July 12, 2023), https://www.propublica.org/article/how-beijing-chinese-mafia-europe-protect-interests.

141 In 2017, the Chinese State Administration of Foreign Exchange capped foreign exchange transfers at $50,000. *See* ICE, Cornerstone Report Issue #48, "Chinese Money Laundering Organizations (CMLOs) - Use of Counterfeit Chinese Passports," (January 2, 2024), https://content.govdelivery.com/bulletins/gd/USDHSICE-37fff16?wgt_ref=USDHSICE_WIDGET_217.

142 ICE, Cornerstone Report Issue #45, "Chinese Money Laundering," (October 5, 2023), https://content.govdelivery.com/bulletins/gd/USDHSICE-3714ed3?wgt_ref=USDHSICE_WIDGET_217.

comparable sum of Mexican pesos is then released – almost immediately and with nearly non-existent commission rates – to the cartel in Mexico using IVTS schemes (*e.g.,* mirror transactions). Dirty dollars remain in the United States, where at least in part, they are broken down into smaller amounts and deposited into U.S. bank accounts opened by money mules, which sometimes involve international students. This method, known as "smurfing," allows the cartels to avoid the risk and cost associated with attempting to smuggle bulk cash across our southern border. The CMLO then sells USD to Chinese nationals for a profit, who, in some instances, use the USDs to purchase real estate or even to pay college tuition expenses.

Unlike other MLOs, which transfer proceeds into and out of the country, a significant amount of the money laundered by CMLOs stays in the United States. Traditionally, CMLOs purchase criminal proceeds in U.S. cities for a nominal fee, transfer the equivalent value of foreign currency to drug traffickers' foreign bank accounts and then "sell" the drug proceeds at a substantially higher rate to Chinese nationals seeking to avoid China's currency controls. These organizations also exploit China's "one country, two systems" policy by using the more liberal banking system in Hong Kong to establish USD bank accounts to facilitate their schemes. These exchange transactions are not independent (*e.g.,* one-for-one) and often involve multiple individuals using multiple currencies. In an example of a scheme involving both IVTS and TBML methods, the CMLOs will receive RMB from Chinese customers who get USD in exchange, and they sell the RMBs to Mexican customers who need it to buy goods. The RMB (equivalent to the amount retrieved in the United States) is then transferred to the account of a CMLO associate in China and then used to fund the purchase of goods for export to source countries such as Mexico. Those goods are sold in Mexico to complete the IVTS scheme. The use of "off-the-books", or informal transactions, allows the CMLO to avoid U.S. reporting requirements and China's currency controls while also hiding the nature and source of the illicit funds being transferred.

SNAPSHOT: Schemes Involving Electronic Goods

A money laundering scheme used by CMLOs involves the procurement of high-value electronics (*e.g.,* smart phones, tablets, etc.) using illicit proceeds derived from drug trafficking, fraud and other criminal activities. Often, these electronics are fraudulently obtained. In some instances, the CMLOs will purchase these goods using stolen or fraudulent gift cards. The smart phones and other high-value electronics are subsequently exported from the United States to Hong Kong, China, Dubai, and other overseas locations where they are resold for a substantial profit. In an OCDETF investigation, tens of millions of dollars' worth of electronic devices were exported from the United States using this scheme. In another example, a registered owner of an electronics and restaurant supply business used their businesses to run a large-scale money laundering and money transmitting operation that involved the laundering of drug proceeds and proceeds from stolen or fraudulent gift cards.[143] These schemes permit CMLOs to significantly profit from the criminal proceeds they purchase.

143 DOJ, "Eight Indicted in Money Laundering Ring", (July 29, 2022), https://www.justice.gov/usao-ma/pr/eight-indicted-money-laundering-ring#:~:text=BOSTON percent20 percentE2 percent80 percent93 percent20Eight percent20individuals percent20have percent20been,used percent20stolen percent20and percent2For percent20fraudulent; Also see United States District Court (USDC), District of Massachusetts, U.S. v. ZANG, Case 1:22-cr-10185.

3. Special Focus: Russian Money Laundering and Sanctions Evasion

Professional money laundering linked to Russia is a significant threat to the national security of the United States because it conceals and facilitates illicit activity on the part of oligarchs and the government of Russia, enables the Kremlin's damaging foreign policy goals, and undermines U.S. national interests.[144] Russian efforts to evade sanctions present a similar threat; the act of circumventing or otherwise avoiding sanctions adversely impacts the United States' ability to disrupt, deter, and prevent actions that undermine U.S. national security and the U.S. financial system.[145] There have been several recent FinCEN and U.S. Department of Commerce's Bureau of Industry and Security (BIS) alerts on Russian sanctions and export control evasion.[146]

Russian and Russia-linked actors, especially oligarchs, involved in money laundering and sanctions evasion activity maintain vast global networks of shell companies, bank accounts, trusts, and other means of hiding and moving funds abroad, including the United States.[147] Notably, these vast networks intentionally span multiple jurisdictions and enable these bad actors to maintain control, obfuscate their ill-gotten gains and assist the Kremlin in its illicit financial activities abroad.

Russian money laundering and sanctions violation activity may involve professional facilitators and enablers who leverage their position in the international financial system to help SDNs. Recent criminal indictments indicate that lawyers may be especially helpful to designated persons, given their professional stature as well as financial tools such as Interest on Lawyers' Trust Accounts (IOLTAs) which can be misused to legitimize payments and draw scrutiny away from designated persons or other facilitators.[148] Investment advisers, trust and company service providers (TCSPs), and other financial proxies and intermediaries may also assist sanctioned Russian actors in accessing their funds, including through the U.S. financial system.[149] Finally, the Russian government has directed its intelligence services to set up complex transnational evasion networks abroad, leveraging front companies to funnel money while attempting to maintain a lawful appearance. Russian actors have sought to exploit and abuse

144 Treasury, "NDAA Russia Illicit Finance Report", (March 2023), https://home.treasury.gov/system/files/136/Treasury-NDAA-Ru-IFR-508.pdf.

145 Treasury, "The Treasury 2021 Sanctions Review", (October 2021), https://home.treasury.gov/system/files/136/Treasury-2021-sanctions-review.pdf.

146 FinCEN, "FinCEN Advises Increased Vigilance for Potential Russian Sanctions Evasion Attempts," (March 7, 2022), https://www.fincen.gov/sites/default/files/2022-03/FinCEN%20Alert%20Russian%20Sanctions%20Evasion%20FINAL%20508.pdf, FinCEN, "Supplemental Alert: FinCEN and the U.S. Department of Commerce's Bureau of Industry and Security Urge Continued Vigilance for Potential Russian Export Control Evasion Attempts," (May 19, 2023), https://www.fincen.gov/sites/default/files/shared/FinCEN%20and%20BIS%20Joint%20Alert%20_FINAL_508C.pdf; FinCEN, "FinCEN Alert on Potential U.S. Commercial Real Estate Investments by Sanctioned Russian Elites, Oligarchs, and Their Proxies," (January 25, 2023), https://fincen.gov/sites/default/files/shared/FinCEN%20Alert%20Real%20Estate%20FINAL%20508_1-25-23%20FINAL%20FINAL.pdf.

147 FinCEN, "Trends in Bank Secrecy Act Data: Financial Activity by Russian Oligarchs in 2022", https://www.fincen.gov/sites/default/files/2022-12/Financial percent20Trend percent20Analysis_Russian percent20Oligarchs percent20FTA percent20_Final.pdf.

148 DOJ, "New York Attorney Pleads Guilty To Conspiring To Commit Money Laundering To Promote Sanctions Violations By Associate Of Sanctioned Russian Oligarch", (April 25, 2023), https://www.justice.gov/usao-sdny/pr/new-york-attorney-pleads-guilty-conspiring-commit-money-laundering-promote-sanctions.

149 FinCEN Alert, FIN-2023-Alert002, *FinCEN Alert on Potential U.S. Commercial Real Estate Investments by Sanctioned Russian Elites, Oligarchs, and Their Proxies*, p.4 (Jan. 25, 2023). In addition, on September 19, 2023, the SEC announced charges against Concord Management LLC and its owner and principal, Michael Matlin, for operating as unregistered investment advisers to their only client—a wealthy former Russian official widely regarded as having political connections to the Russian Federation. SEC, Press Release 2023-186, *SEC Charges New York Firm Concord Management and Owner with Acting as Unregistered Investment Advisers to Billionaire Former Russian Official* (Sep. 19, 2023).

otherwise legitimate economic relationships in third countries such as Türkiye, Singapore, the United Arab Emirates, Armenia, Kyrgyzstan, Uzbekistan, PRC, and others to violate U.S. restrictions.

In May of 2022, OFAC identified accounting, trust and corporate formation, and management consulting as categories of services prohibited from sale or export from the United States to Russia, highlighting the role that TCSPs and similar companies play in assisting wealthy Russians and Russian companies with setting up shell companies and hiding their assets.[150] In 2022 and 2023, FinCEN and the BIS issued two joint alerts for financial institutions on Russian sanctions evasion, providing key information on evasion red flags and illicit activity typologies, including Russia's increasing use of traditional money laundering tactics such as the use of corporate vehicles, shell companies, new company formations, nominee directors, and non-routine foreign exchange transactions.[151] Enhanced U.S. visibility into the financial networks of Russian proliferators, shell companies, and fronts has predicated new investigations and bolstered existing ones, resulting in detentions and seizures of unauthorized exports. In addition, the Russian Elites, Proxies, and Oligarchs (REPO) Task Force has assessed that financial institutions and other entities' compliance with both sanctions and anti-money laundering regulations have helped identify and immobilize assets subject to sanctions.

Corruption[152]

Corruption involves the abuse of power for private gain by public officials exploiting positions of power and public trust and by private individuals or entities aiming to improperly secure influence, enrichment, or preferential treatment. Corrupt politically exposed persons (PEPs) [153] embezzle public funds, receive bribes and kickbacks, and misappropriate wealth. In contrast, corrupt private entities may improperly seek to control government decision-making in the form of improperly awarded concessions or contracts.[154] PEPs should not be confused with the term "senior foreign political figure" as defined under the BSA private banking regulation, a subset of PEPs. PEPs may present a higher risk for foreign public corruption than other customers, due to their potential access to and influence over public assets.[155] The term PEPs also refers to the immediate family members or close associates of individuals holding public functions, reflecting corrupt actors' regular use of third-party individuals and "proxies" in laundering

150 U.S. Department of the Treasury, "U.S. Treasury Takes Sweeping Action Against Russia's War Efforts, (May 8, 2022), https://home.treasury.gov/news/press-releases/jy0771.

151 FinCEN, "FinCEN and the Bureau of Industry and Security (BIS) Issue Joint Notice and New Key Term for Reporting Evasion of U.S. Export Controls Globally," (November 06, 2023), https://www.fincen.gov/news/news-releases/fincen-and-bureau-industry-and-security-bis-issue-joint-notice-and-new-key-term; FinCEN, "FinCEN and the U.S. Department of Commerce's Bureau of Industry and Security Urge Increased Vigilance for Potential Russian and Belarusian Export Control Evasion Attempts," FIN-2022-Alert003, (June 28, 2022), https://www.fincen.gov/sites/default/files/2022-06/FinCEN percent20and percent20Bis percent20Joint percent20Alert percent20FINAL.pdf.

152 The U.S. Strategy on Countering Corruption (2021), National Strategy for Combating Terrorist and Other Illicit Financing (2022), and AML/CFT National Priorities identify countering corruption as a priority for the United States.

153 Foreign individuals who are or have been entrusted with a prominent public function, as well as their immediate family members and close associates, See "Joint Statement on Bank Secrecy Act Due Diligence Requirements for Customers Who May Be Considered Politically Exposed Persons", (August 21, 2020), https://www.fincen.gov/sites/default/files/shared/PEP percent20Interagency percent20Statement_FINAL percent20508.pdf.

154 The White house, "United States Strategy on Countering Corruption," (December 2021), p.6., https://www.whitehouse.gov/wp-content/uploads/2021/12/United-States-Strategy-on-Countering-Corruption.pdf.

155 FFIEC, "Politically Exposed Persons," (November 2021), https://www.ffiec.gov/press/PDF/Politically-Exposed-Persons.pdf.

illicit proceeds.[156] Banks must apply a risk-based approach to customer due diligence (CDD) in developing the risk profiles of their customers, including PEPs. They are required to establish and maintain written procedures reasonably designed to identify and verify beneficial owners of legal entity customers.[157]

These activities generate illicit proceeds, often taking the form of bribes, kickbacks, embezzled or misappropriated assets, or funds received as part of improperly awarded concessions or contracts. These illicit proceeds may be laundered, stored, or moved through the U.S. financial system. Money laundering methods commonly associated with corruption and kleptocracy include the misuse of legal entities and offshore financial accounts; the purchase of real estate, luxury goods, and other high-value assets (including yachts, aircraft, and art); the misuse of certain professions and sectors, such as investment advisers, lawyers, and trust and company service providers; and the reliance on MLOs.[158] Law enforcement also reports an increasing number of corruption-related cases involving the use of digital assets, though the overall number of these cases remains small relative to corruption involving fiat currency.[159]

Corruption results in considerable costs to society depriving governments of essential resources, weakening the business environment, eroding good governance and the rule of law, inhibiting equity and economic growth, and exacerbating other threats like organized crime and drug trafficking.[160] Consequently, in 2021 President Joseph Biden established the fight against corruption as a core U.S. national security interest.[161]

These money laundering risks relate to both domestic and foreign corruption. In the United States, some government officials at the local, state, tribal, and federal levels may engage in corrupt practices. Foreign actors also launder the proceeds of corruption through the movement or investment of funds in the U.S. economy and financial system. Given the size and stability of the U.S. financial system, the United States remains a significant money laundering destination for the proceeds of corruption. Further, U.S. efforts to combat corruption in the past few years have led to an increased focus and fuller understanding of the problem as illustrated in the many typology examples below.

1. Foreign Corruption

Money laundering tied to foreign corruption primarily involves payments to foreign officials to obtain or retain business, as well as the use of the U.S. financial system to launder the proceeds of corruption. The

156 FinCEN, "FinCEN Alert on Real Estate, Luxury Goods, and Other High-Value Assets Involving Russian Elites, Oligarchs, and their Family Members," (March 16, 2022), https://www.fincen.gov/sites/default/files/2022-03/FinCEN percent20Alert percent20Russian percent20Elites percent20High percent20Value percent20Assets_508 percent20FINAL.pdf.

157 "Joint Statement on Bank Secrecy Act Due Diligence Requirements for Customers Who May Be Considered Politically Exposed Persons," (August 21, 2020), https://www.fincen.gov/sites/default/files/shared/PEP%20Interagency%20Statement_FINAL%20508.pdf.

158 FinCEN, "Advisory on Kleptocracy and Foreign Public Corruption," (April 2022), https://www.fincen.gov/sites/default/files/advisory/2022-04-14/FinCEN percent20Advisory percent20Corruption percent20FINAL percent20508.pdf.

159 DOJ, "Bankman-Fried Charged in an Eight-Count Indictment with Fraud, Money Laundering, and Campaign Finance Offenses", (December 13, 2022), https://www.justice.gov/usao-sdny/pr/united-states-attorney-announces-charges-against-ftx-founder-samuel-bankman-fried.

160 The White house, "United States Strategy on Countering Corruption," (December 2021), p.6., https://www.whitehouse.gov/wp-content/uploads/2021/12/United-States-Strategy-on-Countering-Corruption.pdf.

161 The White House, "Memorandum on Establishing the Fight Against Corruption as a Core United States National Security Interest," (June 3, 2021), https://www.whitehouse.gov/briefing-room/presidential-actions/2021/06/03/memorandum-on-establishing-the-fight-against-corruption-as-a-core-united-states-national-security-interest/. Corruption is a national AML/CFT priority.

United States is being used to hide the proceeds of foreign offenses given the size and stability of our financial sector. U.S. law enforcement regularly investigates and prosecutes illicit activities involving extortion, bribery, and misappropriation or embezzlement of public assets by or for the benefit of a public foreign official where the U.S. financial system and markets are misused to disguise or shelter illicit proceeds.

As described in FinCEN's 2022 Advisory on Kleptocracy and Foreign Public Corruption, corruption can occur at any level of government and commonly involves the use of shell companies and offshore financial accounts to move its proceeds; the purchase of real estate, luxury goods, and other high-value assets; long-term government contracts or procurement processes; transactions with state-owned companies, public institutions, or embassies; and exploitation of natural resources or commodities.[162]

Foreign corruption cases involve a range of predicate crimes and money laundering techniques. In April 2023 a federal jury convicted Claudia Patricia Díaz Guillen, the former National Treasurer of Venezuela, and her husband, Adrian José Velásquez, for their roles in an international currency exchange scheme.[163] The scheme involved accepting more than $100 million in bribes, using BCS, offshore shell companies, wire transfers from Swiss bank accounts to accounts in Southern Florida, and purchasing high-value luxury goods in Florida.[164] In another case in 2022, the DOJ filed a civil forfeiture complaint alleging that an Armenian businessperson purchased a high-value mansion in Los Angeles with bribes in excess of $20 million for a former high-ranking Armenian public official and his family in exchange for favorable tax treatment.[165] In 2023, a defendant pleaded guilty to laundering funds embezzled from the health office of the Embassy of Kuwait in Washington, DC. The scheme involved the creation of shell companies with names meant to mimic actual U.S. healthcare providers and the submission of more than $1.5 million in fraudulent invoices to the Embassy's health office.[166]

2. Domestic Corruption

Domestic corruption cases most often involve bribery and subsequent efforts to launder or disguise bribes paid to, solicited by, or received by U.S. public officials. Other prosecutable offenses commonly associated with domestic corruption, such as the misappropriation or embezzlement of public assets, fraud (especially relating to contracting and procurement), election and campaign finance crimes, the solicitation or receiving of kickbacks, and tax evasion, also remain risks.[167] These activities occur at the federal, state, local, and tribal levels, and have involved a range of individuals, including law enforcement

162 FinCEN, "Advisory on Kleptocracy and Foreign Public Corruption," (April 2022), https://www.fincen.gov/sites/default/files/advisory/2022-04-14/FinCEN percent20Advisory percent20Corruption percent20FINAL percent20508.pdf.

163 DOJ, "Former Venezuelan National Treasurer and Husband Sentenced in Money Laundering and International Bribery Scheme," (December 15, 2022), https://www.justice.gov/opa/pr/former-venezuelan-national-treasurer-and-her-husband-sentenced-money-laundering-and.

164 See Southern District of Florida, USA vs. Raul Gorrin Belisario Claudia Patricia Diaz Guillen, andAdrian Jose Velasquez Figueroa, Case 18-cr-80160, superseding indictment.

165 DOJ, "Justice Department Seeks Forfeiture of Los Angeles Mega-Mansion Purchased with Proceeds of Armenian Corruption Scheme," (May 5, 2022), https://www.justice.gov/opa/pr/justice-department-seeks-forfeiture-los-angeles-mega-mansion-purchased-proceeds-armenian.

166 DOJ, "Former Fugitive Pleads Guilty to Laundering Money Embezzled from Kuwaiti Embassy," (May 16, 2023), https://www.justice.gov/opa/pr/former-fugitive-pleads-guilty-laundering-money-embezzled-kuwaiti-embassy; DOJ, "Defendant Returned by Egypt to the United States to Face Charges for Alleged Scheme to Defraud the Kuwaiti Embassy," (December 23, 2021), https://www.justice.gov/opa/pr/defendant-returned-egypt-united-states-face-charges-alleged-scheme-defraud-kuwaiti-embassy.

167 DOJ, "Report to Congress on the Activities and Operations of the Public Integrity Section for 2021," (2021), https://www.justice.gov/criminal-pin/file/1548051/download; DOJ, "Former Puerto Rico Legislator Sentenced for Bribery and Kickback Scheme," (September 7, 2022), https://www.justice.gov/opa/pr/former-puerto-rico-legislator-sentenced-bribery-and-kickback-scheme.

officers, political consultants and campaign employees, contractors, officials engaged in procurement, elected leaders, and members of the judiciary.[168]

Money laundering activity has been a key component of many domestic corruption cases. For example, a March 2022 case involved Alderman Ricardo Munoz, a former elected city official sentenced on federal wire fraud and money laundering charges for using money from a political fund to pay for personal expenses.[169] While serving in office, Munoz used money from a political action committee to pay a relative's college tuition and other personal expenses, and sought to conceal this fraud scheme by making materially false representations to the State elections board.[170] In another 2022 case, a former elected State Representative and an associated staff member were charged with theft from programs receiving federal funds, engaging in bribery and kickbacks concerning programs receiving federal funds, honest services wire fraud, and conspiracy to commit money laundering.[171] It is alleged that the two individuals sought State funds by using a fictitious name and submitting sham invoices to the State from companies the two individuals owned.[172]

3. Special Focus: Unlawful Campaign Finance

Over the past ten years, here have been numerous instances of money laundering occurring in and around domestic political campaigns for federal, state, and local office. When domestic and foreign actors carry out these activities, it undermines the integrity of democratic processes in the United States, erodes institutions, and may afford corrupt or illicit actors unfair political advantages.[173] Domestic and foreign actors have engaged in money laundering to leverage campaign funds for personal use and to obfuscate campaign fundraising efforts (often to conceal the identity of donors or to obstruct campaign finance disclosures). These activities may be perpetrated by political candidates and their campaigns, foreign governments seeking strategic gain, or political supporters aiming to bypass campaign finance law, among others.

Campaign finance-related money laundering may involve a range of techniques, depending on the kind of illicit actors perpetrating the scheme and their respective political, financial, or strategic objectives. Recent cases and law enforcement reports suggest that campaign invoices, business and consulting contracts, donations to nonprofits, and standard business transactions are common methods through which illicit actors carry out campaign finance fraud.

168 DOJ, "Military Contractors Convicted for $7 Million Procurement Fraud Scheme," (March 29, 2023), https://www.justice.gov/opa/pr/military-contractors-convicted-7-million-procurement-fraud-scheme; DOJ, "Former Judge Arrested for Bribery and Obstruction of Justice," (January 5, 2023), DOJ, "Former Arkansas State Senator Sentenced for Bribery and Tax Fraud," (February 3, 2023), https://www.justice.gov/opa/pr/former-arkansas-state-senator-sentenced-bribery-and-tax-fraud; https://www.justice.gov/opa/pr/former-judge-arrested-bribery-and-obstruction-justice.

169 USAO, "Former City of Chicago Alderman Sentenced to More Than a Year in Federal Prison for Using Political Funds To Pay Personal Expenses," (March 17, 2022), https://www.justice.gov/usao-ndil/pr/former-city-chicago-alderman-sentenced-more-year-federal-prison-using-political-funds.

170 Id.

171 DOJ, "Tennessee State Representative and Former Chief of Staff Charged with Bribery and Kickback Conspiracy," (August 23, 2022), https://www.justice.gov/opa/pr/tennessee-state-representative-and-former-chief-staff-charged-bribery-and-kickback-conspiracy.

172 Id.

173 The White House, "United States Strategy on Countering Corruption," (December 2021), p.7, https://www.whitehouse.gov/wp-content/uploads/2021/12/United-States-Strategy-on-Countering-Corruption.pdf.

In 2023, Jessie R. Benton was convicted for his role in funneling illegal foreign campaign contributions from a Russian national to a 2016 U.S. presidential campaign.[174] The scheme entailed Benton's political firm creating a fake invoice for consulting services, the Russian national wiring $100,000 to the firm, and Benton acting as a straw donor by contributing $25,000 to the campaign.[175] The campaign then unwittingly filed reports with the Federal Election Commission inaccurately reporting the U.S. individual, instead of the Russian national, as the source of the funds.[176]

In July 2022, two U.S. citizens were charged with money laundering conspiracy, among other offenses, for a scheme in which they allegedly acted as "straw donors" for foreign nationals to unlawfully contribute to political campaigns.[177] The two individuals allegedly received funds from foreign nationals and gave $600,000 to political campaigns in their own names in violation of Federal Election Commission regulations.[178]

Human Trafficking & Human Smuggling

Human trafficking and human smuggling networks pose a serious criminal threat with devastating human consequences. [179] Human traffickers jeopardize the fundamental human right to personal freedom as criminals seek to profit from forced labor or sexual servitude. Human smugglers frequently place migrants in grave danger in the service of extreme profits. While human trafficking and human smuggling are distinct crimes, individuals who are smuggled are also vulnerable to becoming victims of human trafficking and other serious crimes.

Both crimes generate large profits that may be laundered through the U.S. financial systems. Human trafficking and human smuggling criminal networks use a variety of mechanisms to move illicit proceeds generated by these two crimes, expanding their profits and threatening the integrity of the U.S. financial system. They employ purchases of real estate, wire transfers, credit cards, and bulk cash transfers, among others. Increasingly, virtual assets have facilitated both types of criminal activities.

1. Human Trafficking

Human trafficking is a financially motivated crime whereby traffickers exploit victims by compelling or coercing them to perform labor or services or engage in commercial sex. Human trafficking victims in the United States may be U.S. citizens, foreign nationals who have lawful immigration status, or individuals who are unlawfully present. Victims of human trafficking may likewise come from any socioeconomic group, though significant risk factors may include recent migration, substance use, mental health

174 DOJ, "Political Consultant Convicted for Scheme Involving Foreign Campaign Contribution to 2016 Presidential Campaign," (November 17, 2022), https://www.justice.gov/opa/pr/political-consultant-convicted-scheme-involving-illegal-foreign-campaign-contribution-2016.

175 Id.

176 Id.

177 DOJ, "Oyster Bay Residents Charged with $27 Million Investment Fraud Scheme and Selling Foreign Nationals Access to Prominent U.S. Politicians," (July 18, 2022), https://www.justice.gov/usao-edny/pr/oyster-bay-residents-charged-27-million-investment-fraud-scheme-and-selling-foreign.

178 Id.

179 Human trafficking and human smuggling are identified as an AML/CFT National Priority.

concerns, or involvement with the child welfare system or youth homelessness.[180] Sex trafficking is often facilitated through online social media platforms.[181]

Beyond its enormous human costs, human trafficking is one of the most profitable crimes and predicate offenses for money laundering.[182] While an underreported crime, between January 1, 2020 and August 31, 2022, a total of 26,872 situations of human trafficking were reported to the U.S. National Human Trafficking Hotline involving 42,887 likely victims.[183] An estimated 30 million people are subjected to human trafficking across the world.[184] Estimates suggest that human trafficking generates more than $150 billion in global illicit profits annually.[185]

Financial activity from human trafficking can intersect with the regulated financial system at any point during the recruitment, transportation, and exploitation stages. Transactions related to human trafficking can include payments associated with the transport and housing of victims; the collection of proceeds generated by the exploitation of trafficking victims; and the movement of proceeds.[186] TCOs may make financial investments to facilitate human trafficking-related activities, such as investing in real estate, bars, restaurants, or other businesses to conceal their trafficking-related activities.[187] Companies that appear legitimate may be used to launder money to support human trafficking.

Illicit proceeds from human trafficking can be paid or transferred in cash, electronic funds transfers/

180 National Human Trafficking Hotline, "Human Trafficking: Who is Vulnerable?" https://humantraffickinghotline.org/en/human-trafficking#:~:text=Who percent20is percent20Vulnerable percent3F,a percent20runaway percent20or percent20homeless percent20youth.

181 DOJ, "Kansas Man Convicted for Sex Trafficking in Oklahoma", (August 3, 2023), https://www.justice.gov/usao-ndok/pr/kansas-man-convicted-sex-trafficking-oklahoma; DOJ, "Jamestown Woman Pleads Guilty To Her Role In Sex Trafficking Conspiracy", (August 17, 2023) https://www.justice.gov/usao-wdny/pr/jamestown-woman-pleads-guilty-her-role-sex-trafficking-conspiracy; DOJ, "Marion County Man Convicted of Human Trafficking," (August 23, 2023), https://www.justice.gov/usao-edtx/pr/marion-county-man-convicted-human-trafficking.

182 State, Treasury, "Report to Congress on An Analysis of Anti-Money Laundering Efforts Related to Human trafficking", (October 7, 2020), https://www.state.gov/report-to-congress-on-an-analysis-of-anti-money-laundering-efforts-related-to-human-trafficking/.

183 Polaris, "The Typology of Modern Slavery", (August 30, 2023), https://polarisproject.org/the-typology-of-modern-slavery/

184 DHS, "Countering Human Trafficking: A Year in Review", (January 2023), https://www.dhs.gov/sites/default/files/2023-05/23_0131_CCHT_year-in-review_revised-23_0509.pdf; Department of State, "About Human Trafficking," https://www.state.gov/humantrafficking-about-human-trafficking/#:~:text=With%20an%20estimated%2027.6%20million,them%20for%20their%20own%20profit.

185 The White House, "FACT SHEET: The National Action Plan to Combat Human Trafficking (NAP)" (December 3, 2021), https://www.whitehouse.gov/briefing-room/statements-releases/2021/12/03/fact-sheet-the-national-action-plan-to-combat-human-trafficking-nap/#:~:text=December percent2003 percent2C percent202021-,FACT percent20SHEET percent3A percent20The percent20National percent20Action,to percent20Combat percent20Human percent20Trafficking percent20(NAP)&text=Globally percent2C percent20an percent20estimated percent2025 percent20million,billion percent20annually percent20in percent20illicit percent20profits. The actual value of proceeds from human trafficking is likely to be much higher. In 2014, an International Labour Office study found that forced labor generates approximately $150 billion in proceeds annually. Since that time, the number of persons understood to be victims of human trafficking has increased by nearly 50 percent. International Labour Office, 2014, Profits and Poverty: The Economics of Forced Labour, https://www.ilo.org/wcmsp5/groups/public/---ed_norm/---declaration/documents/publication/wcms_243391.pdf, page 13.

186 FinCEN, "Supplemental Advisory on Identifying and Reporting Human Trafficking and Related Activity", FIN2020-A008, (October 15, 2020,) https://www.fincen.gov/sites/default/files/advisory/2020-10-15/Advisory percent20Human percent20Trafficking percent20508 percent20FINAL_0.pdf; FinCEN, "Advisory *Guidance Recognizing Activity that May be Associated with Human Smuggling and Human Trafficking*", FIN2014-A008, (September 11, 2014), https://www.fincen.gov/sites/default/files/advisory/FIN-2014-A008.pdf; FinCEN, "FinCEN Alert on Huma Smuggling along the Southwest Border of the United States", FIN2023-Alert001, (January 13, 2023), https://www.fincen.gov/sites/default/files/shared/FinCEN percent20Alert percent20Human percent20Smuggling percent20FINAL_508.pdf.

187 FinCEN, "Supplemental Advisory on Identifying and Reporting Human Trafficking and Related Activity", FIN2020-A008, (October 15, 2020,) https://www.fincen.gov/sites/default/files/advisory/2020-10-15/Advisory percent20Human percent20Trafficking percent20508 percent20FINAL_0.pdf.

remittance systems, credit card transactions, payment apps, or virtual assets.

In the United States, human trafficking occurs in a broad range of industries, including hospitality, agriculture, healthcare, manufacturing, commercial cleaning services, construction, peddling and begging, food service industries, beauty salon services, domestic work, fairs and carnivals, escort services, illicit massage, and health and beauty services.[188]

The DOJ regularly prosecutes money laundering with predicate human trafficking offenses.[189] For example, a TCO conspired to make money by compelling hundreds of women from Thailand to engage in commercial sex acts in various cities across the United States. The DOJ pursued prosecutions against the TCO that have resulted in 37 convictions.[190] Sumalee Intarathong pleaded guilty to her role as a visa broker for the TCO, which controlled victims until they could repay an exorbitant "bondage debt" of between $40,000 and $60,000.[191] The TCO dealt primarily in cash and engaged in rampant and sophisticated money laundering to promote and conceal illegal profits. The TCO generated profits in the United States and then used funnel accounts, third-party money launderers, and BCS to transport proceeds. To evade detection, the trafficking organization paid flight attendants to keep quiet and, in some limited instances, to transport bulk cash in their own luggage. Transactions related to the human trafficking scheme in the United States were made using prepaid credit cards and virtual assets.[192] The TCO moved tens of millions of dollars in illegal proceeds from the United States to Thailand and elsewhere.

In another case, Peter Griffin, a retired San Diego Police Department vice detective, owned a network of illicit massage businesses (IMBs) in Southern California and Arizona. Through the course of Griffin's criminal operation, he established several bank accounts for his IMBs, which Griffin and his co-conspirators regularly used to collect payments for the commercial sex services they instructed women to perform inside the businesses. Griffin then used these accounts to pay for online commercial sex advertisements and other business expenses. On three separate occasions, Griffin knowingly used the bank accounts associated with his illicit and illegal businesses to purchase a Cartier watch and a car and issued a cashier's check payable to one of his codefendants. Griffin was sentenced on October 13, 2023, to 33 months in custody.[193]

188 Polaris, "The Typology of Modern Slavery", (August 30, 2023), https://polarisproject.org/the-typology-of-modern-slavery/.

189 *See* Sec. II.E of *Attorney Generals' Annual Report to Congress on U.S. Government Activities to Combat Trafficking in Persons* (FY2021), *available at* Attorney General's Annual Report to Congress on U.S. Government Activities to Combat Trafficking in Persons, Fiscal Year 2021 (justice.gov).

190 DOJ, "Thai Woman Pleads Guilty to Her Role in International Sex Trafficking Conspiracy", (November 29, 2022), https://www.justice.gov/usao-mn/pr/thai-woman-pleads-guilty-her-role-international-sex-trafficking-conspiracy.

191 Id.

192 FinCEN, "Supplemental Advisory on Identifying and Reporting Human Trafficking and Related Activity", FIN2020-A008, (October 15, 2020).

193 DOJ, "Former San Diego Police Officer and Three Others Plead Sentenced from Years-long Operation of Illicit Massage Businesses, (Oct. 13, 2023), https://www.justice.gov/usao-sdca/pr/former-san-diego-police-officer-and-three-others-sentenced-crimes-stemming-years-long.

2. Human Smuggling

Human smugglers engage in bringing people, who have consented to their travel, across international borders through deliberate evasion of immigration laws, often for financial benefit. Human smuggling is an inherently transnational crime, with smuggling routes across the southwest border remaining the most popular for entry into the United States. In recent years, law enforcement has witnessed an increase in the number of women, children, and families seeking transportation by human smugglers.[194] Human smuggling networks are lucrative, and Illicit financial networks of criminals who profit off vulnerable migrants can command smuggling fees ranging from $5,000 up to tens of thousands of dollars per migrant.[195] Moving human beings as cargo pays billions of dollars for transnational criminal smuggling organizations and involves significant risk to the people involved.[196] TCOs that control drug smuggling territory also profit from this illegal activity by charging smuggling organizations a fee or tax to pass through their territories. According to HSI, Human smuggling also represents a national security concern, as identified instances of known or suspected terrorists attempting to infiltrate the United States through illegal migration have occurred.

In one recent criminal indictment, the DOJ alleged that a human smuggling organization had generated millions of dollars in proceeds.[197] The defendant and co-conspirators allegedly employed various methods to conceal the nature, location, source, ownership, and control of the proceeds of the organization, including the use of funnel accounts; investing in property and luxury goods; amassing large amounts of cash to avoid bank reporting requirements; and moving illicit proceeds between accounts, among other methods.

In another case, Homeland Security Investigations (HSI) announced the arrest of six alleged human smugglers in a coordinated, multistate enforcement operation.[198] In this case, the DOJ is prosecuting members of a TCO that allegedly used funnel accounts and directed electronic money transfers to avoid detection, including by making payments for funds derived from the TCO's alien smuggling activity through peer-to-peer money transfer applications to coconspirators. Other members of the TCO are alleged to have been involved in moving money through funnel accounts and electronic money transfers on behalf of the organization.

194 ICE, Features, "Human Smuggling equals grave danger, big money", (Jan. 26, 2022), https://www.ice.gov/features/human-smuggling-danger.

195 ICE, "HSI San Diego, BP case results in migrant smuggler admitting to sexually assaulting a juvenile while being smuggled into the US," (Nov. 6, 2023) https://www.ice.gov/news/releases/hsi-san-diego-bp-case-results-migrant-smuggler-admitting-sexually-assaulting-juvenile; DOJ, "Four Defendants Extradited from Guatemala Sentenced for Roles in Deadly International Human Smuggling Conspiracy," (Nov. 1, 2023) Office of Public Affairs | Four Defendants Extradited from Guatemala Sentenced for Roles in Deadly International Human Smuggling Conspiracy | United States Department of Justice.

196 ICE, Features, "Human Smuggling equals grave danger, big money", (Jan. 26, 2022), https://www.ice.gov/features/human-smuggling-danger.

197 DOJ, "Four Indicted for Money Laundering in Prolific Human Smuggling Network Takedown", (July 28, 2023), https://www.justice.gov/opa/pr/four-indicted-money-laundering-prolific-human-smuggling-network-takedown.

198 DOJ, "Ten Indicted and Six Arrested in Joint Task Force Alpha Investigation of the Lopez Crime Family Human Smuggling Organization Operating in Guatemala, Mexico, and the United States," (June 15, 2023), https://www.justice.gov/usao-nm/pr/ten-indicted-and-six-arrested-joint-task-force-alpha-investigation-lopez-crime-family.

Special Focus: Tax Crime

This section was included primarily due to the increase in State and federal payroll tax evasion and workers' compensation insurance fraud in the U.S. residential and commercial real estate construction industries. Tax crime refers to any illicit activity related to Internal Revenue Code violations.[199] The IRS projected the gross tax gap at $688 billion for tax year 2021 alone, which could result in approximately $7 trillion in lost tax revenue over the next decade. The IRS Criminal Investigation (IRS-CI) is the main LEA that focuses on tax crime. In FY22 the IRS-CI identified over $31 billion from tax and financial crimes, and the agency seized assets valued at approximately $7 billion in FY22.[200] The IRS prevented the loss of an additional $4.6 billion by stopping the issuance of fraudulent refunds during the 2022 tax season.[201] The direct loss of tax revenue resulting from tax crime deprives the U.S. government of proper funding for essential services and programs. For example, in January of 2022, an American chief executive officer (CEO) was sentenced to 60 months in prison for using a foreign trust and real estate transactions to evade over $20 million in income tax.[202]

Tax schemes have evolved into opaque arrangements, often giving the appearance that the perpetrator is not associated with earnings. Abusive tax schemes originally took the structure of fraudulent domestic and foreign trust arrangements. However, the taxpayers receive their funds through debit/credit cards or fictitious loans. These schemes often involve offshore banking and sometimes establish scam corporations or entities.[203]

There has been a concerning increase in state and federal payroll tax evasion and workers' compensation insurance fraud in the U.S. residential and commercial real estate construction industries. Illicit actors perpetrate these schemes through banks and check cashing businesses by exploiting shell construction companies and fraudulent documents to commit insurance fraud and pay their workers "off the books," State and federal tax authorities lose hundreds of millions of dollars to these schemes and legitimate construction companies and their workers are put at a competitive disadvantage.[204]

Criminals launder illicit tax proceeds, using the same money laundering methods applicable to other proceeds-generating crimes, including the misuse of legal entities, trusts, and real estate to conceal the use of illicit tax funds. For example, a Florida developer defrauded investors out of more than $30 million while evading $2.5 million in U.S. income taxes and penalties in July 2023. To launder the proceeds of his scheme, the developer misused legal entities and purchased several real estate properties using discrete LLCs.[205]

199 U.S. Code: Title 26.

200 IRS, "2023 Annual Report", (November 3, 2022), https://www.irs.gov/pub/irs-pdf/p3583.pdf.

201 TIGTA, "Results of the 2022 Filling Season", (Mar. 30, 2023), https://www.tigta.gov/sites/default/files/reports/2023-04/202340021fr.pdf.

202 DOJ, "CoFounder and Former CEO of Foreign Oil Company Sentenced to 60 Months in Prison for Failure to File Taxes Causing over $20 Million in Losses to U.S. Treasury", (January 26 2022), https://www.justice.gov/usao-sdny/pr/co-founder-and-former-ceo-foreign-oil-company-sentenced-60-months-prison-failure-file.

203 IRS, "Tax Fraud Alerts", (August 2023), https://www.irs.gov/compliance/criminal-investigation/tax-fraud-alerts.

204 FinCEN, "FinCEN Notice Highlights Concerning Increase in Payroll Tax Evasion, Workers' Compensation Fraud in the Construction Sector," (August 2023), https://www.fincen.gov/news/news-releases/fincen-notice-highlights-concerning-increase-payroll-tax-evasion-workers.

205 DOJ, "Real Estate Developer Sentenced for Investment Fraud, Bank Fraud, Money Laundering, and Tax," (July 31. 2023), https://www.justice.gov/usao-ct/pr/real-estate-developer-sentenced-investment-fraud-bank-fraud-money-laundering-and-tax.

Tax refund fraud typologies have become more prevalent. In one case, King Isaac Umoren, a tax preparer, was sentenced for filing false tax returns, aggravated identity theft, wire fraud, money laundering, and impersonating an FBI agent. Umoren required clients to use a refund anticipation check program, which Umoren then used to take fees from clients' tax refunds without their knowledge.[206] In a different scheme, in March 2023, a federal grand jury unsealed an indictment charging seven individuals in a conspiracy to claim fraudulent tax refunds using the stolen identities of accountants and taxpayers by filing at least 371 false tax returns claiming over $111 million in refunds. The conspirators posed as authorized agents of multiple taxpayers and allegedly used prepaid debit cards to receive the fraudulent refunds. They used the cards to launder the funds by purchasing money orders from local stores in amounts low enough to avoid reporting thresholds. The conspirators purchased designer clothing and used cars with the proceeds from the illicit activity.[207]

Update on Wildlife Trafficking and other Nature Crimes

As an update to the 2022 NMLRA's special focus section on wildlife trafficking, the Treasury is calling attention to the broader category of nature crime. Given its strong association with corruption and transnational organized crime (AML/CFT National Priorities), FinCEN indicates that wildlife trafficking affects the U.S. financial sector.[208] The illicit proceeds generated in the U.S. or that pass through the U.S. financial system related to nature crimes are not as significant compared to the top threats described above. Still, the importance of the U.S. dollar and financial system to international trade and finance, these types of crimes pose a unique money laundering threat to the United States.

A recent example of a money laundering scheme involving nature and other crimes involves Bhagavan "Doc" Antle, who pleaded guilty to money laundering and conspiracy to commit offenses against the United States. Antle owned and operated a South Carolina-based safari park and conducted financial transactions with cash he believed was obtained from transporting and harboring illegal aliens. Antle violated the Lacey Act by directing the sale or purchase of numerous animals that are protected under the Endangered Species Act.[209] He used bulk cash payments to hide the transactions and falsified paperwork to show non-commercial transfers entirely within one state. In addition, Antle requested that payments for endangered species be made to his nonprofit so they could appear as "donations".[210]

1. The Intersection of Nature Crimes with Other Threats

Foreign corruption: According to law enforcement sources, foreign corruption consistently plays a critical role for wildlife trafficking networks in facilitating poaching, smuggling, transportation,

206 IRS, "Las Vegas tax preparer sentenced to prison for multiple fraud schemes," (December 1, 2022), https://www.irs.gov/compliance/criminal-investigation/las-vegas-tax-preparer-sentenced-to-prison-for-multiple-fraud-schemes.

207 DOJ, "Seven Charged in Sophisticated Stolen Identity Tax Refund Fraud Scheme that Sought Over $100 Million from the IRS", (March 13, 2023), https://www.justice.gov/opa/pr/seven-charged-sophisticated-stolen-identity-tax-refund-fraud-scheme-sought-over-100-million.

208 FinCEN, Financial Threat Analysis, "Illicit Finance Threat Involving Wildlife Trafficking and Related Trends in Bank Secrecy Act Data," (December 22, 2021), https://fincen.gov/sites/default/files/2021-12/Financial_Threat_Analysis_IWT_FINAL%20508_122021.pdf.

209 The Lacey Act prohibits trafficking of illegally taken wildlife, fish or plants, including animals protected under the Endangered Species Act.

210 DOJ, November 6, 2023, "Doc Antle, Owner of Myrtle Beach Safari, Pleads Guilty to Federal Wildlife Trafficking and Money Laundering Charges", https://www.justice.gov/opa/pr/doc-antle-owner-myrtle-beach-safari-pleads-guilty-federal-wildlife-trafficking-and-money.

distribution, trade, and money laundering. In November 2022, the DOJ indicted a senior Cambodian Forestry official who allegedly conspired with other officials to smuggle wild-caught primates into the United States for biomedical research. This left U.S. pharmaceutical companies exposed to transacting with corrupt officials and their intermediaries. This case, which involved financial flows of nearly $20 million, was a major initiative involving coordination among U.S. law enforcement agencies and U.S. financial institutions registered under section 314(b) of the USA PATRIOT Act.[211]

Drug trafficking: According to law enforcement sources, there are instances of Mexican DTOs trading wildlife and wildlife parts to Chinese drug traffickers in exchange for precursor chemicals for fentanyl and methamphetamine that may be destined for the United States. In May 2023, Abdi Hussein Ahmed, a member of a wildlife trafficking ring, was sentenced to 48 months in prison for conspiring to traffic large quantities of rhinoceros horns (rhino horn) and elephant ivory and conspiring to distribute and possess with intent to distribute heroin. The value of the wildlife products involved in the case exceeded $7 million. Ahmed and his co-conspirators received payments from foreign customers by international wire transfers, some of which were sent through U.S. financial institutions. [212]

Transnational Criminal Organizations: On October 7, 2022, OFAC designated the Teo Boon Ching TCO,[213] which has been involved in wildlife trafficking for two decades. The TCO focused its business model on exploiting high-value assets, such as ivory, rhino horn, and pangolins, and coordinating transport from Africa to customers in Asia, especially in China and Vietnam. Malaysian national Teo Boon Ching was arrested in Thailand and extradited to the United States. Ching pleaded guilty to conspiracy to commit wildlife trafficking, and was sentenced to 18 months in prison. Ching served as a specialized smuggler, transporting rhino horns from rhinoceros poaching operations located predominantly in Africa to the eventual customers who were primarily in Asia. Ching also claimed to be able to ship rhino horns to the United States.[214] As outlined in the plea agreement, Ching charged a fee in RMB (rather than USD) for his trafficking services and operated through an "underground bank" to get around AML/CFT controls at certain banks. Ching also accepted USD in cash because he could convert it to RMB. Ching instructed rhino horn customers to structure payments into multiple Chinese bank accounts before he would release the rhino horn. Upon confirming the deposit of funds, Ching directed the delivery of the rhino horn to undercover law enforcement in Bangkok.

211 DOJ, Environmental Crimes Bulletin November 2022 , "United States v. Omaliss Keo, et al., No. 1:22-CR-20340 (S. D. Fla.)," https://www.justice.gov/enrd/blog/ecs-bulletin-december-2022#Keo.

212 DOJ, "Fifth Defendant Sentenced To 48 Months In Prison For Large-Scale Trafficking Of Rhinoceros Horns And Elephant Ivory And Heroin Conspiracy," (May 11, 2023), https://www.justice.gov/usao-sdny/pr/fifth-defendant-sentenced-48-months-prison-large-scale-trafficking-rhinoceros-horns#:~:text=Damian percent20Williams percent2C percent20the percent20United percent20States,species percent20 percentE2 percent80 percent94 percent20worth percent20millions percent20of percent20dollars.

213 Treasury, October 7, 2022, "Treasury Sanctions Wildlife Trafficking Organized Crime Group", https://home.treasury.gov/news/press-releases/jy1001.

214 DOJ, "U.S. Attorney Announces Extradition of Malaysian National For Large-Scale Trafficking Of Rhinoceros Horns," (October 7, 2022), https://www.justice.gov/usao-sdny/pr/us-attorney-announces-extradition-malaysian-national-large-scale-trafficking-rhinoceros.

SECTION II. VULNERABILITIES AND RISKS

In the context of the 2024 NMLRA, 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 section represents the residual risk of a particular sector or service. It takes into consideration any remaining risk after the effect of mitigating measures including regulation, supervision, and enforcement, among other things.

Money launderers attempt to identify and exploit money laundering vulnerabilities, given the nature, location, and form of their illicit proceeds. Money laundering methods shift and evolve in response to opportunities and changes in financial services, regulation, and enforcement.

Cash

Criminals use cash-based money laundering strategies in significant part because cash offers anonymity. The commonly use U.S. currency due to its wide acceptance and stability. To combat this, the United States requires that large cash transactions be reported to the Treasury.[215] However, according to federal agency reports, TCOs and other criminals take steps to avoid this reporting through the following strategies.

1. Bulk Cash Smuggling

The use of U.S. dollar banknotes (cash) remains a popular method to transport and launder illicit proceeds both within and outside of the United States. BCS involves moving physical currency across an international border, often to be deposited in another country's financial institution.[216] Unreported bulk currency may sometimes be the proceeds of illegal activity, such as financial fraud and money scams. BCS remains a favored means for TCOs to repatriate their illicit funds from or move funds into the United States to support their criminal operations. TCO networks on the Southwest border smuggle narcotics into the United States while illegally exporting currency from drug proceeds and firearms into Mexico. TCO networks also use the northern border to smuggle high-potency drugs and currency both into and out of the United States.

At the nation's more than 300 ports of entry, U.S. Customs and Border Protection's (CBP) Office of Field Operations (OFO) has a complex mission with broad law enforcement authorities tied to screening all foreign visitors, returning American citizens, and imported cargo that enters the United States. Along the

215 For example, federal law requires a person to file IRS Form 8300 for cash transactions of $10,000 or more received in a trade or business, and financial institutions generally must report currency transactions of $10,000 or more made by, through, or to the institution. *See* 31 C.F.R. part 1010, subpart C.

216 The United States prohibits knowingly concealing more than $10,000 in currency or other monetary instruments and transporting or transferring or attempting to transport or transfer such currency or monetary instruments across a U.S. border with the intent to evade currency reporting requirements. 31 U.S.C. § 5332. In addition, 18 U.S.C. § 1956 prohibits the international transportation, transmission or transfer of funds (or attempted transportation, transmission or transfer of funds) that the person knows represent the proceeds of an unlawful activity and conducts the transportation, transmission or transfer to disguise circumstances of the unlawful activity or avoid state or federal transaction reporting requirements.

nation's borders. From an inbound perspective, for calendar year (CY) 2023, there were a total of 1,480 seizures of currency and monetary instruments totaling $18 million.[217]

Law enforcement has indicated that although there had been a decline in outbound BCS activity (and stockpiling) due to a decline in travel and trade related to the COVID pandemic, the activity has again reached pre-pandemic levels.[218] For CY 2023, there were 1,010 outbound currency and monetary seizures totaling approximately $53 million.[219] The top sites for outbound bulk cash seizure sites were Detroit International Airport, Chicago O'Hare International Airport, and the Port of Fort Lauderdale. The top three recorded intended destination countries for bulk cash seized during 2023 were Mexico, Vietnam, and Haiti.[220] Historically, there has not been a specific budget allocation for outbound inspection. Although OFO policies do not require outbound inspections, officers at some land border crossings conduct inspections of personal vehicles and pedestrians departing the United States to prevent the illegal exportation of currency and other contraband, and there have been some significant currency seizures.[221]

Previous NMLRAs have focused mainly on cash couriers, those individuals directly responsible for moving the cash across international borders. Recent insights by law enforcement have shed further light on the role of "currency handlers," who are thought to occupy positions with higher levels of responsibility and trust within criminal organizations than couriers and are more likely to be involved in the coordination and scheduling of BCS activities. Law enforcement sources have indicated that they suspect financial supply chain specialists employed by some TCOs send their trusted agents to the currency points of origin to coordinate shipments of bulk cash across the country and then return to the destination to oversee onward movement of those proceeds.

Identifying a currency handler can provide a window to the inner workings of the criminal networks they serve. According to discussions with U.S. law enforcement, over half of the identified currency handlers were U.S. citizens. Mexican citizens represented the largest block (approximately one third) of foreign currency handlers, followed by citizens from the Dominican Republic and Jamaica.

2. Cash Consolidation Cities

Every year, illicit cash proceeds from all crimes including illegal opioid sales travel on the U.S. highway system. In FY 2022, most cash seized from domestic cash couriers on U.S. highways originated in California, Colorado, Georgia, Florida, Ohio, Oklahoma, Texas, and Virginia.

According to U.S. law enforcement personnel, there has been a shift in location where conversions in bill denominations (*e.g.,* converting smaller denominations into $100 bills) take place. This conversion traditionally took place within the interior United States, but can now be found in border states such as California, Florida, and Texas.

217 CBP, *Currency & Other Monetary Instrument Seizures,* (Data current as of November 6, 2023), https://www.cbp.gov/newsroom/stats/currency-other-monetary-instrument-seizures.

218 See 2022 NMLRA, PP.31-32.

219 CBP, *Currency & Other Monetary Instrument Seizures,* (Data current as of November 6, 2023), https://www.cbp.gov/newsroom/stats/currency-other-monetary-instrument-seizures.

220 HSI, BSCS statistics as of 9/8/2023.

221 DHS, Office of the Inspector General, "CBP Outbound Inspections Disrupt Transnational Criminal Organization Illicit Operations (REDACTED)," August 3, 2023, https://www.oig.dhs.gov/sites/default/files/assets/2023-08/OIG-23-39-Aug23-Redacted.pdf.

While most domestic bulk cash is destined for California, lesser (though still significant) amounts are destined for Arizona and Texas. Ohio, Virginia, Georgia, North Carolina, Florida, Missouri, and New York (from lowest to highest) were the nation's top seven states of origin for cross-country bulk cash destined for the Southwest Border region. Once these proceeds reach their border destinations, criminals may smuggle them across the border or enter one of several money laundering schemes intended to unite illicit proceeds with the drug cartels that raised them.[222]

Case examples

- In May 2022, a California woman residing in Atlanta, Georgia, was charged with smuggling over $114,000 of cash into Mexico from the United States. According to court documents, the defendant attempted to pass through a Border Patrol checkpoint as a taxi passenger. The vehicle was referred to secondary inspection, when the defendant denied the relevant custom form (i.e., made a negative declaration) for having more than $10,000. However, according to the charges, $114,294 was discovered in her purse.[223]
- In February 2022, a Mexican man was charged with smuggling $195,731 in cash into Mexico. The cash was hidden in the bed and center console of a pickup truck. According to the charges, the defendant attempted to exit the United States through the Juarez-Lincoln Port of Entry in Laredo as a solo driver in a pickup truck. There, he allegedly gave a negative declaration for possessing currency over $10,000.[224]

SNAPSHOT: Use of Private Aircraft

Law enforcement sources have noted an increased use of private aircraft to smuggle bulk cash. The use of aircraft is a more expeditious method to move currency into, through, and out of the United States over longer distances than by loading money into a vehicle or strapping it to a pedestrian. U.S.-registered aircraft are less likely to be inspected by state, local or federal agencies and can be identified by the "N" designated tail number on the tail of the aircraft. In many small airports along the Mexico-U.S. border, CBP does not maintain a 24-hour presence. This security gap allows TCOs and criminal elements to move currency derived from criminal endeavors into and out of the United States with greater ease than by cars or pedestrians.

Law enforcement sources note TCOs manipulate Federal Aviation Administration (FAA) reporting requirements to purchase, register, and export U.S. aircraft. TCO members will establish shell companies and then use LLCs to purchase and register aircraft, which allows the aircraft to be registered through a trust pursuant to FAA regulations.[225] This enables TCO members to circumvent the regulatory requirement that a foreign company must be organized and doing business under the laws of the United States to register an aircraft and that the aircraft must be based and primarily used in the United States.[226]

222 Information provided by HSI, BCSC.

223 ICE, "California woman charged with smuggling over $114k inside taxi, following HSI, federal partner, probe," (May 18, 2022) https://www.ice.gov/news/releases/california-woman-charged-smuggling-over-114k-inside-taxi-following-hsi-federal#:~:text=However percent2C percent20A percent20search percent20of percent20Zuniga percent27s,a percent20possible percent20 percent24250 percent2C000 percent20maximum percent20fine.

224 DOJ, "Visa holder caught smuggling nearly $200,000 to Mexico", (February 23, 2022), https://www.justice.gov/usao-sdtx/pr/visa-holder-caught-smuggling-nearly-200000-mexico.

225 *See* 14 CFR 47.7(c).

226 *See* 14 CFR 47.3(a)(3).

3. Cash-Intensive Businesses and Front Companies

Criminal actors continue to use cash intensive businesses (CIBs) as a laundering vehicle. Criminal organizations and individuals often attempt to set up a front company associated with a CIB to launder criminally derived proceeds. Criminal actors have long relied on these "fronts" which otherwise conduct legitimate business and have a physical location and natural cash flows to launder large volumes of cash. To introduce illicit funds, individuals mix legitimate business revenue with illicit proceeds using cash deposits and other conventional placement techniques. Furthermore, criminal actors can exploit seemingly reasonable business operations to facilitate bulk cash movements.

LEAs see a wide array of CIBs utilized as front companies such as convenience stores, restaurants, and liquor stores.[227] In recent years, laundering operations have continued to exploit automotive shops including dealers and repair shops as front companies for money laundering.[228] An IRS/FinCEN Report of Cash Payments Over $10,000 in a Trade or Business (referred to as the "Form 8300") is required to be filed if a person in a trade or business receives more than $10,000 in cash in a single transaction or in related transactions.[229]

Case examples

- A March 2022 indictment charged multiple codefendants with allegedly using an Oregon beauty salon as a front to launder proceeds for a DTO that dealt fentanyl, heroin, and counterfeit oxycodone pills throughout the Pacific Northwest.[230] Agents seized 115,000 counterfeit Oxycodone pills that contained fentanyl and 57 pounds of heroin as part of their investigation. The salon owner allegedly opened several accounts at different banks for her salon entity. She then made numerous large cash deposits and purchases of cashier's checks under the guise of "business transactions". The defendant allegedly used her salon to avoid scrutiny regarding the size of cash-based transactions. After the owner made the deposits and purchased the cashier checks, they used the funds to buy several real estate properties. The salon owner tried to further disguise the source of these funds by claiming the real estate transactions were purchases of "rental properties."[231]
- A March 2022 indictment charged the owners of a Sacramento area grocery store with operating a front business for a CJNG-supplied cocaine operation.[232] Law enforcement was able to observe laundering by infiltrating the operation. Most laundering activity took place via money remittances and bulk cash smuggling. The laundering activity allegedly involved transporting $230,000 of bulk cash and exchanging it with a DTO associate. Court documents indicate this was one week of cocaine sales. Evidence within the criminal complaint notes the grocery store was allegedly used to store cash, disguise the source of illicit deposits, and support individual remittances to Mexico.[233]

227 FFIEC, Risks Associated with Money Laundering and Terrorist Financing, Cash-Intensive Business – Overview, https://bsaaml.ffiec.gov/manual/RisksAssociatedWithMoneyLaunderingAndTerroristFinancing/26.

228 DOJ, "Milton Man Sentenced for Money Laundering: Owner of used car dealership laundered fraud proceeds through his business", (August 5, 2022) https://www.justice.gov/usao-ma/pr/milton-man-sentenced-money-laundering#:~:text=BOSTON percent20 percentE2 percent80 percent93 percent20The percent20owner percent20of percent20a,two percent20years percent20of percent20supervised percent20release.

229 31 C.F.R. § 1010.330.

230 United States District Court District of Oregon, See case 3:22-cr-00045 (Feb. 09, 2022).

231 DOJ, "12 Members of Drug Trafficking Organization Indicted for Distributing Counterfeit Oxycodone Pills Containing Fentanyl, Laundering Proceeds", Mar. 18, 2022, https://www.justice.gov/usao-or/pr/12-members-drug-trafficking-organization-indicted-distributing-counterfeit-oxycodone.

232 DOJ, "Two Sacramento Area Men Indicted for Cocaine Trafficking", (Mar. 31, 2022), https://www.justice.gov/usao-edca/pr/two-sacramento-area-men-indicted-cocaine-trafficking.

233 United States District Court Eastern District of California, see case 2:22-cr-00064, (Mar. 14, 2022).

4. Funnel Accounts

Funnel accounts are bank accounts used to collect deposits from various locations. Multiple individuals deposit cash in a bank account available to other members of the criminal network in another part of the country. Criminal actors continue to use funnel accounts to circumvent Currency Transaction Report (CTR) thresholds and other BSA obligations to facilitate money laundering. Funnel accounts allow individuals to make multiple deposits utilizing separate accounts at numerous financial institutions to stay below regulatory threshold amounts. Criminal and money laundering organizations use geographic structures where money mules deposit cash across several accounts in one area while another member of the organization withdraws the funds in a consolidation region. Accounts being used to transfer or "funnel" cash are often used to make rapid transactions and withdrawals after depositing criminal proceeds.

Funnel accounts remain a key component of DTOs moving funds across the Mexican border. Organizations funnel cash through accounts in U.S. regional hubs and consolidate the funds by withdrawing them at branches closer to the border, commonly in California, Texas, and Arizona. They then employ BCS techniques to transport the cash over the border into Mexico. Recent and historical examples demonstrate that criminal actors often utilize funnel accounts in tandem with a front company to achieve widescale placement of illicit funds.

Case examples

- Pharmacy owners Arkadiy Khaimov and Peter Khaim, who made millions by submitting fraudulent claims for expensive medications during the pandemic, pleaded guilty to conspiracy to commit money laundering in November 2022. The owners used 16 different registered corporate entities to funnel $47 million of illicit funds through their associated bank accounts. The codefendants conspired with an unregistered MSB to trade cash in return for their fraudulent Medicare funds. The scheme then utilized nominee account signatories to act as mules, purchasing cashier checks with the illicit money as a form of deposit. These cashier's checks and other cash deposits were then aggregated within accounts that the codefendants ultimately owned. This allowed the codefendants to purchase legitimate assets with the proceeds of their fraud scheme.[234]
- An Oklahoma City restaurant owner was charged with conspiracy to commit money laundering in a May 2023 indictment for using funnel accounts as a vehicle to launder $25 million. A branch manager reported the defendant's suspicious behavior after they allegedly attempted to open 14 separate accounts for their singular restaurant entity. The defendant moved to another bank after being denied the accounts, where they successfully open 14 accounts that resembled cash deposit funnel accounts. Court documents also detailed a separate financial institution closing the defendant's accounts due to large deposits and rapid withdrawals.[235]
- A June 2023 indictment charged a Honduran national with money laundering in connection to their role as a high-level human smuggling coordinator. Court documents outlined the defendant allegedly showing associates how to open additional bank accounts to facilitate funneling activity. Investigators were also able to present a financial accounting ledger that explicitly showed smuggling fees and cash flows. Court documents also claim that the defendant's organization had money mules deposit cash at several different banks in different regions within the United States. Following these geographically diverse deposits, the criminal actors allegedly withdrew millions of dollars in smuggling proceeds in the Phoenix, Arizona area.[236]

234 DOJ, "Two Pharmacy Owners Plead Guilty in COVID-19 Money Laundering and Health Care Fraud Case", (November 16, 2022), https://www.justice.gov/opa/pr/two-pharmacy-owners-plead-guilty-covid-19-money-laundering-and-health-care-fraud-case.

235 Western District of Oklahoma, USA vs Lin et al, case 5:24-mj-276-STE (May 2, 2023), See https://www.pacermonitor.com/public/case/49505889/USA_v_Lin_et_al.

236 DOJ, "Prolific Human Smuggler Extradited to the United States from Honduras", (Jun. 23, 2023), https://www.justice.gov/usao-az/pr/prolific-human-smuggler-extradited-united-states-honduras.

Financial Products and Services

1. Money Orders

Criminal actors continue to attempt to evade the controls in place on money orders to launder proceeds from narcotic and fraud schemes. A money order is a financial instrument that acts as a secure form of cash replacement. Because a money order is paid for in advance, unlike a personal check, a money order cannot be rejected for insufficient funds. Issuers or sellers of money orders are a type of MSB and thus subject to certain registration, recordkeeping, program, and reporting obligations under the BSA and its implementing regulations applicable to MSBs.[237] Specifically, issuers or sellers of money orders are required to develop, implement, and maintain an AML program to obtain, verify and record customer identification for currency purchases of money orders totaling $3,000 or more,[238] and file CTRs and SARs.[239] Money orders are offered for a fee by MSBs such as Western Union and MoneyGram as well as the United States Postal Service (USPS).[240]

In 2023, FinCEN received 396,763 SARs related to transactions that utilized money orders.[241] According to law enforcement sources, money order investigations can be challenging based on the minimal amount of information recorded during transactions.

Laundering facilitated through the misuse of money orders often follows a similar typology. In many cases, criminals use prepaid debit cards or illicit cash to purchase bulk money orders. They then use these money orders to purchase material assets, such as cars, and export the vehicles or assets to a foreign country.[242] Criminals may also deposit money orders into bank accounts where the funds can be further wire transferred to other bank accounts to further layer the illicit proceeds. Businesses that accept bulk money orders from customers as payment for goods or services are also vulnerable to abuse by criminals laundering illicit proceeds.

In contrast to recordkeeping requirements involving funds transfer services provided by banks, there is no explicit requirement for sellers of money orders to collect payee information. The issuer does not know the payee's name until that payee negotiates the money order and the instrument subsequently clears the banking system. This situation means money order sellers may be unable to screen the name of the payee and, depending on the amount, the sellers may not be able to verify the payer's name. The BSA recordkeeping obligation applicable to money orders only requires issuers and sellers of money orders to obtain, verify and record customer identification with the purchase of money orders for $3,000, or more in currency. However, sellers of money orders may request payee information to satisfy other BSA requirements, such as AML program and SAR filing obligations. Nonetheless, criminals circumvent

237 31 C.F.R. Part 1022.

238 31 C.F.R. § 1022.210

239 31 CFR § 1010.310-1010.314 and 31 CFR § 1010.320.

240 DOJ, "Drug Conspiracy Leader Gets 262-Months Imprisonment for Distributing Methamphetamine in Southern Illinois," (September 7, 2023), https://www.justice.gov/usao-sdil/pr/drug-conspiracy-leader-gets-262-months-imprisonment-distributing-methamphetamine.

241 FinCEN, "Suspicious Activity Report Statistics (SAR Stats)," https://www.fincen.gov/reports/sar-stats.

242 DOJ, "Four Men Charged in a Superseding Indictment with Conspiring to Launder Funds from Various Fraud Schemes," (Jul. 3, 2023), https://www.justice.gov/opa/pr/four-men-charged-superseding-indictment-conspiring-launder-funds-various-fraud-schemes.

this record keeping requirement by structuring their money order transactions below this requirement, as demonstrated in the following case examples:

Case examples

- In February 2022, the U.S. Court of Appeals for the Eleventh Circuit affirmed a defendant's conviction in a marijuana distribution and money laundering conspiracy. After receiving drugs from California, the defendant helped distribute and launder money for more than 900 kilograms of marijuana by processing drug money through casinos and nail salons before converting the cash into money orders under the $3,000 record keeping threshold.[243]
- In January 2023, 24 defendants were charged with marijuana distribution, money laundering, firearms, and related offenses. They allegedly laundered proceeds from the sale of marijuana and edibles through a variety of means, including money transfers; the transportation and delivery of cash, including $179,710 in cash that authorities seized at the Albany International Airport; the purchase of cashier's checks; real estate transactions; and cash and money order deposits into various bank accounts.[244]

2. Prepaid Cards

Prepaid cards (also referred to as prepaid debit cards, stored value cards, or prepaid access devices) are a type of prepaid access that enables pre-loading and in some cases, reloading of funds onto physical or digital cards.

The use of prepaid cards is growing rapidly. The most recent Federal Reserve Payments Study found that, on average, the number of prepaid card transactions increased by 9.6 percent per year from 2018 to 2021, and the value of prepaid card transactions grew by 20.6 percent per year, compared with 12.7 percent for debit cards and 7.0 percent for credit cards.[245] The total value of prepaid card payments was $610 billion in 2021, accounting for 6.5 percent of the value of all card payments. Globally, the prepaid card market was valued at $1.73 trillion in 2019 and is projected to reach $6.87 trillion by 2030.[246]

There are two systems under which prepaid cards operate: an "open" or "closed" loop system. Open loop (also called general purpose) prepaid cards are branded by a payment network (*e.g.,* Visa, Mastercard, American Express, Discover) and can be used for purchases at any merchant that accepts cards on that network, as well as to access cash at ATMs that connect to the affiliated ATM network. Some open-loop prepaid cards may be reloaded with additional funds, allowing the cardholder or other person (such as an employer) to add value. Closed-loop prepaid cards generally can only be used at a specific merchant or a select group of merchants and cannot be used for cash access or transfer of funds. Examples of closed-loop cards include retail gift cards and mass transit cards.[247] Providers and sellers of prepaid access are types of MSBs under FinCEN's regulations unless they qualify for an applicable exemption.[248]

243 United States v. Bui, No. 21-10356, 2022 WL 475002 (11th Cir. Feb. 16, 2022).

244 DOJ, "24 People Indicted for Cross-Country Marijuana Distribution and Money Laundering Conspiracies, Firearms Offenses, and Other Crimes," (January 31, 2023), https://www.justice.gov/usao-ndny/pr/24-people-indicted-cross-country-marijuana-distribution-and-money-laundering.

245 Federal Reserve, The Federal Reserve Payments Study: 2022 Triennial Initial Data Release, Table 1, https://www.federalreserve.gov/paymentsystems/fr-payments-study.htm.

246 Allied research, Prepaid Card Market Research 2023, https://www.alliedmarketresearch.com/prepaid-card-market.

247 FFIEC, BSA/AML Manual, https://bsaaml.ffiec.gov/manual/RisksAssociatedWithMoneyLaunderingAndTerroristFinancing/09.

248 31 C.F.R. 1010.100(ff)(4) and (7).

Prepaid cards can also be used in some cases as a method of cross-border funds transfer, in which two or more prepaid cards are linked to the same account: funds loaded to a prepaid card in the United States, for instance, could be withdrawn from a second, linked card in another country.[249]

Several features of prepaid cards make them popular for use by criminals as a tool for fraud and money laundering: they are easy to purchase and use; people can fund them, through a variety of methods; they typically do not require the cardholder to have an account and can often be used anonymously; and they are highly portable, providing an attractive alternative to bulk cash smuggling. In addition, individuals can use many open-loop prepaid cards globally, enabling money to move easily across borders. In some cases, criminals use false identification and fund initial loads onto prepaid cards with stolen credit or debit card credentials or may purchase multiple prepaid cards under aliases.[250] Another common fraud scheme involves criminals calling victims and impersonating the government or a company. Through false and fraudulent claims, they will convince victims that they owe money and must pay it by purchasing gift cards or prepaid cards and providing the criminals with the card information. Both open and closed- loop prepaid cards have been used as an alternative to bulk cash smuggling.

Prepaid cards are used in all stages of money laundering. In the placement stage, criminals purchase prepaid cards in bulk using illegal funds, or they hire or convince others to purchase or transport the cards for them. In the layering stage, criminals can use prepaid cards to purchase merchandise or other prepaid cards, which they can sell for cash. According to law enforcement sources, a common money laundering scheme involves criminals using prepaid cards to purchase money orders. These, in turn, are used to purchase material goods, which can then be re-sold. In the integration stage, criminals may use prepaid cards to fund illicit and legitimate activities and transactions.

Case examples

- In March 2023, Chaohui Chen and Wenyi Zheng were sentenced to 21 months and 36 months imprisonment, respectively, after pleading guilty to wire fraud. Under their wire fraud scheme and gift card conspiracy they deceived victims into purchasing prepaid Walmart gift cards and providing that information to the defendants for their personal gain. According to the plea agreement, a typical execution of the scheme involved unnamed third parties who would make false and fraudulent telephone calls, sometimes claiming to the victims they were part of the Social Security Administration. Using false pretenses, the callers would convince victims to purchase prepaid gift cards and provide to them with the 16-digit gift card numbers and unique pins for the gift cards, in return for a cashier's check in the amount of the gift card purchased. Once in control of the gift cards, the defendants would redeem the gift cards at various stores by purchasing household items and additional prepaid gift cards, which they would convert and use for their personal gain, and neglect to return any of the money to the victims.[251]
- In June 2022, Yanio Montes De Oca and Atnetys Ferreira Milian were sentenced to 27 months and one year of probation for their respective roles in a conspiracy to commit money laundering. Between December 2015 and July 2019, De Oca laundered thousands of gift cards that were obtained using fraudulent debit and credit cards encoded with information stolen using gas station skimming devices. After obtaining the gift cards from co-conspirators, De Oca sold them and transferred the

249 FFIEC, BSA/AML Manual, https://bsaaml.ffiec.gov/manual/RisksAssociatedWithMoneyLaunderingAndTerroristFinancing/09.

250 FFIEC BSA Manual, https://bsaaml.ffiec.gov/manual/RisksAssociatedWithMoneyLaunderingAndTerroristFinancing/09.

251 DOJ, "Defendants Sentenced in a $217,200 Gift Card Conspiracy and Wire Fraud Scheme that Cheated Victims, Including the Elderly, Out of Thousands of Dollars," (March 20, 2023) https://www.justice.gov/usao-ut/pr/defendants-sentenced-217200-gift-card-conspiracy-and-wire-fraud-scheme-cheated-victims.

resulting amounts to bank accounts he controlled. De Oca would distribute some of the money to the other conspirators and retain the rest of the funds for himself. Ferreira Milian used multiple bank accounts that she controlled to launder money orders that had been purchased with fraudulent debit cards. The debit cards used stolen account numbers that had been skimmed at gas station pumps across the country. During the period of the conspiracy, Ferreira Milian deposited over 1,100 money orders, totaling over $691,000, into her accounts, and then withdrew most of the laundered funds in cash.[252]

- In February 2022, Malan Doumbia and Souleymane Diarra were convicted of nine counts including conspiracy to commit wire fraud, access device fraud, aggravated identity theft, and conspiracy to commit money laundering. This criminal activity was in connection with a scheme to purchase stolen credit card numbers from the dark web, using the accounts to purchase consumer products, and then re-selling the products for cash. The defendants worked with several associates to purchase stolen credit card numbers from black market websites located in Russia, Ukraine, and elsewhere overseas. After encoding these card numbers onto blank cards, they employed a network of runners to use the cards to purchase large quantities of gift cards and other items that could be quickly resold for cash. When the United States Secret Service searched the defendants' homes, they found more than 200,000 stolen credit card numbers.[253]

3. Peer-to-Peer Payments

Over the last decade, peer-to-peer (P2P) payments have grown in popularity and become ubiquitous throughout the United States. P2P services – such as mobile applications Venmo, PayPal, Cash App, and Zelle – allow individuals to send and receive instant digital payments directly with another person, either in fiat currency or virtual currency.

The P2P market has grown dramatically in recent years, helped along by a spike in adoption during the COVID-19 pandemic. P2P users are forecast to reach 168 million in 2024, with a total transaction value projected to exceed $1.2 trillion.[254] According to a survey conducted by Fiserv in 2020, 79 percent of consumers say they have used a P2P service.[255] However, the convenience and speed that make P2P platforms popular for legitimate purposes also make them attractive to scammers. In 2021, the Federal Trade Commission received nearly 70,000 complaints from consumers who sent money to fraudsters via payment apps or similar services, totaling $130 million in losses.[256]

Depending on the platform and form of currency, a consumer can initiate a P2P payment from their online bank account, prepaid card account, virtual asset wallet or through a mobile application. With respect to mobile applications, P2P apps are free to download, and payments are typically free when made using a linked checking account, debit card, or stored balance; some platforms also allow funding via credit card for a fee. P2P services operate as relatively closed environments where users can only

252 DOJ, "Miami Residents Sentenced for Their Roles in a Money Laundering Conspiracy Connected to a Nationwide Gas Station Skimming Scheme", (June 30, 2022) https://www.justice.gov/usao-ndny/pr/miami-residents-sentenced-their-roles-money-laundering-conspiracy-connected-nationwide.

253 DOJ, "Two Philadelphia Men Convicted of Running Credit Card Fraud Ring Using 200,000+ Stolen Accounts," (February 28, 2022), https://www.justice.gov/usao-edpa/pr/two-philadelphia-men-convicted-running-credit-card-fraud-ring-using-200000-stolen.

254 CFPB, Person-to-Person (P2P) Payment Fraud Conversation, (November 2022), https://files.consumerfinance.gov/f/documents/cfpb_person-to-person-p2p-payment-fraud-conversation_presentation_2022-11.pdf.

255 Fiserv, "Consumer Payments Executive Summary," (February 2021), file:///C:/Users/SandersA/Downloads/EE_Consumer_Payments_Executive_Summary_0221.pdf.

256 Federal Trade Commission, "Consumer Sentinel Network Data Book 2021," (February 2022), https://www.ftc.gov/system/files/ftc_gov/pdf/CSN percent20Annual percent20Data percent20Book percent202021 percent20Final percent20PDF.pdf#page=12.

send funds to another individual on the same platform. Because of this feature, bank account details can be kept private from individual users: all that is typically required from a user to send a payment is the recipient's email address or phone number. When users receive a payment, they usually can maintain a balance in the app or transfer the funds to their bank accounts. While most P2P services in the United States only operate domestically, some, such as PayPal, offer cross-border payment options. P2P payment services are considered either banks or MSBs (depending on the platform) and thus subject to the reporting, recordkeeping, and AML program requirements under the BSA, and, if it classifies as an MSB, must register with FinCEN.[257]

P2P services have come to play a sizable role in various types of fraud and scams. These include unauthorized electronic fund transfers, seller scams, buyer scams, and money mule scams, among others.[258] In unauthorized electronic fund transfers, scammers often impersonate a bank, fraud department, or merchant and ask the victim to confirm information such as account name and password. Unauthorized electronic fund transfers can also result from a hacked account, stolen phone, or phishing scheme. In a seller scam, scammers impersonate legitimate sellers or businesses and request a P2P payment for a good or service from the victim. Once the victims sends the payment, the scammer disappears and the victim never receives what they paid for.[259] In money mule scams, scammers send money to a victim, sometimes by check, and ask the victim to send some of it to someone else. Often, these victims are instructed to make these payments via P2P services. Typically, the check is fake, and the victims are on the hook for the funds they sent out (and potentially legally liable for helping a scammer move stolen money).[260] In another version of money mule scams, a scammer will "accidentally" send a person funds on a P2P platform and request that they send the money back. The original funds are stolen funds that the P2P service will eventually flag as fraud, and the victim is held responsible for the funds they sent back to the scammer.[261]

Case examples

In June 2021, an indictment was unsealed charging 60 members of a San Diego-based methamphetamine trafficking organization with ties to the Sinaloa Cartel with money laundering, drug trafficking, and firearm offenses. The network obtained thousands of kilograms of methamphetamine from the Sinaloa Cartel in Mexico to smuggle across the international border concealed in hidden compartments in passenger cars and motorcycles. The network then, at the order of the Sinaloa Cartel, distributed the methamphetamine to dozens of sub-distributors located across 12 states and at least two other countries. The members of the DTO returned tens of thousands of dollars in narcotics proceeds to the network's leaders via shipments of bulk cash, structured cash deposits into bank accounts, and money transfers through MoneyGram, Western

257 31 C.F.R. Part 1022.

258 Capital One, "Peer-to-peer payment scams & fraud: How to protect yourself," (November 2, 2022), https://www.capitalone.com/bank/money-management/financial-tips/what-is-p2p-fraud/.

259 American Bankers Association, "Peer to Peer Payment Scams," https://www.aba.com/advocacy/community-programs/consumer-resources/protect-your-money/peer-to-peer-payment-scams#:~:text=Scammers percent20posing percent20as percent20a percent20legitimate,paid percent20for percent20and percent20they percent20disappear.

260 FTC, "What's a money mule scam?" (March 4, 2020), https://consumer.ftc.gov/consumer-alerts/2020/03/whats-money-mule-scam.

261 American Bankers Association, "Peer to Peer Payment Scams," https://www.aba.com/advocacy/community-programs/consumer-resources/protect-your-money/peer-to-peer-payment-scams#:~:text=Scammers percent20posing percent20as percent20a percent20legitimate,paid percent20for percent20and percent20they percent20disappear.

Union, PayPal, Zelle, Venmo, and Cash App.[262]

In July 2022, Linda Ann Been pleaded guilty to conspiracy, wire fraud, conspiracy to commit wire fraud, and conspiracy to commit money laundering for her role in heading a retail theft organization that caused more than $10 million in losses to retailers. Fifteen others involved in the organization also pleaded guilty. According to state and federal court documents, Been led a ring of "boosters" that netted $4.5 million from selling stolen merchandise to "fencing organizations," which then sold the stolen products through e-commerce sites. Been provided her boosters with a detailed list of items to steal and the pricing she would pay for each. Been further instructed her ring on boosting techniques. Been and her team of boosters stole products from retailers in Oklahoma, Kansas, Texas, Missouri, Arkansas, and Colorado. Been would pay boosters' expenses when they traveled outside the state. Been would further pay boosters' bond when arrested so they could continue boosting. Been and her team normally made financial payments for stolen products through PayPal, Venmo, and Cash App.[263]

Legal Entities and Arrangements

As reported in previous risk assessments, illicit actors deliberately misuse legal entities to facilitate money laundering schemes, fraud, sanctions evasion, tax evasion, and drug trafficking, among other types of offenses. These actors rely on the anonymity and perceived legitimacy afforded to legal entities, including limited liability companies and other corporate structures, to disguise illicit financial activity and criminal beneficial owners. Recent cases highlight the misuse of legal entities as a significant, ongoing vulnerability in the U.S. financial system; for example, illicit actors have used complex schemes involving shell companies to commit COVID-19 relief fraud and to procure dual-use U.S. technology to advance Russian aggression in Ukraine. These schemes often feature layers of corporate entities, trusts, and nominee arrangements, and can involve both domestic and foreign natural or legal persons.

1. Legal Entities

In addition to the use of shell companies, criminals also rely on shelf and front companies to obfuscate illicit financial activity. Shelf companies are ready-to-use legal entities that were incorporated in the past and put on the 'shelf' to age, which may give them the appearance of being 'established.' Unlike shell and shelf companies that typically have no employees, operations, or even a physical location other than a registered agent, front companies generate real economic activity and are used to commingle illicit proceeds with earnings from legitimate business operations. In a recent case, front companies were used as part of a scheme to raise capital and acquire goods for North Korea in violation of U.S. sanctions.

Case examples

- In September 2023, a Russian citizen and Hong Kong resident, was charged with participating in an illicit procurement scheme that provided military grade microelectronics to end users in Russia. According to the complaint, the defendant and two co-conspirators used shell companies based in Hong Kong and other deceptive means to conceal from U.S. Government agencies and U.S.

262 DEA, "Sixty Defendants Charged in Nationwide Takedown of Sinaloa Cartel Methamphetamine Network", (June 29, 2021) https://www.dea.gov/press-releases/2021/06/29/takedown-sinaloa-cartel.

263 FBI, "Woman Pleads Guilty for Leading a Retail Theft Organization that Netted $4.5 Million", (July 14, 2022), https://www.justice.gov/usao-ndok/pr/woman-pleads-guilty-leading-retail-theft-organization-netted-45-million.

distributors that the OLED micro-displays that they purchased were destined for Russia. In total, between about May 2022 and August 2023, the defendant's shell companies allegedly funneled a total of more than $1.6 million to the United States in support of the procurement network's efforts to smuggle the OLED microdisplays to Russia.[264]

- In September 2022, the DOJ announced federal criminal charges against 47 defendants for their alleged roles in a $250 million fraud scheme that exploited a federally funded child nutrition program in Minnesota during the COVID-19 pandemic. The defendants are alleged to have defrauded the Federal Child Nutrition Program, exploiting changes in the program intended to ensure underserved children received adequate nutrition during the COVID-19 pandemic. The defendants are alleged to have created dozens of shell companies to receive and launder the proceeds of their fraudulent scheme.[265]
- In May 2022, brothers Luis Enrique Martinelli Linares and Ricardo Enrique Martinelli Linares, both dual citizens of Panama and Italy, pleaded guilty to conspiracy to commit money laundering and admitted to agreeing with others to establish offshore bank accounts in the names of shell companies to receive and disguise over $28 million in bribe proceeds from Odebrecht S.A., a Brazil-based global construction conglomerate, for the benefit of a close relative, a high-ranking public official in Panama. Both were sentenced to 36 months in prison and ordered to forfeit more than $18.8 million, pay a $250,000 fine, and serve two years' supervised release.[266]

2. Beneficial Ownership Information

Lack of transparency in legal entity ownership structures has continued to be a challenge for U.S. law enforcement agencies, requiring time and resource-intensive processes to obtain beneficial ownership information (BOI). This issue also remains a key vulnerability globally. A 2022 FATF study on the state of global effectiveness and compliance with the FATF standards revealed that only half of jurisdictions, on average, have the necessary laws and regulations to understand, assess the risks of, and verify the beneficial owners or controllers of legal persons and arrangements. Furthermore, only 9 percent of countries are meeting the overall effectiveness requirements concerning beneficial ownership transparency.[267] To strengthen the standard on beneficial ownership transparency for legal persons, in March 2022, FATF adopted significant amendments to Recommendation 24.[268] These amendments seek to enhance the quality of BOI collected by governments, facilitate efficient access to BOI by competent authorities (including through registries or an alternative mechanism), and improve international

264 DOJ, "Russian International Money Launderer Arrested for Illicitly Procuring Large Quantities of U.S.-Manufactured Dual-Use Military Grade Microelectronics for Russian Elites", (September 18, 2023), https://www.justice.gov/opa/pr/russian-international-money-launderer-arrested-illicitly-procuring-large-quantities-us.

265 DOJ, "U.S. Attorney Announces Federal Charges Against 47 Defendants in $250 Million Feeding Our Future Fraud Scheme", (September 20, 2022), https://www.justice.gov/opa/pr/us-attorney-announces-federal-charges-against-47-defendants-250-million-feeding-our-future.

266 DOJ, May 20, 2022, Panama Intermediaries Each Sentenced to 36 Months in Prison for International Bribery and Money Laundering Scheme, https://www.justice.gov/opa/pr/panama-intermediaries-each-sentenced-36-months-prison-international-bribery-and-money.

267 FATF "Report on the State of Effectiveness and Compliance with the FATF Standards", (April 2022), https://www.fatf-gafi.org/en/publications/Fatfgeneral/Effectiveness-compliance-standards.html.

268 FATF "Public Statement on Revisions to R.24", (March 4, 2022), https://www.fatf-gafi.org/en/publications/Fatfrecommendations/R24-statement-march-2022.html.

cooperation. The amendments also include a new requirement for national authorities to collect BOI in the course of public procurement as a means to combat corruption.[269]

In the United States, criminals have historically been able to take advantage of the lack of uniform laws and regulations pertaining to the disclosure of BOI to law enforcement. FinCEN's 2016 CDD Rule, which became applicable in May 2018 and requires certain financial institutions, such as banks and broker-dealers, to identify and verify the identities of the beneficial owners of most legal entity customers at account opening, has helped mitigate this vulnerability to an extent. However, the lack of timely access to high-quality BOI and BOI disclosure requirements at the time of a legal entity's creation or registration has continued to hamper law enforcement investigations, which is why the Treasury continues to prioritize the implementation of the Corporate Transparency Act (CTA).

Enacted as part of the Anti-Money Laundering Act of 2020 (AML Act),[270] the CTA requires certain U.S. and foreign companies to disclose BOI to FinCEN. It also requires FinCEN to build a secure, non-public database of this information and disclose to authorized government authorities and financial institutions, subject to safeguards and controls. In September 2022, FinCEN issued a final BOI Reporting Rule to implement the reporting requirements of the CTA.[271] The rule describes who must file a BOI report, what information must be reported, and when a report is due. This rule represents the culmination of years of bipartisan efforts by Congress, the Treasury, national security agencies, law enforcement, and other stakeholders to bolster the United States' corporate transparency framework and address the most significant gap in the U.S. AML/CFT regime that the FATF identified in the 2016 U.S. Mutual Evaluation.

FinCEN began accepting BOI on January 1, 2024, the effective date of the final BOI Reporting Rule. In parallel, in December 2023, FinCEN issued a final BOI Access Rule to establish who may request and receive BOI, how recipients may use it, and how they must secure it.[272] This rule becomes effective on February 20, 2024. As required by the CTA, FinCEN will also revise the CDD Rule to conform with the CTA. However, until these revisions are finalized, existing requirements for covered financial institutions to collect BOI under the CDD Rule remain unchanged presenting a lingering information gap.

Looking ahead, while the full implementation of the CTA will help facilitate law enforcement investigations and make it more difficult for illicit actors to hide behind anonymous shell companies created in the United States or foreign entities registered to do business in the United States, there is a risk that illicit actors will seek to exploit certain types of entities that are exempt under the CTA or shift their activities to corporate structures that are not covered by the CTA (*e.g.,* trusts that do not qualify as reporting companies under the final BOI Reporting Rule).

269 In March 2023, FATF also adopted revisions to Recommendation 25 on beneficial ownership transparency of legal arrangements, including trusts. Also in March, FATF adopted revised guidance to assist countries in implementing the changes to Recommendation 24; work on developing guidance associated with revised Recommendation 25 is ongoing and is expected to be finalized in 2024.

270 Public Law No. 116-283 (Jan. 1, 2021).

271 FinCEN, Beneficial Ownership Information Reporting Requirements, 87 FR 59498, (Sept. 30, 2022), https://www.federalregister.gov/documents/2022/09/30/2022-21020/beneficial-ownership-information-reporting-requirements.

272 FinCEN, Beneficial Ownership Information Access and Safeguards, 88 FR 88732, (Dec. 21, 2022), https://www.federalregister.gov/documents/2023/12/22/2023-27973/beneficial-ownership-information-access-and-safeguards.

3. Trusts

In the United States, as in many countries, trusts are private legal arrangements commonly used by individuals and legal entities (known as grantors/settlors) to place assets in custody and to provide the benefit of those assets[273] or to disburse assets on behalf of designated individuals or entities (known as beneficiaries), such as upon the death of the individual conveying assets to the trust (also known as the grantor/settlor). Trusts have long been a cornerstone of estate and tax planning, and many individuals choose to use trusts for legitimate reasons, including protecting the privacy of estate management decisions; safeguarding the interests of beneficiaries who are not of age or otherwise not capable of making sound financial decisions; and, in the case of inheritance, avoiding the requirements of probate and, under some circumstances, enjoying certain tax benefits.

The FATF has previously identified trusts and other similar legal arrangements as vulnerable to money laundering and has worked to strengthen its Recommendation 25 to impose requirements to obtain information on the beneficial ownership of trusts.[274] Trusts, in the aggregate, are susceptible to misuse primarily for fraud and tax evasion. This illicit activity may occur through the unethical and illegal conduct of the trustee themselves, for instance, engaging in fraud or embezzlement against the wishes and interests of the settlor and beneficiaries. Additionally, trusts may be utilized by the grantor/settlor to hide and move illicit proceeds of crime, in which case the trustee may be fulfilling their fiduciary obligations without knowledge that the assets were illegally obtained. The IRS has also cited a number of tax-related abuses of trusts, including false claims related to instruments that are advertised as trusts but do not meet the legal definition of trust.

In reviewing the risks associated with trusts used to launder funds in the United States, it is important to distinguish between the risks of U.S. trusts and foreign trusts with a U.S. nexus. While law enforcement does see criminal actor abuse of trusts, particularly for those trusts settled in what LEAs call "notorious privacy states" like South Dakota, Wyoming, Delaware, Alaska, and Nevada, the risk is higher for those trusts settled outside of the United States (or settled overseas and then converted into U.S. trusts).[275] At present, based on available information and consultations with subject matter experts, the Treasury continues to assess that while they pose risk and there have been instances of abuse, U.S. trusts may not be systemically used for money laundering. Certain factors contribute to the apparent current lack of systematic misuse of trusts for money laundering or sanctions evasion. For illicit finance purposes, creating a trust is complex and time consuming and involves too many co-conspirators or knowledgeable parties as compared to creating a shell company, which any individual (non-professional) can do for a nominal fee. Additionally, U.S. law enforcement has judicial and administrative recourse to find information for U.S. trusts created by a U.S. settlor or for a U.S. beneficiary. Based on discussion with law enforcement and case review, these factors may make trusts less attractive than, or not as easy to use as, other methods to launder funds or obfuscate the ownership or control of assets (such as the misuse of shell companies). However, this is a preliminary baseline assessment, and we acknowledge some current data limitations.

273 For example, the interest on principal invested, or rental income from property held in trust.

274 See FATF Recommendation 25 and its interpretative note, available at https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Fatf-recommendations.html, that was amended at the February 2023 Plenary (described further in this document), see https://www.fatf-gafi.org/en/publications/Fatfgeneral/outcomes-fatf-plenary-february-2023.html.

275 ICE, Cornerstone September 2023 Issue #44, "Money Laundering via Trusts," https://content.govdelivery.com/bulletins/gd/USDHSICE-36cc596?wgt_ref=USDHSICE_WIDGET_217.

In contrast to U.S. trusts, trusts settled in foreign jurisdictions that establish sufficient links[276] to the U.S. financial system present a higher risk for money laundering and sanctions evasion because the non-U.S. status of grantors, settlors, trustees, or beneficiaries may limit law enforcement access to beneficial ownership and other information about those arrangements. [277] A review of cases indicates a higher degree of risk arising from trusts being used to custody assets derived from foreign corruption, especially to obtain U.S. real estate or investments.

Except for certain trusts that are taxed as business entities, the federal government does not require trusts formed in the United States to register or otherwise disclose their creation. However, trusts must disclose themselves when applying for a tax identification number or filing annual income tax or information returns. Law enforcement access to this type of information is limited without a court order. The federal government also does not any comprehensive AML/CFT obligations or regulations on trustees except for financial institutions that offer trust services (including commercial banks and trust companies).

Case examples

- On June 30, 2022, OFAC issued a Notification of Blocked Property to Heritage Trust, a Delaware-based trust in which OFAC-designated Russian oligarch Suleiman Abusaidovich Kerimov holds a property interest. Heritage Trust was formed in July 2017 for the purpose of holding and managing Kerimov's U.S.-based assets. Kerimov used a complex series of legal structures and front persons to obscure his interest in Heritage Trust, the funds of which first entered the U.S. financial system through two foreign Kerimov-controlled entities prior to imposing sanctions against him. The funds were subsequently invested in large public and private U.S. companies and managed by a series of U.S. investment firms and facilitators. Kerimov and his proxies used various layers of U.S. and non-U.S. shell companies to hold formal titles to assets and to conduct transactions in a manner that concealed his interest.[278]
- On August 31, 2022, the DOJ announced the return of approximately $686,000 in forfeited criminal proceeds to the Republic of Peru linked to the corruption and bribery of former Peruvian President Alejandro Celestino Toledo Manrique (Toledo) by Odebrecht S.A. (Odebrecht), a Brazil-based construction conglomerate. In the civil forfeiture matter and a related case, the United States alleged that Toledo, while holding public office as President of Peru, solicited millions in bribe payments from Odebrecht in connection with government contracts awarded for construction of the Peru-Brazil Southern Interoceanic Highway, a Peruvian government infrastructure project. Odebrecht

276 In February 2023, the FATF amended Recommendation 25 to require jurisdictions to conduct risk assessments for, inter alia, "3.(c) types of foreign legal arrangements that have sufficient links with their country." The FATF leaves it to countries to determine what is considered a "sufficient link." The Interpretative Note provides examples of what a sufficiency test may include, including when a trustee has "significant and ongoing business relations with financial institutions or DNFBPs, has significant real estate/other local investment, or is a tax resident, in the country." (see https://www.fatf-gafi.org/content/dam/fatf-gafi/recommendations/FATF percent20Recommendations percent202012.pdf.coredownload.inline.pdf.)

277 Non-U.S. settlors who settle trusts in the United States raise particular issues in collecting data about them. One of the issues is that such settlors create a mismatch between U.S. trust residence rules which treat the trust as foreign and the rules of their home jurisdiction/another jurisdiction where the same trust may be viewed as a foreign trust as well (because it is established under U.S. law). By virtue of the trust being non-resident in both jurisdictions, the overall tax and information reporting stance is diminished.

278 Treasury, "Treasury Sanctions Global Russian Military Supply Chain, Kremlin-linked Networks, and Elites with Western Fortunes," (November 14, 2022), https://home.treasury.gov/news/press-releases/jy1102#:~:text=In percent20June percent202022 percent2C percent20OFAC percent20issued,valued percent20at percent20over percent20 percent241 percent20billion.

subsequently made bribery payments to Toledo through accounts maintained by Toledo's co-conspirators. Ultimately, Toledo and his family used approximately $1.2 million of the bribery payments to purchase real estate in Maryland in 2007 through a scheme designed to hide Toledo's ownership of the funds and their connection to Odebrecht. The forfeited assets represent the proceeds from the sale of the Maryland real estate, which were further laundered through a trust and bank account controlled by Toledo. After acquiring a Maryland residential property, obtained through legal entities, Toledo had the title transferred to the Havenell Trust, an irrevocable trust with the trust documents prepared by a law firm. Toledo and a relative were initially listed as the trustees and the beneficiaries before amending the trust to successively make a real estate agent and then an attorney as the trustees. The trust later sold the property in question and placed the sale proceeds into a bank account. Toledo later used the Havenell Trust as the final destination for additional proceeds of corruption transferred through offshore shell companies. Toledo also used the Havenell Trust account to transfer money to an attorney escrow account belonging to a cooperating witness, which was then transferred to different accounts controlled by Toledo or his associates.[279]

Virtual Assets[280]

Since the publication of the 2022 NMLRA, the virtual asset ecosystem has been in flux. The market value of virtual assets have fallen considerably since their height in the fall of 2021, with many virtual assets losing value through early 2023 but rebounding in the fall of 2023. Despite several large virtual asset-related firms declaring bankruptcy, hundreds of virtual asset service providers (VASPs) continue to operate in the United States. Traditional financial institutions continue to consider virtual asset-related products and services, including offering to custody virtual assets, banking VASPs, and using the technology underpinning virtual assets to experiment with tokenizing existing traditional financial assets.

In the United States, VASPs have AML/CFT obligations if they fall under the BSA definition of a financial institution, which covers banks, broker-dealers, mutual funds, MSBs, futures commission merchants (FCMs), introducing brokers, and other forms of financial institutions.[281] Many VASPs in the United States are considered MSBs, but depending on the activities in which the VASP engages, they may be considered FCMs or securities intermediaries such as broker-dealers.[282] Foreign-located VASPs that operate wholly or in substantial part in the United States are considered MSBs, unless an applicable exemption applies, and must comply with applicable BSA requirements. Each of these types of financial institutions has AML/CFT obligations, including requirements to establish and implement an effective AML Program[283] and

279 DOJ, "Justice Department Will Return Approximately $686,000 in Forfeited Corruption Proceeds to the Republic of Peru," (August 31, 2022), https://www.justice.gov/opa/pr/justice-department-will-return-approximately-686000-forfeited-corruption-proceeds-republic.

280 This report uses the terms "virtual asset" and "VASP (virtual asset service provider)," terms not contained explicitly in U.S. law or regulation, to align with the terminology defined by the FATF. Virtual assets, as used in this report, include non-sovereign-administered digital assets such as convertible virtual currencies [CVCs], like bitcoin and stablecoins. For 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. This, however, does not cover central bank digital currencies, which are representations of fiat currency.

281 31 U.S.C. § 5312(a)(2); 31 C.F.R. § 1010.100(t).

282 FinCEN, "Leaders of CFTC, FinCEN, and SEC Issue Joint Statement on Activities Involving Digital Assets," (Oct. 11, 2019), https://www.fincen.gov/sites/default/files/2019-10/CVC percent20Joint percent20Policy percent20Statement_508 percent20FINAL_0.pdf.

283 See 31 C.F.R. § 1020.210 (banks); 31 C.F.R. § 1021.210 (casinos and card clubs); 31 C.F.R. § 1022.210 (MSBs); 31 C.F.R. § 1023.210 (brokers or dealers in securities); 31 C.F.R. § 1024.210 (mutual funds); 31 C.F.R. § 1026.210 (futures commission merchants and introducing brokers in commodities).

recordkeeping and reporting requirements, including SAR filing obligations.[284] FinCEN, OFAC, SEC, and the Commodities Futures Trading Commission (CFTC) have issued statements and guidance on regulatory requirements for VASPs.[285]

Further, VASPs that are U.S. persons, like all other U.S. persons, wherever located, are required to comply with economic sanctions programs administered and enforced by OFAC. At the same time, 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 virtual assets or traditional fiat currency.[286]

While the use of virtual assets for money laundering continues to remain far below that of fiat currency and more conventional methods that do not involve virtual assets, U.S. law enforcement agencies have observed virtual assets being misused for ransomware, scams, drug trafficking, human trafficking, and other illicit activities.

1. Inconsistent Compliance with Domestic Obligations

In the United States, there are cases in which VASPs fail to comply with their AML/CFT and sanctions obligations. When covered VASPs 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, including circumventing United States and United Nations sanctions. For example, some VASPs currently do not implement adequate AML/CFT controls or other processes to identify customers, allowing placement, layering, and integration of illicit proceeds to occur instantaneously and pseudonymously without collecting appropriate identifying information.

In some cases, such VASPs may claim not to be subject to U.S. jurisdiction despite doing business wholly or in substantial part in the United States. In some instances, VASPs have directed U.S.-based users to use virtual private networks or other methods such as the creation of shell companies to obscure that they are based in the United States.[287] VASPs have also marketed themselves as requiring little to no customer

284 See 31 C.F.R. § 1020.320 (banks); 31 C.F.R. § 1021.320 (casinos and card clubs); 31 C.F.R. § 1022.320 (MSBs), 31 C.F.R. § 1023.320 (brokers or dealers in securities), 31 C.F.R. § 1024.320 (mutual funds), and 31 C.F.R. § 1026.320 (futures commission merchants and introducing brokers in commodities). A suspicious transaction must be reported if it is conducted or attempted by, at, or through the financial institution and the amount involved exceeds a certain threshold.

285 See, *e.g.,* SEC, "Strategic Hub for Innovation and Financial Technology," https://www.sec.gov/finhub; SEC, Crypto Assets, https://www.investor.gov/additional-resources/spotlight/crypto-assets; FinCEN, "FinCEN Guidance," (May 9, 2019), https://www.fincen.gov/sites/default/files/2019-05/FinCEN percent20Guidance percent20CVC percent20FINAL percent20508.pdf; SEC, "Leaders of CFTC, FinCEN, and SEC Issue Joint Statement on Activities Involving Digital Assets," (October 11, 2019), https://www.sec.gov/news/public-statement/cftc-fincen-secjointstatementdigitalassets; Treasury, "Sanctions Compliance Guidance for the Virtual Currency Industry," (October 2021), https://ofac.treasury.gov/media/913571/download?inline; OFAC, "Frequently Asked Questions: Questions on Virtual Currency," (May 9, 2019), https://home.treasury.gov/policy-issues/financialsanctions/faqs/, FinCEN, "FinCEN Guidance", https://www.fincen.gov/sites/default/files/2019-05/FinCEN percent20Guidance percent20CVC percent20FINAL percent20508.pdf; FinCEN, "Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies," (March 18, 2013), https://www.fincen.gov/sites/default/files/administrative_ruling/FIN-2014-R002.pdf.

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.

287 FinCEN, "In the Matter of: Binance Holdings Limited, Binance (Services) Holdings Limited, Binance Holdings (IE) Limited, d/b/a Binance and Binance.com, Number 2023-04, Consent Order Imposing Civil Money Penalty," (November 21, 2023), https://fincen.gov/sites/default/files/enforcement_action/2023-11-21/FinCEN_Consent_Order_2023_04_Final508.pdf.

information from users prior to transactions, in violation of U.S. AML/CFT requirements.[288] However, even among VASPs that do take steps to register or obtain a license with U.S. regulators, some VASPs may be licensed or registered incorrectly and, therefore, not meeting the full AML/CFT obligations for the services that they are providing. For example, a VASP registered as an MSB may also be operating as an unlicensed FCM or broker dealer, in which case they would be required to implement measures as an FCM, like a customer identification program, that do not apply to MSBs. More recently, many purportedly DeFi services (see Special Focus Section on DeFi) and some virtual asset peer-to-peer platforms claim that they are not subject to BSA requirements, purporting to enable automated transactions without the need for an account or custodial relationship. These entities may, however, be regulated financial institutions depending on specific facts and circumstances surrounding their financial activities.[289]

There have also been instances in which VASPs subject to BSA obligations based on their financial activities have failed to meet AML program requirements under the BSA and its implementing regulations. For example, based on services the VASP provides, the VASP may be required to implement an AML program, with internal controls that are commensurate with the risks posed by their customers, the nature and volume of the financial services they provide, and the jurisdictions in which they provide services. Some VASPs have scaled quickly without adequately assessing and mitigating potential regulatory risks associated with providing new or additional services, including offering anonymity-enhancing cryptocurrencies (AECs) and expanding into new geographic markets.[290] Law enforcement and regulators have observed VASPs offering services to so-called nested VASPs, (*i.e.,* smaller VASPs that offer services to their customers through accounts and sub-accounts held at larger VASPs to benefit from the liquidity and convenience the larger market players provide). In such instances, VASPs 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 which will vary based on the services the VASP offers.[291]

Law enforcement has also observed the misuse of virtual asset kiosks, which are often considered MSBs for BSA purposes, to launder illicit proceeds. Some perpetrators of scams or fraud may direct victims to use virtual asset kiosks to purchase virtual assets with fiat currency and send virtual assets to the perpetrator, sometimes by sharing Quick Response codes that auto-populate the perpetrator's virtual asset wallet address.[292] Some kiosk owners have failed to comply with AML/CFT obligations or disabled features designed to support compliance, enabling misuse by illicit actors.[293]

---

288 DOJ, "Justice Department Seizes and Forfeits Approximately $500,000 from North Korean Ransomware Actors and their Conspirators", (July 19, 2022), https://www.justice.gov/opa/pr/justice-department-seizes-and-forfeits-approximately-500000-north-korean-ransomware-actors.

289 CFTC, "Statement of CFTC Division of Enforcement Director Ian McGinley on the Ooki DAO Litigation Victory" (June 9, 2023), https://www.cftc.gov/PressRoom/PressReleases/8715-23#:~:text=June percent2009 percent2C percent202023&text=Critically percent2C percent20in percent20a percent20precedent percent2Dsetting,violate percent20the percent20law percent20as percent20charged; CFTC, CFTC Orders Event-Based Binary Options Markets Operator to Pay $1.4 Million Penalty, (January 3, 2022), https:// www.cftc.gov/PressRoom/PressReleases/8478-22; SEC, SEC Charges Decentralized Finance Lender and Top Executives for Raising $30 Million Through Fraudulent Offerings, (August 6, 2021), https://www.sec.gov/news/press-release/2021-145.

290 FinCEN, "Consent Order Imposing Civil Money Penalty, In the Matter of Bittrex, Inc.," (Number 2022-03), https://www.fincen.gov/sites/default/files/enforcement_action/2023-04-04/Bittrex_Consent_Order_10.11.2022.pdf.

291 See Footnotes 338 and 339.

292 IC3, "The FBI Warns of Fraudulent Schemes Leveraging Cryptocurrency ATMs and QR Codes to Facilitate Payment" (November 04, 2021), https://www.ic3.gov/Media/Y2021/PSA211104.

293 DOJ, "Ian Freeman Sentenced to 8 Years in Prison for Operating a Bitcoin Money Laundering Scheme" (October 2, 2023), https://www.justice.gov/usao-nh/pr/ian-freeman-sentenced-8-years-prison-operating-bitcoin-money-laundering-scheme.

Case examples:

- Binance: In November 2023, Binance Holdings Limited and its affiliates, which operate the world's largest VASP, Binance.com, entered into the largest resolutions in the Treasury's history with FinCEN (including a penalty of $3.4 billion) and OFAC (including a penalty of nearly $1 billion), as well as resolutions of parallel investigations by the DOJ and the CFTC. As part of these resolutions, Binance pleaded guilty and paid penalties totaling over $4.3 billion, to resolve the Justice Department's investigation into violations related the BSA, failure to register as a money transmitting business, and the International Emergency Economic Powers Act.[294]
- Binance's founder and CEO also pleaded guilty to BSA violations and resigned from Binance.[295] After launching in 2017, Binance quickly became the largest VASP in the world, with the greatest share of its customers coming from the United States. As a result of serving U.S. customers, Binance was required to register with FinCEN as an MSB and to establish, implement and maintain an effective AML program. Due in part to Binance's failure to implement an effective AML program, including (among other things) failing to perform KYC on a large number of its users, illicit actors used Binance's exchange in various ways. Furthermore, Binance failed to file SARs on their suspicious transactions, including those related to terrorist financing, ransomware, child sexual abuse materials, as well as darknet markets, scams, and other illicit activity. As part of the resolution with FinCEN, Binance has also agreed to retain an independent compliance monitor for three years and remediate and enhance its AML and sanctions compliance programs. Binance separately has also reached agreements with the CFTC, FinCEN, and OFAC, and the Justice Department will credit approximately $1.8 billion toward those resolutions. Under its settlement with FinCEN, Binance also agreed to significant compliance undertakings, including a groundbreaking five-year monitorship, an independent review of its AML program, and a SAR lookback review.
- Bittrex: In October 2022, OFAC and FinCEN announced that Bittrex, a VASP, had entered into separate settlements of over $24 million and $29 million, respectively.[296] Bittrex failed to prevent persons located in sanctioned jurisdictions, namely the Crimea region of Ukraine, Cuba, Iran, Sudan, and Syria, from using its platform to transact approximately $263 million in virtual assets between March 2014 and December 2017. Additionally, from February 2014 to December 2018, Bittrex failed to maintain an effective AML program as required under the BSA by maintaining an inadequate transaction monitoring system on its platform, to address the risks associated with its products appropriately, and failing to file any SARs over a three-year period, including on transactions involving sanctioned jurisdictions. Bittrex's inadequate AML compliance program and transaction monitoring left its platform open to abuse by bad actors, including money launderers, terrorist financiers, ransomware attackers, and sanctions evaders.

294 Treasury, "U.S. Treasury Announces Largest Settlements in History with World's Largest Virtual Currency Exchange Binance for Violations of U.S. Anti-Money Laundering and Sanctions Laws," (November 21, 2023), https://home.treasury.gov/news/press-releases/jy1925; DOJ, "Binance and CEO Plead Guilty to Federal Charges in $4B Resolution" (November 21, 2023), https://www.justice.gov/opa/pr/binance-and-ceo-plead-guilty-federal-charges-4b-resolution.

295 DOJ, "Binance and CEO Plead Guilty to Federal Charges in $4B Resolution," (November 21, 2023), https://www.justice.gov/opa/pr/binance-and-ceo-plead-guilty-federal-charges-4b-resolution.

296 Treasury, "Treasury Announces Two Enforcement Actions for Over $24M and $29M Against Virtual Currency Exchange Bittrex, Inc.," (October 11, 2022), https://home.treasury.gov/news/press-releases/jy1006.

2. Inconsistent Implementation of International AML/CFT Obligations

As highlighted in previous NMLRAs, uneven and often inadequate regulation and international supervision allows VASPs and illicit actors to engage in regulatory arbitrage. This risk can expose the U.S. financial system to VASPs with deficient or nonexistent AML/CFT controls operating abroad. VASPs operating in the U.S. that constitute financial institutions under the BSA are generally subject to the BSA and its implementing regulations, including foreign-located VASPs obligations that operate wholly or in substantial part in the United States. This issue is of particular concern with VASPs given the ability to transfer virtual assets across borders nearly instantaneously compared to other financial transfers, the fact that many VASPs operate or have architecture in several jurisdictions, and the breadth of gaps in implementing international AML/CFT standards set forth by the FATF. Four years ago, the FATF clarified how its global standards on AML/CFT apply to virtual assets and VASPs. However, a recent FATF report based on a voluntary survey of jurisdictions found that jurisdictions continue to struggle with fundamental elements of the FATF standards. It also found that one-third of countries have not yet completed an illicit finance risk assessment for virtual assets and over 40 jurisdictions had not decided if and how to regulate the virtual asset sector for AML/CFT purposes. Even jurisdictions that have decided on and begun implementing an approach often lack sufficient supervision and monitoring systems to effectively conduct supervision and sanction non-compliant VASPs, when applicable.[297] The uneven implementation of effective AML/CFT requirements can allow VASPs to concentrate their operations in jurisdictions with minimal or nonexistent AML/CFT requirements, weak supervision of VASPs, or both.[298] Other VASPs have adopted a distributed architecture where they register in one country, have personnel in a second country, maintain data on servers located in a third country, and offer services in several countries with different legal and regulatory approaches to virtual assets. This approach can complicate supervision and enforcement, which often require considerable cooperation amongst competent authorities.

3. Obfuscation Tools and Methods

Criminals commonly use obfuscation tools and methods to introduce challenges for investigators attempting to trace illicit funds. These tools include mixers (see snapshot) and mixing-enabled wallets, as well as AECs, which reduce the transparency of virtual financial flows through anonymizing features. For example, the virtual asset Monero obfuscates transaction information using cryptographic technologies, such as (1) ring signatures, which are used to hide the identity of the transaction originator; (2) ring confidential transactions, which obfuscate the amount of the transaction; and (3) stealth addresses, which hide the identity of the beneficiary.[299] Other methods may include laundering as a service, which is available in some darknet markets.

Additional methods, such as chain hopping, may frustrate the ability to trace financial transactions quickly or for service providers to detect if incoming funds are tied to illicit activity. Actors can chain-hop by exchanging virtual assets on one blockchain for virtual assets on another. Chain hopping can pose challenges to tracing if actors use specific assets or blockchains that are more difficult to trace given

297 FATF, "Virtual Assets: Targeted Update on Implementation of the FATF Standards on Virtual Assets and Virtual Asset Service Providers," (June 27, 2023), https://www.fatf-gafi.org/en/publications/Fatfrecommendations/targeted-update-virtual-assets-vasps-2023.html.

298 Treasury, "Action Plan to Address Illicit Financing Risks of Digital Assets," September 22, 2022, https://home.treasury.gov/system/files/136/Digital-Asset-Action-Plan.pdf.

299 See Treasury, National Money Laundering Risk Assessment, February 2022.

current limits on blockchain analysis or if the transactions are done quickly. Criminals are constantly evolving techniques to obfuscate illicit proceeds and are learning how to use these techniques effectively. The pace of change can present challenges for competent authorities.

Virtual asset transactions often occur on public blockchains, which means that anyone with internet access can view the pseudonymous transaction data in a public ledger for the blockchain. Public ledgers can support investigations in tracing the movement of illicit proceeds and, paired with other pieces of information, law enforcement can sometimes identify transaction participants. However, the ability to use public blockchain data can be limited by the effective execution or use of the techniques and services described above.

Case examples

- In February 2022, two individuals were arrested for an alleged conspiracy to launder virtual assets stolen during a 2016 hack, presently valued at approximately $4.5 billion.[300] Over the last five years, approximately 25,000 of those stolen bitcoin were allegedly transferred out of the defendant's wallet via a complicated money laundering process that ended with some of the stolen funds being deposited into financial accounts controlled by both defendants.
- A criminal complaint filed by DOJ alleges that the defendants employed numerous sophisticated laundering techniques, including converting bitcoin to other forms of virtual assets, including anonymity-enhanced cryptocurrencies, via chain hopping and depositing the stolen funds into accounts at a variety of VASPs and darknet markets and then withdrawing the funds. In August 2023, one defendant, Ilya Lichtenstein, pleaded guilty to money laundering conspiracy, which carries a maximum penalty of 20 years in prison, and the other defendant, Heather Morgan, pleaded guilty to one count of money laundering conspiracy and one count of conspiracy to defraud the United States, each of which carries a maximum penalty of five years.[301]

4. Mixing

Criminals can use virtual asset mixing to functionally obfuscate the source, destination, or amount involved in a transaction.[302] Mixing can accomplish this through various mechanisms, including pooling or aggregating virtual assets from multiple individuals, wallets, or accounts into a single transaction or transactions. Mixing is frequently used by cybercriminals connected to the DPRK, money launderers, ransomware actors, participants in illicit darknet markets, among others. Mixing services may be advertised as a way to evade AML/CFT requirements and rarely, if ever, include the willingness to provide upon request to regulators or law enforcement the resulting transactional chain or information collected as part of the transaction.[303]

300 DOJ, "Two Arrested for Alleged Conspiracy to Launder $4.5 Billion in Stolen Cryptocurrency," (February 8, 2022), https://www.justice.gov/opa/pr/two-arrested-alleged-conspiracy-launder-45-billion-stolen-cryptocurrency.

301 DOJ, "Bitfinex Hacker and Wife Plead Guilty to Money Laundering Conspiracy Involving Billions in Cryptocurrency," (August 3, 2023), https://www.justice.gov/opa/pr/bitfinex-hacker-and-wife-plead-guilty-money-laundering-conspiracy-involving-billions.

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

303 Treasury, "U.S. Treasury Issues First-Ever Sanctions on a Virtual Currency Mixer, Targets DPRK Cyber Threats," (May 6, 2022), https://home.treasury.gov/news/press-releases/jy0768; FinCEN, "First Bitcoin "Mixer" Penalized by FinCEN for Violating Anti-Money Laundering Laws," (October 19, 2020), https://www.fincen.gov/news/news-releases/first-bitcoinmixer-penalized-fincen-violating-anti-money-laundering-laws.

Because mixing provides foreign illicit actors with enhanced anonymity that allows them to launder their illicit proceeds, in October 2023 FinCEN announced a notice of proposed rule making (NPRM) that identifies international CVC mixing as a class of transactions of primary money laundering concern pursuant to section 311 of the USA PATRIOT Act. FinCEN's proposal would require covered financial institutions to implement certain recordkeeping and reporting requirements on transactions that the covered financial institutions know, suspect, or have reason to suspect it involves CVC mixing within or involving jurisdictions outside the United States.[304]

Case examples

- In March 2023, the DOJ announced a coordinated action against ChipMixer, a virtual asset "mixing" service responsible for laundering more than $3 billion worth of virtual assets.[305] The operation involved U.S. federal law enforcement's court-authorized seizure of two domains that directed users to the ChipMixer service and one Github account, as well as the German Federal Criminal Police's seizure of the ChipMixer back-end servers and more than $46 million in cryptocurrency. As alleged in the complaint, ChipMixer processed hundreds of millions of dollars' worth of bitcoin connected to or associated with ransomware strains, stolen funds, customers of Hydra Market, and Russian intelligence services. ChipMixer also served U.S. customers but failed to register with FinCEN and employed technology to conceal the operating location of servers to avoid law enforcement detection. In addition to the coordinated action, an individual was charged with money laundering, operating an unlicensed money transmitting business, and identity theft, connected to the operation of ChipMixer.
- In August 2023, the DOJ unsealed an indictment charging a Russian and U.S. national of creating, operating, and promoting Tornado Cash, a virtual asset mixer that facilitated more than $1 billion in money laundering transactions, and laundered hundreds of millions of dollars for the Lazarus Group, the sanctioned DPRK cybercrime organization.[306] According to the indictment, Tornado Cash service advertised to customers that it provided untraceable and anonymous financial transactions. Storm and Semenov allegedly chose not to implement know-your customer or anti-money laundering programs as required by law. Even after the Treasury designated Tornado Cash in August 2022, the operators allegedly helped the Lazarus Group to transfer criminal proceeds from a virtual asset wallet that OFAC had designated as blocked property. The operators are each charged with one count of conspiracy to commit money laundering, one count of conspiracy to operate an unlicensed money transmitting business, and one count of conspiracy to violate the International Economic Emergency Powers Act. OFAC also sanctioned Semenov for his role in providing material support to Tornado Cash and to the Lazarus Group.[307]

304 FinCEN, "FinCEN Proposes New Regulation to Enhance Transparency in Convertible Virtual Currency Mixing and Combat Terrorist Financing", (October 19, 2023), https://www.fincen.gov/news/news-releases/fincen-proposes-new-regulation-enhance-transparency-convertible-virtual-currency.

305 DOJ, "Justice Department Investigation Leads to Takedown of Darknet Cryptocurrency Mixer that Processed Over $3 Billion of Unlawful Transactions" (March 15, 2023), https://www.justice.gov/opa/pr/justice-department-investigation-leads-takedown-darknet-cryptocurrency-mixer-processed-over-3.

306 DOJ, "Tornado Cash Founders Charged with Money Laundering and Sanctions Violations", (August 23, 2023), https://www.justice.gov/opa/pr/tornado-cash-founders-charged-money-laundering-and-sanctions-violations#:~:text=According percent20to percent20the percent20indictment percent2C percent20unsealed,laundering percent20transactions percent2C percent20and percent20laundered percent20hundreds.

307 Treasury, "Treasury Designates Roman Semenov, Co-Founder of Sanctioned Virtual Currency Mixer Tornado Cash", (August 23, 2023), https://home.treasury.gov/news/press-releases/jy1702.

5. Disintermediation

Many virtual assets can be self-custodied and transferred without the involvement of an intermediary financial institution, which can be referred to as disintermediation. For example, funds transfers between two users of unhosted wallets may not involve a regulated financial institution. The absence of a regulated financial institution, subject to AML/CFT obligations can limit authorities' collection of and access to information. It can also reduce the effectiveness of preventive measures by other financial institutions with exposure to disintermediated transactions or users involved in such transactions. Such instances present a vulnerability, although these transactions may occur on public blockchains providing some transparency.

6. Special Focus: Decentralized Finance (DeFi)

In April 2022, the Treasury published an illicit finance risk assessment on DeFi.[308] The DeFi risk assessment identified that illicit actors, including ransomware cybercriminals, thieves, scammers, and DPRK cyber actors, are using DeFi services transferring and laundering their illicit proceeds. To accomplish this, illicit actors are exploiting vulnerabilities in the U.S. and foreign AML/CFT regulatory, supervisory, and enforcement regimes as well as the technology underpinning DeFi services. As explained in the risk assessment, a DeFi service that constitutes a financial institution as defined by the BSA, regardless of whether the service is centralized or decentralized, is required to comply with BSA requirements, including AML/CFT obligations. Despite this, many existing DeFi services covered by the BSA fail to comply with AML/CFT obligations, a vulnerability that illicit actors exploit.

For example, in June 2023, a federal judge ruled in favor of the CFTC, entering a default judgment order that requires Ooki DAO, a DAO, to pay a civil monetary penalty of over $643,000.[309] The CFTC had charged Ooki DAO in an administrative order against Ooki DAO's predecessor LLC (bZeroX), which had transferred control of the software to a DAO, and its founders. The bZx Protocol purported to offer users the ability to engage in transactions in a decentralized environment supported by smart contracts - *i.e.,* without third-party intermediaries taking custody of user assets.[310] However, the court held that the Ooki DAO is a "person" under the Commodity Exchange Act and thus can be held liable for violating the law. The administrative order and this enforcement action charged that bZeroX (and then the Ooki DAO) unlawfully offered leveraged and margined retail commodity transactions outside of a registered exchange, unlawfully acted as an FCM, and unlawfully failed to comply with BSA obligations applicable to FCMs.

308 Treasury, "Illicit Finance Risk Assessment of Decentralized Finance" (April 2023), https://home.treasury.gov/system/files/136/DeFi-Risk-Full-Review.pdf. *See also* IOSCO, "Final Report with Policy Recommendations for Decentralized Finance (DeFi)," (December 2023), https://www.iosco.org/library/pubdocs/pdf/IOSCOPD754.pdf.

309 CFTC, "Statement of CFTC Division of Enforcement Director Ian McGinley on the Ooki DAO Litigation Victory" (June 9, 2023), https://www.cftc.gov/PressRoom/PressReleases/8715-23#:~:text=June percent2009 percent2C percent202023&text=Critically percent2C percent20in percent20a percent20precedent percent2Dsetting,violate percent20the percent20law percent20as percent20charged.

310 CFTC, "CFTC Imposes $250,000 Penalty Against bZeroX, LLC and Its Founders and Charges Successor Ooki DAO for Offering Illegal, Off-Exchange Digital-Asset Trading, Registration Violations, and Failing to Comply with Bank Secrecy Act," (September 22, 2022), https://www.cftc.gov/PressRoom/PressReleases/8590-22.

AML/CFT Compliance Deficiencies

Financial institutions and entities in the United States are subject to the provisions of the BSA and play an important role in preventing and detecting illicit activity that threatens the integrity of the U.S. financial system. Many of these financial institutions and entities implement effective AML/CFT programs and controls to guard against their misuse. However, some have demonstrated significant AML/CFT failings.

1. Banks

Over the past 10 years there has been a decline in the number of banks operating in the United States. Recent data indicates that there were approximately 4,672[311] Federal Deposit Insurance Corporation (FDIC)-insured commercial banks and savings institutions in existence as of the first quarter of 2023, compared to 7,019 from the first quarter of 2013.[312] This decline appears to be primarily driven by the consolidation and merger of existing financial institutions. A shift in traditional banking activities, and an increase in financial technology (*i.e.,* "FinTech") companies partnering with banks, a trend referred to as "banking-as-a-service" has also impacted the financial services landscape.[313]

Recent actions taken by the FinCEN and Federal Financial Institutions Regulatory Agencies (FFIRAs),[314] indicate that some banks still struggle to implement corrective actions for issues identified in examinations within the necessary time frames including implementing an adequate system of AML/CFT internal controls or filing SARs in a timely manner. This struggle is especially true for banks lacking a federal functional regulator, which only became subject to comprehensive federal BSA requirements in 2021.

New technologies employed by financial institutions have advanced financial crimes compliance but also exposed banks to risks. In 2022, the Office of the Comptroller of the Currency (OCC) cautioned that use of new technologies or entry into new markets may cause familiar risks to manifest in different ways or may necessitate new techniques to identify, measure, monitor, and control them appropriately.[315]

Recent activity shows that the emergence of virtual asset-focused firms may pose unique vulnerabilities as these entities evolve into financial institutions (*e.g.,* banks) as defined under the BSA and seek to resource themselves sufficiently to deal with their risk exposure and regulatory requirements. Other enforcement actions indicate that some banks have failed to follow the procedures to identify their customers in a timely manner and are not properly utilizing technological solutions to mitigate customer risk. More recently, in 2023, the OCC noted an increase in financial crime and AML/CFT risks in traditional banking products and services that align with this assessment.[316]

311 FDIC, "QUARTERLY BANKING PROFILE: FIRST QUARTER 2023, (2023, Vol.17, #2) (https://www.fdic.gov/analysis/quarterly-banking-profile/fdic-quarterly/2023-vol17-2/fdic-v17n2-1q2023.pdf.

312 FDIC, QUARTERLY BANKING PROFILE: THIRD QUARTER 2022, (2022, Vol.16, #2) https://www.fdic.gov/analysis/quarterly-banking-profile/fdic-quarterly/2022-vol16-2/fdic-v16n2-1q2022.pdf.

313 FRB, Governor Michelle W. Bowman, "The Consequences of Fewer Banks in the U.S. Banking System", (April 14, 2023) https://www.federalreserve.gov/newsevents/speech/bowman20230414a.htm.

314 As defined in 12 U.S.C. 3302(1).

315 OCC, "Semiannual Risk Perspective", (Fall 2022), https://www.occ.treas.gov/publications-and-resources/publications/semiannual-risk-perspective/files/pub-semiannual-risk-perspective-fall-2022.pdf.

316 OCC, "OCC Report Identifies Key Risks Facing Federal Banking System", (Spring 2023), https://www.occ.treas.gov/publications-and-resources/publications/semiannual-risk-perspective/files/semiannual-risk-perspective-spring-2023.html.

Further, OFAC's sanctions in response to Russia's invasion of the Ukraine in February 2022 are complex and evolving, requiring financial institution management to assess the applicability and impact of sanctions on their institutions and customers, including the impact of sanctions imposed by both the United States and other countries on foreign branches, overseas offices, and subsidiaries.[317]

Case examples

- In October 2023, the Federal Reserve Board (FRB) fined Metropolitan Commercial Bank (MCB), of New York, New York, approximately $14.5 million for violations of customer identification rules and deficient third-party risk management practices relating to the bank's issuance of reloadable prepaid card accounts.[318] In 2020, MCB opened prepaid card accounts for illicit actors using stolen identities who subsequently used the accounts to collect more than $300 million in illegally obtained state unemployment insurance benefits. By opening prepaid card accounts through a third-party program manager without having adequate procedures for verifying each applicant's true identity, MCB violated customer identification rules set forth in the BSA and its implementing regulations. The Board required MCB to improve its customer identification, customer due diligence, and third-party risk management programs.
- In September 2023, FinCEN issued a consent order imposing a civil money penalty of $15,000,000 on Bancrédito International Bank and Trust Corporation, an International Banking Entity operating in Puerto Rico for willfully violating the BSA between October 2015 and May 2022, by failing to timely report suspicious transactions to FinCEN; failing to establish a due diligence program for correspondent accounts established, maintained, administered, or managed in the United States for foreign financial institutions; and failing to implement and maintain an AML program.[319] Bancrédito did not comply with SAR reporting obligations, failing to file SARs for years and ignoring violations cited by its primary regulator, the Puerto Rico Office of the Commissioner of Financial Institutions. These transactions included suspicious activity by a Bancrédito executive and suspicious activity involving customers in the high-risk jurisdiction of Venezuela, including customers linked to foreign bribery and money laundering.
- In September 2023, FinCEN assessed a concurrent civil money penalty of $15 million against Shinhan Bank America (SHBA)for willfully violating the BSA from April 2016 through March 2021, including failure to implement and maintain an effective AML program that was reasonably designed to guard against money laundering and failing to timely report several hundred transactions to FinCEN involving suspicious financial activity by its customers processed by, at, or through the bank.[320] As a result, tens of millions of dollars in suspicious transactions were not reported to FinCEN in a timely manner, including transactions connected to tax evasion, money laundering, and other financial crimes. The FDIC issued a concurrent civil money penalty of $5 million against SHBA for violations of the BSA and its implementing AML regulations and for failure to comply with the requirements of an FDIC-issued consent order dated June 12, 2017.[321] The New York Department of Financial Services also assessed a civil penalty of $10 million for AML-related violations.

317 OCC, "SEMIANNUAL RISK PERSPECTIVE", (Spring 2022), https://www.occ.treas.gov/publications-and-resources/publications/semiannual-risk-perspective/files/pub-semiannual-risk-perspective-spring-2022.pdf.

318 The New York Department of Financial Services also took a joint action against Metropolitan. *See* FRB, "In the Matter of METROPOLITAN COMMERCIAL BANK New York, New York", https://www.federalreserve.gov/newsevents/pressreleases/files/enf20231019a1.pdf.

319 FinCEN, "FinCEN Announces $15 Million Civil Money Penalty against Bancrédito International Bank and Trust Corporation for Violations of the Bank Secrecy Act", (September 15, 2023), https://www.fincen.gov/news/news-releases/fincen-announces-15-million-civil-money-penalty-against-bancredito-international.

320 FinCEN, CONSENT ORDER IMPOSING CIVIL MONEY PENALTY, "IN THE MATTER OF Shinhan Bank America New York, NY: Number 2023-03", https://www.fincen.gov/sites/default/files/enforcement_action/2023-09-29/SHBA_9-28_FINAL_508.pdf.

321 FDIC, "In the Matter of SHINHAN BANK AMERICA NEW YORK, NEW YORK", https://www.fdic.gov/news/press-releases/2023/pr23080a.pdf.

- In April 2023, FinCEN assessed a $1.5 million civil money penalty on South Dakota-chartered The Kingdom Trust Company (Kingdom Trust) for violations of the BSA and its implementing regulations. As part of the consent order, Kingdom Trust admitted that it willfully failed to accurately and timely report hundreds of transactions to FinCEN involving suspicious activity by its customers, including transactions with connections to a trade-based money laundering scheme and multiple securities fraud schemes that were the subject of both criminal and civil actions. These failures stemmed from Kingdom Trust's severely underdeveloped and ad-hoc process for identifying and reporting suspicious activity.[322]
- In January 2023, the FRB issued a civil money penalty on Popular Bank $2.3 million for processing six Paycheck Protection Program (PPP) loans despite "having detected that the loan applications contained significant indications of potential fraud."[323] Specifically, in addition to the processing and funding of the loans, the Bank failed to timely report the potential fraud which demonstrated "ineffective controls and procedures that resulted in violations of the Bank's internal BSA protocols".[324]
- In December 2022, Danske Bank pleaded guilty and agreed to forfeit $2 billion to resolve the United States' investigation into Danske Bank's fraud on U.S. banks related to the Bank's concealment of the state of its AML/CFT controls. According to court documents, Danske Bank defrauded U.S. banks regarding subsidiary Danske Bank Estonia's customers and anti-money laundering controls to facilitate access to the U.S. financial system for Danske Bank Estonia's high-risk customers, who resided outside of Estonia – including in Russia.[325] Specifically, between 2008 and 2016, Danske Bank Estonia – which Danske Bank acquired through an acquisition of Finland-based Sampo Bank in 2007 [326]-- processed $160 billion through U.S. banks on behalf of its high-risk customer base that resided outside of Estonia. By at least February 2014, as a result of internal audits, information from regulators, and an internal whistleblower, Danske Bank knew that some high-risk customers were engaged in highly suspicious and potentially criminal transactions, including transactions through U.S. banks. Danske Bank also knew that Danske Bank Estonia's anti-money laundering program and procedures did not meet Danske Bank's standards and were not appropriate to meet the risks associated with the high-risk customers. Instead of providing the U.S. banks that processed Danske Bank's transactions with truthful information, Danske Bank lied about the state of Danske Bank Estonia's AML compliance program, their transaction monitoring capabilities, and information regarding Danske Bank Estonia's customers and their risk profiles. Danske Bank did this allegedly to continue to gain access to the U.S. financial system.[327]
- In October 2022, OFAC issued a Finding of Violation to Nodus International Bank, an international financial entity in Puerto Rico, for violations of the Venezuelan Sanctions Regulations and the Reporting, Penalties, and Procedures Regulations. According to OFAC documentation, upon

322 FinCEN, "FinCEN Assesses $1.5 Million Civil Money Penalty against Kingdom Trust Company for Violations of the Bank Secrecy Act", (April 26, 2023), https://www.fincen.gov/news/news-releases/fincen-assesses-15-million-civil-money-penalty-against-kingdom-trust-company.

323 FRB, "Federal Reserve Board announces it has fined Popular Bank $2.3 million for processing six PPP loans despite having detected that the loan applications contained significant indications of potential fraud," (January 24, 2023), https://www.federalreserve.gov/newsevents/pressreleases/enforcement20230124a.htm.

324 FRB, Order of Assessment of Civil Money Penalty, "In the Matter of Popular Bank, New York, New York", (January 20, 2023), https://www.federalreserve.gov/newsevents/pressreleases/files/enf20230124a1.pdf.

325 DOJ, "Danske Bank Pleads Guilty to Fraud on U.S. Banks in Multi-Billion Dollar Scheme to Access the U.S. Financial System", (December 13, 2022) https://www.justice.gov/opa/pr/danske-bank-pleads-guilty-fraud-us-banks-multi-billion-dollar-scheme-access-us-financial.

326 DOJ, SDNY, USA v. Danske Bank, https://www.justice.gov/d9/press-releases/attachments/2022/12/13/danske_information_508_compliant_0.pdf.

327 DOJ, "Danske Bank Pleads Guilty to Fraud on U.S. Banks in Multi-Billion Dollar Scheme to Access the U.S. Financial System", (December 13, 2022), https://www.justice.gov/opa/pr/danske-bank-pleads-guilty-fraud-us-banks-multi-billion-dollar-scheme-access-us-financial.

determining that a designated individual held an interest in certain securities, Nodus sought to redeem the designated person's securities and place the proceeds into a blocked account, a process that would require a license from OFAC. Nodus compliance personnel relayed this to senior Nodus bank officials, but Nodus processed the securities redemption without a license. Separately, the designated individual also held other accounts and financial products at Nodus, which were blocked upon learning of the individual's designation. However, due to human error Nodus allowed an automatic debit from one of the blocked accounts to credit the designated person's blocked credit card account – the balance of which was written off by Nodus. Additionally, during the OFAC investigation, Nodus informed OFAC that the Bank lacked access to all records or communications related to the handling of the designated person's blocked property. The Bank also submitted several inconsistent Annual Reports of Blocked Property to OFAC.[328]

- In September 2022, the OCC assessed a $6 million civil money penalty against Sterling Bank and Trust, FSB, Southfield, Michigan. According to the consent order, in addition to prudential deficiencies, the Bank failed to implement an adequate system of AML/CFT internal controls and failed to file SARs in a timely manner.[329]
- In July 2022, OFAC announced that it reached an agreement with American Express National Bank (Amex), a subsidiary of the American Express Company that provides charge and credit card products and travel-related services to consumers and businesses, to settle the potential civil liability for 214 apparent violations of OFAC's Kingpin sanctions. According to OFAC documentation, Amex processed transactions for an account whose supplemental card holder was designated. A combination of human error and sanctions compliance program deficiencies enabled the account to process $155,189.42 worth of transactions.[330]
- In July 2022, OFAC issued a Finding of Violation to MidFirst Bank (MidFirst) for violations of the Destruction Proliferators Sanctions Regulations (WMDPSR). According to OFAC documentation, MidFirst maintained accounts for and processed 34 payments on behalf of two individuals added to OFAC's SDN List for 14 days post-designation. The violations stemmed from the Bank's misunderstanding of the frequency of its vendor's screening of new names added to the SDN List against its existing customer base; the vendor only engaged in screening of MidFirst's entire existing customer base once a month instead of daily.[331]
- In June 2022, the FDIC issued a consent order regarding Oxford University Bank of Oxford, Mississippi.[332] The order required the bank, among other things, to: (1) assess AML/CFT department staffing; (2) appoint a BSA officer; (3) develop, adopt, and implement appropriate CDD procedures; (4) develop and establish a system of internal controls; (5) establish and maintain an independent testing program for compliance with the BSA and its implementing rules and regulations; (6) develop an effective training program and revise the Bank's AML/CFT Risk Assessment; and (7) develop, adopt, and implement revised procedures and processes for monitoring and reporting suspicious activity.

328 OFAC, "OFAC Issues a Finding of Violation to Nodus International Bank, Inc. for Violations of the Venezuelan Sanctions Regulations and the Reporting, Penalties and Procedures Regulations" (October 18, 2022), https://ofac.treasury.gov/media/928941/download?inline#:~:text=The%20RPPR%20violations%20reflected%20Nodus's,of%20a%20civil%20monetary%20penalty.

329 OCC, Consent Order, "In the Matter of: Sterling Bank and Trust, FSB Southfield, Michigan", https://www.occ.gov/static/enforcement-actions/ea2022-039.pdf.

330 OFAC, "OFAC Settles with American Express National Bank for $430,500 Related to Apparent Violations of Foreign Narcotics Kingpin Sanctions Regulations" (July 15, 2022), https://ofac.treasury.gov/media/924406/download?inline.

331 OFAC, "OFAC Issues Finding of Violation to MidFirst Bank", (July 21, 2022) https://ofac.treasury.gov/media/924506/download?inline.

332 FDIC, Consent Order, "In the Matter of OXFORD UNIVERSITY BANK, OXFORD, MISSISSIPPI."

In April 2022, the OCC issued a consent order to Anchorage Digital Bank of Sioux Falls, South Dakota. The order found that Anchorage Digital Bank – a bank specializing in virtual assets – "failed to adopt and implement a compliance program that adequately covers the required AML/CFT program elements." The specific deficiencies that the Bank did not adopt and implement included: internal controls for customer due diligence and procedures for monitoring suspicious activity; appointment of BSA officer and staff; and training." [333]

2. Money Services Businesses

The term "money services business" is defined by regulation[334] as any of the following categories of business: (1) dealers in foreign exchange; (2) check cashers; (3) issuers or sellers of traveler's checks or money orders; (4) providers of prepaid access; (5) money transmitters; (6) U.S. Postal Service; or (7) sellers of prepaid access.[335] MSBs are non-bank financial institutions often used by customers who may have difficulty obtaining financial services at banks as well as those that send remittance payments abroad to family members in a cost-effective manner. Notably, the United States is the world's largest source of remittances, having sent approximately $72.1 billion abroad in 2021.[336]

There are approximately 26,472 registered MSBs in the United States,[337] as of December 15, 2023. MSBs, which are commonly used in the U.S. are continuously innovating, leveraging mobile and internet-based options to ensure convenient payment of funds across the world. Hundreds of MSBs offer services in virtual assets, and many VASPs in the United States are registered as MSBs.

IRS Small Business/Self Employed (SB/SE) is the entity delegated by FinCEN to examine MSBs compliance with obligations under the BSA. There has been no change to the previously reported decrease in principal exams by IRS SB/SE and the current examiner force is still half of what it was in 2010. In investigations in which IRS-CI is involved, 18 USC 1960 is often cited regarding unlicensed MSBs, specifically as a predicate offense in virtual currency cases involving money laundering charges. (*see* Virtual Asset Vulnerabilities for cases involving MSBs and other financial institutions offering virtual asset services).

In 2022, depository institutions submitted almost 3,580 SARs, citing potential unlicensed MSB activity.[338] Almost half of the SARs (49 percent) were filed in California, New York, Ohio, Texas, North Carolina, and Virginia collectively.[339] Many institutions identified grocery or convenience stores, gas stations, or liquor stores as potentially operating illegally as money transmitters, check cashers, or dealers in foreign exchange.[340] Additionally, individuals may misuse their personal or business bank accounts to transmit funds for customers on a commercial scale, thus operating as unregistered MSBs.

333 OCC, Consent Order, "In the Matter of: Anchorage Digital Bank, National Association Sioux Falls, South Dakota", https://www.occ.gov/static/enforcement-actions/ea2022-010.pdf.

334 31 C.F.R. § 1010.100(ff). See also https://www.fincen.gov/am-i-msb.

335 See previous sections for vulnerabilities unique to check, money orders, and providers and sellers of prepaid access.

336 CRS, Remittances: Background and Issues for the 118th Congress, (May 10, 2023), https://sgp.fas.org/crs/misc/R43217.pdf; https://www.worldbank.org/en/news/press-release/2023/12/18/remittance-flows-grow-2023-slower-pace-migration-development-brief.

337 FinCEN, MSB Registrant Search, https://www.fincen.gov/msb-state-selector.

338 FinCEN, Depository Institution, Exhibit 5, Line 102, https://www.fincen.gov/reports/sar-stats/sar-filings-industry.

339 FinCEN, Depository Institution, Exhibit 3, Lines 15-20, https://www.fincen.gov/reports/sar-stats/sar-filings-industry.

340 GAO, "VIRTUAL CURRENCIES: Additional Information Could Improve Federal Agency Efforts to Counter Human and Drug Trafficking" (December 2021), https://www.gao.gov/assets/gao-22-105462.pdf.

Unregistered and unlicensed MSBs can include hawalas and other forms of IVTS. There is no practical or functional distinction between a hawala and any other money transmitter. While it is theoretically possible for IVTS to operate wholly outside the banking system, it is not often the case. Instead, law enforcement investigations indicate IVTS often use an account at a bank to clear and settle transactions internationally. The following are case examples of AML/CFT compliance failures and unregistered or unlicensed MSBs.

Case Examples

- In September 2023, Ryan Salame, the co-CEO of FTX's Bahamian affiliate (FTX Digital Markets Ltd.), pleaded guilty to a conspiracy to make unlawful political contributions and defraud the Federal Election Commission and a conspiracy to operate an unlicensed money transmitting business.[341] Between 2019 and 2021, Salame along with other co-conspirators, owned and operated an unlicensed money-transmitting business to transmit customer deposits of virtual assets and traditional currencies on and off the FTX exchange. Salame opened a fraudulent bank account by using false and misleading statements on the bank's due diligence questionnaire. Ultimately, Salame agreed to forfeit more than $1.5 billion to authorities.[342]
- In June 2023, a Paraguayan man admitted his role in facilitating an international money laundering conspiracy; he pled guilty to one count of operating an unlicensed money-transmitting business. According to court documentation, the individual was the owner and operator of a money exchange business in the Republic of Paraguay, which was not licensed or registered to operate as a money-transmitting business under the laws of the United States or the state of New Jersey. The individual's associates traveled to New Jersey and Florida and accepted approximately $800,000 in U.S. currency from purported drug traffickers and caused those funds to be transmitted through the individual's money exchange business. Using the unlicensed business, the individual caused those funds to be transmitted through accounts located in multiple countries and ultimately caused the funds to be transferred back to an account maintained by the purported drug traffickers. To disguise the illicit source of funds, the individual and his associates coordinated to generate fraudulent invoices that stated legitimate business reasons for the transfers of the laundered funds. Unbeknownst to the individual and one of his associates, the currency they accepted was actually from two undercover FBI agents as part of an undercover investigation of the money laundering network.[343]
- In June 2023, in Massachusetts, a man was charged with money laundering in connection with an alleged unlicensed money transmitting business. The business was allegedly responsible for converting more than $1 million in cash to bitcoin - largely on behalf of scammers and drug dealers. The defendant used his vending machine business and encrypted messaging apps to secretly communicate with customers.[344]
- In May 2023, in Florida, the president, chief executive officer, and founder of Aurae Lifestyle and Club Swann was charged with illegally operating an unlicensed money-transmitting business. The defendant provided fiat and virtual asset financial services to customers through his different lines of

341 DOJ, "Statement Of U.S. Attorney Damian Williams On The Guilty Plea Of Ryan Salame, Former CEO Of FTX", (September 7, 2023), https://www.justice.gov/usao-sdny/pr/statement-us-attorney-damian-williams-guilty-plea-ryan-salame-former-ceo-ftx.

342 Reuters, "Former Bankman-Fried lieutenant Salame pleads guilty to illegal campaign contributions," (September 8, 2023), https://www.reuters.com/legal/ex-ftx-executive-salame-due-us-court-expected-guilty-plea-2023-09-07/.

343 DOJ, "Paraguayan National Admits Unlicensed Money Transmitting in Connection with International Money Laundering Investigation", (June 23, 2022), https://www.justice.gov/usao-nj/pr/paraguayan-national-admits-unlicensed-money-transmitting-connection-international-money.

344 DOJ, "Danvers Man Arrested for Money Laundering and Operating Unlicensed Money Transmitting Business", (June 12, 2023), https://www.justice.gov/usao-ma/pr/danvers-man-arrested-money-laundering-and-operating-unlicensed-money-transmitting.

business. The conspiracy charge carries a fine up to $250,000.[345]

In May 2023, an individual was indicted in the Northern District of Georgia on one count of operating an unlicensed money transmitting business and 39 accounts of money laundering. According to the indictment and other information presented in court, the individual allegedly registered eight companies in Georgia, that were used to transmit over $150 million in a series of 1,300 transactions. The companies were purportedly headquartered in Buford, Georgia, and Dacula, Georgia but the companies did not generate typical business expenses or maintain employees. The money was used, in part, to purchase more than $65 million in overseas gold bullion. The individual, a Russian citizen who resides in North Georgia, allegedly transferred millions overseas from multiple bank accounts in Georgia. [346]

In April 2023, four defendants were indicted for wire fraud, mail fraud, money laundering, transacting in criminal proceeds, tax evasion, and conducting an unlawful money transmitting business. The defendants used online romance scams and apartment rental scams to collect money from over 100 victims, which totaled about $4.5 million in illicit funds. Afterward, one of the defendants used an international hawala system to transfer the illicit funds from his U.S. bank accounts to overseas accounts in Nigeria and Turkey.[347]

In July 2022, Ping Express U.S. LLC (Ping) – a money transfer company – pleaded guilty to failure to maintain an effective anti-money laundering program. According to court documents, Ping failed to file a single report over a three-year period, despite its requirement to report suspicious transactions to regulators. Ping also admitted that it conducted money transmission business in states in which it was not licensed to do so; the company claimed to have software that could detect and deter transmissions initiated in "unlicensed" states, but the software did not function. Additionally, the company transmitted more than $167 million overseas, including $160 million to Nigeria, of which it admitted it failed to seek sufficient details about the sources or purposes of the funds involved in the transactions or the customers initiating the transmissions. According to the HSI investigation, some of the funds Ping transmitted were illegally derived.[348]

3. Securities Broker-Dealers and Mutual Funds

Broker-dealers and mutual funds have AML/CFT obligations under the BSA and their implementing regulations. In its 2024 Examination Priorities, the SEC reiterated that it will continue to focus on AML/CFT programs to review whether broker-dealers and certain registered investment companies are: (1) appropriately tailoring their AML program to their business model and associated AML risks; (2) 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.[349] The SEC also noted that it will review policies and procedures to oversee applicable financial intermediaries during examinations

345 IRS, "Businessman charged with conspiring to own unlicensed money transmitting business", (May 25, 2023), https://www.irs.gov/compliance/criminal-investigation/businessman-charged-with-conspiring-to-own-unlicensed-money-transmitting-business.

346 DOJ, "Russian charged with money laundering and illegally transmitting more than $150 million", (May 1, 2023), https://www.justice.gov/usao-ndga/pr/russian-charged-money-laundering-and-illegally-transmitting-more-150-million.

347 IRS, "Four people indicted for roles in romance and internet frauds, illegal money transmitting" (April 13, 2023), https://www.irs.gov/compliance/criminal-investigation/four-people-indicted-for-roles-in-romance-and-internet-frauds-illegal-money-transmitting.

348 DOJ, "Money Transfer Company Ping Pleads Guilty to Failure to Combat Money Laundering", (July 7, 2022), https://www.justice.gov/usao-ndtx/pr/money-transfer-company-ping-pleads-guilty-failure-combat-money-laundering.

349 SEC, "FISCAL YEAR 2024 EXAMINATION PRIORITIES", https://www.sec.gov/files/2024-exam-priorities.pdf.

of certain registered investment companies. Additionally, the 2023 Examination Priorities highlighted the elevated risk for broker-dealers and certain registered investment companies due to the current geopolitical environment and the increased imposition of OFAC and international sanctions.[350]

The Financial Industry Regulatory Authority (FINRA), a self-regulatory organization responsible for examining broker-dealers in the United States, notes a variety of emerging money laundering risk areas: manipulative trading in small cap initial public offerings (IPOs); sanctions evasion; and automated customer account transfer service (ACATS Fraud).[351] Overall, recent enforcement actions by regulatory authorities indicate that broker-dealers and certain registered investment companies demonstrated failures linked to a lack of SAR filings, independent testing, or establishment and implementation of an AML program, among other issues.

Case examples

- In September 2023, the SEC announced charges against registered investment adviser DWS Investment Management Americas Inc. (DIMA or DWS), a subsidiary of Deutsche Bank AG, for its failure to develop a mutual fund AML/CFT program. The SEC's order found that DIMA caused mutual funds it advised to fail to develop and implement a reasonably designed AML program to comply with the BSA and applicable FinCEN regulations. The order also found that DIMA caused such mutual funds' failure to adopt and implement policies and procedures reasonably designed to detect activities indicative of money laundering and to conduct AML/CFT training specific to the mutual funds' business.[352]
- In July 2023, the SEC announced charges against Merrill Lynch, Pierce, Fenner & Smith (Merrill Lynch), and its parent company BAC North America Holding Co. (BACNAH) for failing to file hundreds of SARs from 2009 to late 2019. According to the SEC's order, BACNAH assumed responsibility for Merrill Lynch's SAR policies and procedures and for filing their SARs. Over the course of a decade, BACNAH improperly used a $25,000 threshold instead of the required $5,000 threshold for reporting suspicious transactions or attempted transactions where a suspect may have been seeking to use Merrill Lynch to facilitate criminal activity. As a result, BACNAH caused Merrill Lynch to fail to file hundreds of required SARs.[353]
- In March 2023, the SEC announced settled charges against Utah-based brokerage firm Cambria Capital, LLC, for failing to file SARs on numerous transactions. The SEC's order finds that from March 2017 through May 2019, Cambria failed to file SARs on suspicious activity that raised red flags identified in the firm's anti-money laundering policies and procedures. According to the SEC's order, most of the suspicious activity was associated with the liquidation of microcap securities, including the deposit of physical certificates; the liquidation of large quantities of microcap securities; and the immediate wire out of liquidation proceeds from customer accounts. In addition, the order also finds that in many of these transactions, the pattern of liquidations often occurred in combination with other red flags noted in Cambria's policies and procedures, such as unusually large deposits; suspicious wire activity; or multiple accounts simultaneously trading in the same microcap security.[354]

350 SEC, "FISCAL YEAR 2023 EXAMINATION PRIORITIES", https://www.sec.gov/files/2023-exam-priorities.pdf.

351 FINRA, "Regulatory Obligations and Related Considerations", https://www.finra.org/rules-guidance/guidance/reports/2023-finras-examination-and-risk-monitoring-program/aml.

352 See SEC, "Deutsche Bank Subsidiary DWS to Pay $25 Million for Anti-Money Laundering Violations and Misstatements Regarding ESG Investments" (Sept. 25, 2023), https://www.sec.gov/news/press-release/2023-194.

353 SEC, "SEC Charges Merrill Lynch and Parent Company for Failing to File Suspicious Activity Reports", (July 11, 2023), https://www.sec.gov/news/press-release/2023-128.

354 SEC, "SEC Charges Broker-Dealer with Failing to Report Suspicious Transactions", (March 2, 2023), https://www.sec.gov/enforce/34-97020-s.

- In May 2022, the SEC announced charges against Wells Fargo Advisors for failing to file at least 34 SARs in a timely manner between 2017 and October 2021. According to the SEC's order, due to Wells Fargo Advisors' deficient implementation and failure to test a new version of its internal AML transaction monitoring and alert system adopted in January 2019, the system failed to reconcile the different country codes used to monitor foreign wire transfers. As a result, Wells Fargo Advisors did not timely file at least 25 SARs related to suspicious transactions in its customers' brokerage accounts involving wire transfers to or from foreign countries that it determined to be at high or moderate risk for money laundering, terrorist financing, or other illegal money movements. The order also found that beginning in April 2017, Wells Fargo Advisors failed to timely file at least nine additional SARs due to a failure to appropriately process wire transfer data into its AML transaction monitoring system in certain other situations.[355]

4. Complicit Professionals

As indicated in other sections of this report and previous NMLRAs, money laundering can be perpetrated by complicit insiders who abuse their positions of trust and access across professions and corporate structures to engage or facilitate illicit financial activity. Criminals continue to seek out complicit professionals, including those in the financial services sector. This is an acute problem because such complicit financial services professionals may undermine an institution's AML/CFT compliance program.

Case examples

- In January 2024, Peter McVey, who served as vice president and director of treasury services for a Missouri bank, pleaded guilty to failing to maintain an appropriate anti-money laundering program under the BSA. According to court documents, between April 2014 and July 2022, McVey assisted high-risk bank customers engaged in deceptive sweepstakes and short-term online loan activities in evading the bank's AML/CFT controls. Specifically, McVey worked with other bank officials and customers to submit fraudulent CTR exemption forms to FinCEN and knowingly accepted forged bank forms from customers that permitted them to exceed applicable limits on daily transaction values. McVey also admitted that he did not follow KYC or SAR requirements.[356]
- In October 2023, a New Jersey-based employee of an international financial institution was arrested for accepting bribes to facilitate millions of dollars of money laundering.[357] According to documents filed in this case and statements made in court, in early 2022, the employee exploited his position as a bank employee to facilitate money laundering activities in exchange for bribes. The employee used his position and inside access to open bank accounts in the names of shell companies with nominee owners. Those accounts were then used to launder narcotics proceeds, including to Colombia. The employee allegedly assisted the money laundering efforts by giving those who bribed him online access to the accounts, along with dozens of debit cards for the accounts that were later used to withdraw cash from ATMs in Colombia. The employee allegedly received thousands of dollars in bribes for each account he opened. The investigation has revealed that millions of dollars were laundered to Colombia through accounts opened by the employee since early 2022.

355 SEC, "SEC Charges Wells Fargo Advisors with Anti-Money Laundering Related Violations", (May 20, 2022), https://www.sec.gov/news/press-release/2022-85.

356 DOJ, "Former Banking Executive Pleads Guilty to Evading Anti-Money Laundering Regulations," (January 17, 2024), https://www.justice.gov/opa/pr/former-banking-executive-pleads-guilty-evading-anti-money-laundering-regulations.

357 DOJ, "Bank Insider Charged with Accepting Bribes to Facilitate Millions of Dollars of Money Laundering" (October 30, 2023), https://www.justice.gov/usao-nj/pr/bank-insider-charged-accepting-bribes-facilitate-millions-dollars-money-laundering.

- In March 2023, Stephen Roland Reyna, a former bank branch manager, was ordered to federal prison for helping a drug trafficking ring launder money through his bank. Reyna was the manager of a bank branch in Harlingen, Texas. While serving in that position and utilizing his position and knowledge of the banking industry, he assisted a drug trafficking organization in laundering $410,000 in drug sale proceeds. The organization would transport multi-kilogram cocaine loads from the Rio Grande Valley to northern states. Upon successful delivery, thousands of dollars in drug proceeds would then be dispersed through multiple bank accounts in the northern states. Reyna would coordinate with multiple co-conspirators in the Rio Grande Valley to launder the funds through their bank accounts. Reyna ensured the proceeds were successfully withdrawn from his branch in Harlingen. Co-conspirators would frequently pay Reyna in cash right after he helped them get their drug proceeds out of the bank.[358]

Luxury and High-Value Goods

Purchases of high-value assets, such as real estate, precious metals, stones, jewels, art, automobiles and other types of vehicles are another strategy that criminals and TCOs use. By holding the value of their proceeds in a moveable commodity that later can be sold elsewhere, traffickers can convert the proceeds to currency in a different country. As noted above, CMLOs and other criminal organizations are known to export high-value goods purchased with criminal proceeds from the United States where they resell the goods for a profit. Sales documentation can provide a veil of legitimacy should a financial institution seek to understand the source of a client's funds.

1. Real Estate

The U.S. real estate market is one of the largest and most valuable real estate markets in the world and is attractive to both domestic and international buyers. In 2023, the U.S. residential market is estimated to be valued at $47 trillion,[359] and numerous U.S. cities including New York, Los Angeles, San Francisco, Dallas, Washington D.C., and Boston are amongst the top ten leading commercial real estate market hubs in the world.[360] The relative stability of the U.S. real estate market and its historic reputation as a reliable store of long-term value has traditionally attracted both legitimate interest and those looking to find a reliable mechanism to launder money. Money laundering through real estate can negatively affect home prices, particularly since illicit actors seeking to integrate illicit funds may be willing to over or under pay for a property. According to a Commission in British Columbia, Canada, this activity can distort the market and disadvantage legitimate buyers and sellers.[361]

The financed portion of the U.S. real estate market is well-regulated and banks and non-bank lenders that issue residential and commercial mortgages and housing-related government-sponsored

358 DOJ, "Local banker sent to prison for money laundering conspiracy", (March 8, 2023), https://www.justice.gov/usao-sdtx/pr/local-banker-sent-prison-money-laundering-conspiracy.

359 RedFin, "U.S. Housing Market Recovers the Nearly $3 Trillion It Lost, Hitting Record $47 Trillion in Total Value," (Updated on August 31st, 2023), https://www.redfin.com/news/housing-market-value-hits-record-high-2023/.

360 Mordor Intelligence, U.S. Residential Real Estate Market Size & Share Analysis - Growth Trends & Forecasts (2023 - 2028), https://www.mordorintelligence.com/industry-reports/residential-real-estate-market-in-usa., 16 U.S. Metros Are in Top 30 Largest Commercial Markets Globally in 2020; NYC is the Number One CRE Market, April 2021, https://www.nar.realtor/blogs/economists-outlook/16-u-s-metros-are-in-top-30-largest-commercial-markets-globally-in-2020-nyc-is-the-number-one-cre.

361 See The Honourable Austin F. Cullen, Commission of Inquiry into Money Laundering in British Columbia, (June 3, 2022), https://cullencommission.ca/files/reports/CullenCommission-FinalReport-Full.pdf.

enterprises, must establish AML/CFT programs and file SARs.[362] However, an estimated 20 to 30 percent of residential real estate purchases in the United States are non-financed and not fully subject to comprehensive AML/CFT requirements.[363] Since 2002, "persons involved in real estate closings and settlements" have received a temporary exemption from compliance as a financial institution from FinCEN and are exempt from instituting and maintaining comprehensive AML/CFT programs.[364] Because of the key role real estate professionals play in closings and settlements, this is a critical vulnerability, and real estate professionals have been found to act as both witting and unwitting participants in money laundering schemes. Currently, under FinCEN's Real Estate Geographic Targeting Order (GTO),[365] in effect since 2016, title insurance companies involved in the non-financed purchase of residential real estate by a legal entity in select jurisdictions are required to report the legal entity's beneficial ownership information. FinCEN has utilized this tool to gather information about vulnerabilities in the non-financed market, and the Real Estate GTOs currently cover 69 counties.[366] However, GTOs are time-limited and location-specific and remain a temporary solution to information gaps. In December 2021, the Treasury issued an advance notice of proposed rulemaking (ANPRM) to solicit public feedback on how to address the risks associated with this sector. Building on this information and public feedback, FinCEN has an NPRM in OMB review that will continue the process of addressing money laundering vulnerabilities in the residential real estate sector.

Predicate offenses for money laundering through real estate continue to involve domestic and transnational activity, including narcotics trafficking, corruption, human trafficking, fraud, and sanctions evasion.[367] Illicit actors often make non-financed purchases using legal vehicles or arrangements designed to obfuscate the purchaser's identity and source of funds to integrate ill-gotten proceeds into the formal economy.

Additional factors that make the U.S. real estate market vulnerable to money laundering include the ease through which illicit actors can anonymize their identity or the source of their funds through legal entities, legal arrangements, and pooled accounts like IOLTAs. Money laundering typologies include the use of nominees and gatekeepers[368] to facilitate transfers without revealing the identity of the true owner

362 31 USC § 5318 (g),(h).

363 "Anti-Money Laundering Regulations for Real Estate Transactions," Federal Register (December 8, 2021), https://www.federalregister.gov/documents/2021/12/08/2021-26549/anti-money-laundering-regulations-for-real-estate-transactions. See also FinCEN, "Statement of FinCEN Acting Director Himamauli Das before the House Committee on Financial Services," (April 7, 2023).

364 67 FR 21110: FinCEN Interim final rule 'Anti-Money Laundering Programs for Financial Institutions'; 31 CFR §1010.205(b)(v)

365 FinCEN, "FAQ: Geographic Targeting Orders Involving Certain Real Estate Transactions", (April 21, 2023), https://www.fincen.gov/sites/default/files/shared/508_FAQ_April2023REGTO.pdf.

366 FinCEN, "FinCEN Renews and Expands Real Estate Geographic Targeting Orders", (October 20, 2023), https://www.fincen.gov/news/news-releases/fincen-renews-and-expands-real-estate-geographic-targeting-orders-2.

367 CRS, Money Laundering in the real estate sector, (January 4, 2022), https://sgp.fas.org/crs/misc/IF11967.pdf.

368 The term "gatekeepers" refers to financial facilitators that have the "ability to furnish access (knowingly or unwittingly) to the various functions that might help the criminal with funds to move or conceal". *See FATF Report on Money Laundering Typologies 2000-2001*, February 1, 2001, available at http://www.fatf-gafi.org/dataoecd/29/36/34038090.pdf. The Treasury Department has used the term gatekeeper in prior risk assessments and public remarks. *See, e.g.,* Remarks by Assistant Secretary for Terrorist Financing and Financial Crimes Elizabeth Rosenberg at The Brookings Institution, September 7, 2022, available at https://home.treasury.gov/news/press-releases/jy0938 (observing that the 2022 National Money Laundering Risk Assessment examined concerns around "financial facilitators – sometimes known as gatekeepers – that move…dirty money along"). The term's application to illicit finance was coined at the 1999 meeting of the G-8 Finance Ministers. *See* Ministerial Conference of the G-8 Countries on Combating Transnational Organized Crime (October 19-20, 1999), Communique, available at http://www.justice.gov/criminal/cybercrime/g82004/99MoscowCommunique.pdf.

or source of funds for the property, the use of all-cash payments to avoid the AML/CFT scrutiny that comes with financing, the use of loan-back mortgage schemes to reintegrate illicit proceeds into the licit economy, over or under paying for real estate, and the successive transfer of real estate at a higher value or between legal entities and arrangements or natural persons, sometimes for no consideration.[369]

As highlighted in FinCEN's January 2023 alert on "Potential U.S. Commercial Real Estate Investments by Sanctioned Russian Elites, Oligarchs and their Proxies," the commercial real estate sector is also exposed to risk, as it is common to use purpose-built legal entities, indirect ownership chains, multiple types of ownership and financing options, and the presence of multiple parties to each commercial real estate transfer, each of which can obscure an owner's identity and source of funds.[370]

Further, the anonymity of ownership in the residential and commercial real estate markets presents both a money laundering and a national security risk because it can help facilitate sanctions evasion, corruption, and even espionage. A 2016 GAO report found that ownership information for 1406, or one-third of high-security General Services Administration (GSA)-leased commercial real estate spaces was unavailable. The report found that some of these spaces were rented by foreign companies based in Canada, China, Israel, Japan, and South Korea, all countries that may have an interest in obtaining information about U.S. government-owned facilities. Beginning in 2018, a series of actions culminating with the passage of the Secure Federal Leases from Espionage and Suspicious Entanglements Act of 2020 requires collecting foreign ownership information, including beneficial ownership information of foreign-owned high-security commercial real estate leased by the GSA.[371]

Case examples

- In April 2023, Robert Wise, a New York-based attorney, pleaded guilty to paying on behalf of sanctioned Russian oligarch, Viktor Vekselberg, nearly four million dollars to help him maintain his ownership of six properties in the United States. The properties in question were (i) two apartments on Park Avenue in New York, New York, (ii) an estate in Southampton, New York, (iii) two apartments on Fisher Island, Florida, and (iv) a penthouse apartment also on Fisher Island, Florida. The properties were all acquired using a series of shell companies prior to Vekselberg's OFAC designation. Before his designation, accounts associated with Vekselberg sent 90 wire payments totaling $18.5 million to Wise's IOLTA. After Vekselberg's designation as an SDN, Wise's IOLTA started to receive payments from an account in the Bahamas held in the name of a shell company, Smile Holding Ltd., that was controlled by Vekselberg's longtime associate, Vladimir Voronchenko and from another Russian bank account held by a Russian national related to Voronchenko. Between approximately June 2018 and March 2022, Wise's IOLTA received around 25 wire transfers totaling $3.8 million. Wise used these funds to maintain and service Vekselberg's properties knowing that he was violating ongoing U.S. sanctions.[372]

369 Lakshmi Kumar, Kaisa de Bel, Global Financial Integrity, August 2021, Acres of Money Laundering, https://34n8bd.p3cdn1.secureserver.net/wp-content/uploads/2021/08/Acres-of-Money-Laundering-Final-Version-2021.pdf?time=1698916839.

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

371 Secure Federal Leases from Espionage and Suspicious Entanglements Act, Public Law 116–276, 134 Stat. 3362 (2020) (the "Secure Federal LEASEs Act").

372 DOJ, "New York Attorney Pleads Guilty to Conspiring to Commit Money Laundering to Promote Sanctions Violations by Associate of Sanctioned Russian Oligarch," (April 25, 2023), https://www.justice.gov/opa/pr/new-york-attorney-pleads-guilty-conspiring-commit-money-laundering-promote-sanctions.

- In January 2023, a Miami federal grand jury indicted a Venezuelan Supreme Court justice for conspiring to launder bribes he received in exchange for using his position to resolve civil and criminal cases in Venezuela to favor bribe payers. It is alleged that the justice received more than $10 million in bribes, typically from Venezuelan contractors who had received contracts from Venezuelan government-owned entities. The individual allegedly used the bribe proceeds to purchase or renovate real estate around the world, including a villa in Tuscany, Italy, for 2.4 million euros, a luxury villa in La Romana, Dominican Republic, for $1.5 million; a building in Las Mercedes in Caracas, Venezuela, for $1.3 million, and an apartment in Miami for $1.3 million. He also used the bribe proceeds for cars, luxury goods, expensive travel, and musical entertainment.[373]
- In December 2022, a Russian intelligence agent designated by OFAC was charged with conspiracy to violate the International Emergency Economic Powers Act, bank fraud conspiracy, money laundering conspiracy, and four counts of money laundering in connection with the purchase and maintenance of two condominiums in Beverly Hills, California. As alleged in the indictment, beginning in 2013, the individual and a co-conspirator devised a scheme to purchase and maintain two luxury condominiums in Beverly Hills while concealing his interest in the transactions from U.S. financial institutions. Specifically, the individual used the services of a corporate nominee, a multi-tiered structure of California-based shell companies, and numerous U.S. bank and brokerage accounts. Using this framework, the individual wired approximately $3.92 million to the nominee from overseas accounts in Latvia and Switzerland belonging to companies registered in the British Virgin Islands. The suspect then used the money to pay $3.2 million in cash for real estate in the name of a corporate entity set up by the nominee, with the individual having no visible affiliation with the purchase. The remaining $800,000 was invested in a brokerage account maintained by the nominee and used to pay expenses for the condominiums.[374]
- In November 2022, an individual in Delaware was sentenced to 45 years in prison for conspiracy to commit money laundering, conspiracy to distribute cocaine, and various other drug and money laundering offenses. According to court records and evidence presented at trial, between 2009 and 2017, the individual and his wife laundered over a million dollars in drug proceeds through the purchase of real estate in Delaware and Pennsylvania using their company, Zemi Property Management. They deposited drug money into several different bank accounts – and asked their friends and family members to do the same – and then used those funds to buy cashier's checks that funded the property purchases.[375]

2. Precious Metals, Stones, and Jewels

The precious metals, stones, and jewels (PMSJs) industry in the United States presents varying money laundering risks.[376] Persons involved include large-scale mining interests, artisanal and small-scale mining, traders, refiners, manufacturers, designers, retailers, and secondary markets such as auction

373 DOJ, "Former President of Venezuelan Supreme Court Indicted on Charges of Accepting Bribes to Resolve Court Cases," (January 26, 2023), https://www.justice.gov/usao-sdfl/pr/former-president-venezuelan-supreme-court-indicted-charges-accepting-bribes-resolve.

374 DOJ, "Russian Intelligence Agent Charged with Fraud and Money Laundering in Connection with Purchase and Use of Luxury Beverly Hills Real Estate," https://www.justice.gov/usao-edny/pr/russian-intelligence-agent-charged-fraud-and-money-laundering-connection-purchase-and.

375 DOJ, Delaware Man Sentenced to 45 years in Federal Prison for Trafficking over 150 Kilograms of Cocaine and Laundering the Proceeds, (November 23, 2022), https://www.justice.gov/usao-de/pr/delaware-man-sentenced-45-years-federal-prison-trafficking-over-150-kilograms-cocaine-and.

376 U.S. Bureau of Statistics, Occupational Employment and Wage Statistics, (May 2022), https://www.bls.gov/oes/current/oes519071.htm.

houses and pawnshops.[377] "Dealers" of PMSJs - or a person who both buys and sells covered goods - are required to develop and implement AML/CFT programs reasonably designed to prevent the dealer from being leveraged to facilitate money laundering and terrorist financing if they meet a $50,000 annual threshold for both the purchase and sale of PMSJs in the preceding calendar or tax years, with some exceptions for those who sell primarily to the U.S. public.[378] While PMSJ dealers are subject to some BSA reporting requirements, vulnerabilities for bad actors seeking to launder their illicit proceeds remain.[379]

PMSJs are an attractive money laundering vehicle due to their high value, high value to low mass ratio, stable pricing, anonymity, and exchangeability for other commodities. Moreover, the PMSJ industry is a cash-intensive trade, allowing bad actors to disguise their involvement.[380] PMSJ pipelines, such as the cutting and polishing of diamonds or the refinement of gold, are extensive, increasing opportunities for money laundering at different stages. Criminals may view PMSJs as a useful laundering tool allowing them to conceal illicit wealth without increased scrutiny, because the underlying commodity is legal. From a smuggling perspective, PMSJs can be transported across borders by couriers on their person, hidden in other items, or melted down into ordinary objects, making it difficult for law enforcement and customs personnel to detect the criminal activity.[381] Once the PMSJs enter the United States, criminals sell the items to refineries or trade the items through illicit shell or front companies using falsified documents.

Case Examples

- In June 2023, Eduard Ghiocel and Floarea Ghiocel pleaded guilty to laundering $1.4 million in proceeds from robberies, scams, and fraudulent employment claims.[382] Among other actions, the pair stole jewelry from elderly communities in San Diego and pawned the items in jewelry stores in San Francisco. The Ghiocels wired the cash via an MSB to Romania in addition to shipping gold bars, gold coins, and luxury vehicles bought with the stolen proceeds to Romania. These efforts were in support of an international crime ring that targeted elderly victims.
- In April 2023, nine individuals were federally charged with conspiring to defraud the United States, evade U.S. sanctions laws, and money laundering. The conspirators used a web of business entities to obtain valuable artwork from U.S. artists and to secure U.S.-based diamond grading services for the benefit of Nazem Ahmad, who the U.S. sanctioned for being a financier for Hizballah. Ahmad was involved in the international trade of diamonds, real estate development, and the global art market. The defendants used U.S.-based Diamond Grading Company-1 to affect the sale prices of diamonds,

377 FinCEN, FAQs: Interim Final Rule - Anti-Money Laundering Programs for Dealers in Precious Metals, Stones, or Jewels, (May 3, 2005), https://www.fincen.gov/resources/statutes-regulations/guidance/frequently-asked-questions-0.

378 Federal Register, Financial Crimes Enforcement Network; Anti-Money Laundering Programs for Dealers in Precious Metals, Stones, or Jewels, (June 9, 2005), https://www.federalregister.gov/documents/2005/06/09/05-11431/financial-crimes-enforcement-network-anti-money-laundering-programs-for-dealers-in-precious-metals.

379 FATF, Money laundering and terrorist financing through trade in diamonds, (October 2013), https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/ML-TF-through-trade-in-diamonds.pdf.coredownload.pdf.https://www.fatf-gafi.org/en/publications/Methodsandtrends/Ml-tf-through-trade-in-diamonds.html.

380 UN CTED, "Concerns over the Use of Proceeds from the Exploitation, Trade, and Trafficking of Natural Resources for the Purposes of Terrorism Financing", (June 2022), https://www.un.org/securitycouncil/ctc/sites/www.un.org.securitycouncil.ctc/files/files/documents/2022/Jun/cted_cft_trends_alert_june_2022.pdf.

381 CBP, Black Gold Seized by CBP Officers in Florida," (October 8, 2021), https://www.cbp.gov/newsroom/local-media-release/black-gold-seized-cbp-officers-florida.

382 DOJ, Romanian Citizens Plead Guilty to Laundering $1.4 Million in Proceeds from Jewelry Thefts and Covid Fraud, (June 20, 2023), https://www.justice.gov/usao-sdca/pr/romanian-citizens-plead-guilty-laundering-14-million-proceeds-jewelry-thefts-and-covid.

increasing the profit made from the diamonds. By using a network of corporate entities and individuals to hide Ahmad's involvement, the group attempted to evade U.S. sanctions.[383]

- In May 2022, a Russian national was indicted for operating an unlicensed money transmitting business and money laundering.[384] The individual used the U.S. banking system to transmit more than $150 million. This money was used, in part, to purchase more than $65 million in overseas gold bullion. The individual purchased the gold bullion in two ways. First, he transferred money from his business bank accounts to the Singapore Precious Metals Exchange. Second, money was transferred to the Scottsdale Mint in Arizona then to the Singapore Precious Metals Exchange.[385] These transactions are linked to the assets of "Russian oligarchs with potential ties to the Russian government," indicating the accused individual acted as a potential facilitator for sanctions evasion related to the Russian invasion of Ukraine.

3. Update on Art

As demonstrated in the Treasury's detailed study conducted in 2022,[386] the art market is susceptible to abuse. During the reporting period there was little change in its risk profile. The high-dollar values of single transactions, the ease of transportability of works of art (including across borders), the long-standing culture of privacy in the market, and the increasing use of art as an investment or financial asset all contribute to making high-value art vulnerable to money laundering. Further, LEAs can face challenges investigating money laundering through art due to the subjectivity of the pricing of artworks, the cross-border nature of the market, and having less art market expertise across competent authorities.

Case Examples

- In April 2023, nine individuals were indicted for conspiring to defraud the United States and foreign governments, evade U.S. sanctions and customs laws, and launder money by securing goods and services for the benefit of one of the defendants, a sanctioned individual. According to court documents, the co-conspirators relied on a complex web of entities and individuals to obtain valuable artwork from U.S. artists and art galleries while hiding the involvement of the sanctioned individual. The network's acquisition and sale of high-value artwork served as tools for sanctions evasion and "layering," or disconnecting proceeds from the activities that generated them.[387]

383 DOJ, OFAC-Designated Hizballah Financier and Eight Associates Charged with Multiple Crimes Arising Out of Scheme to Evade Terrorism-Related Sanctions," (April 18, 2023), https://www.justice.gov/usao-edny/pr/ofac-designated-hizballah-financier-and-eight-associates-charged-multiple-crimes.

384 DOJ, Russian Charged with Money Laundering and Illegally Transmitting More than $150 Million," (May 1, 2023), https://www.justice.gov/usao-ndga/pr/russian-charged-money-laundering-and-illegally-transmitting-more-150-million.

385 U.S. District Court for the Northern District of Georgia, United States v. Feliks Medvedev, Criminal Indictment," Case 1:22-cr-00184-TWT-CMS, (May 17, 2022), https://storage.courtlistener.com/recap/gov.uscourts.gand.303502/gov.uscourts.gand.303502.1.0.pdf.

386 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.

387 Treasury, *Treasury Disrupts International Money Laundering and Sanctions Evasion Network Supporting Hizballah Financier, (*April 18, 2023), https://home.treasury.gov/news/press-releases/jy1422.

4. Automobiles

The purchase of high-end vehicles with proceeds of crime, particularly drug proceeds, has been a long-standing money laundering typology. The use of car dealerships, vehicle auctions and international car shipping companies has also been used to launder and transmit the proceeds of romance scams, pandemic unemployment fraud, and other fraudulent schemes.[388]

Case examples

- In November 2022, Daniel Fruits was sentenced to six years in federal prison after pleading guilty to wire fraud and money laundering. According to court documents, Fruits, who was hired to manage and run a Greenwood, Indiana-based trucking company, defrauded his employer out of more than $14 million over a 4.5-year period. From January 2015 through June 2019, a Kentucky-based legal entity invested over $14 million into the trucking company. Fruits used those embezzled funds to purchase real estate; several vehicles, including two Ferraris and a Corvette; farm equipment including a horse trailer; a show horse; expensive jewelry, including multiple Rolex watches; firearms; private jet flights; and high-end escort services.[389]
- In May 2022, Stephen Mudd, Jr. was convicted and sentenced for conspiring to commit money laundering by assisting in the unlawful purchase of automobiles with criminal proceeds and was sentenced for a financial crime involving the use of a nominee to purchase automobiles to conceal the source of the funds used. While working as a car salesman, Mudd helped falsify employment and bank account information to facilitate the purchase of automobiles with criminal proceeds—with either the proceeds providing a cash down payment or the means of monthly payments on an automobile loan from a financial institution. Mudd knew that lenders would not extend financing without proof of a legitimate source of income.[390]
- In March 2022, James Pinson, the owner of a used car dealership, was convicted of three counts of wire fraud, six counts of mail fraud, one count of aggravated identity theft, and two counts of conspiring to commit money laundering. Evidence at trial revealed that to carry out his scheme, Pinson bought pick-up trucks at wholesale prices at auction, obtained hundreds of copies of Kentucky and West Virginia residents' driver's licenses, fraudulently titled the trucks in the name of those residents, and fraudulently induced the auto manufacturer to repurchase the trucks at 150 percent of their retail value. The auto manufacturer issued 350 checks in the names of individual false owners between 2013 and 2015. Pinson forged signatures on all 350 checks and deposited them into his bank account.[391]

---

388 Any person in a trade or business who receives more than $10,000 in cash in a single transaction or in related transactions must file a Form 8300. By law, in this context, a "person" is an individual, company, corporation, partnership, association, trust or estate. See IRS Form 8300 and Reporting Cash Payments of Over $10,000, https://www.irs.gov/businesses/small-businesses-self-employed/form-8300-and-reporting-cash-payments-of-over-10000.

389 IRS, Greenwood man sentenced to six years in federal prison for embezzling $14 million from his former employer to fund his lavish lifestyle available at IRS-CI, (November 29, 2022), https://www.irs.gov/compliance/criminal-investigation/greenwood-man-sentenced-to-six-years-in-federal-prison-for-embezzling-14-million-from-his-former-employer-to-fund-his-lavish-lifestyle.

390 IRS, Four men convicted of federal financial crimes involving money laundering, structuring, wire fraud, and bank fraud, (June21, 2022), https://www.justice.gov/usao-wdky/pr/four-men-convicted-federal-financial-crimes-involving-money-laundering-structuring-wire.

391 DOJ. Two Men Sentenced to Prison for Roles in $4.3 Million Fraud and Money Laundering Scheme, (March 3, 2022), https://www.justice.gov/usao-sdwv/pr/two-men-sentenced-prison-roles-43-million-fraud-and-money-laundering-scheme#:~:text=Money percent20Laundering percent20Scheme-,Two percent20Men percent20Sentenced percent20to percent20Prison percent20for percent20Roles percent20in,Fraud percent20and percent20Money percent20Laundering percent20Scheme&text=CHARLESTON percent2C percent20W.Va.,a percent20Toyota percent20Customer percent20Support percent20Program.

Casinos and Gaming

The recent growth of gaming activity at brick-and-mortar casinos and online gaming platforms has raised the risk profile for U.S. casinos and gaming activity in the United States. Casinos and card clubs are considered financial institutions subject to BSA requirements if they are licensed to do business as a casino or card club (by the relevant state, tribal, or territorial authority) and have gross annual gaming revenues in excess of $1,000,000.[392] The gaming industry has expanded considerably in recent years with increases in commercial revenue and an influx of new market participants, such as online gaming platforms (*see Special Focus Section on Online Gaming below*).

The sophistication and resourcing of regulatory and supervisory regimes for casinos and card clubs vary considerably across federal, state, tribal, and territorial levels. This variation may create opportunities for jurisdictional arbitrage in the casino sector. The risk profiles of casinos and card clubs also vary considerably, owing to their differences in size, volume of cash flow, location, customers and clientele, and range of games and services offered, among other factors. There are also continuing challenges with AML/CFT supervision of some gaming operators - including online platforms, firms offering "games of skill" (as opposed to "games of chance"), and third-party operators that may engage in casino-like activities but that are not necessarily subject to BSA obligations because they are not licensed as casinos.

The casino and gaming industry has expanded considerably in recent years with increases in commercial revenue and an influx of new market participants, such as online gaming platforms. There are roughly 1,500 casinos and card clubs in the United States and commercial revenue from casino gaming and sports betting reached a record $60 billion in 2022.[393] Casino and gaming activity is increasingly dispersed across the United States as a growing number of state, tribal, and territorial jurisdictions legalize and operationalize gaming activity, including online and sports betting. The jurisdictions with the largest commercial casino markets by revenue are Las Vegas (Nevada) and Atlantic City (New Jersey).[394] Casinos and card clubs in these regions are also among the most highly regulated and file among the most SARs in the country.[395]

Those BSA requirements include AML program obligations, including written procedures, internal controls, training of personnel, a designated compliance officer, and independent testing, among other requirements.[396] Both casinos and card clubs are also subject to obligations relating to general and gaming-specific SAR and CTR filing as well as recordkeeping, and, other requirements.[397] In addition to federal AML/CFT reporting obligations under the BSA, some states, such as Nevada, require additional state-level reporting by casinos and gaming operators. FinCEN supervises casinos and card clubs and delegated examination authority belongs to the IRS SB/SE.

392 IRS-CI, ITG FAQ #1 Answer-When are casinos considered to be financial institutions subject to requirements of the Bank Secrecy Act (Title 31)?, https://www.irs.gov/government-entities/indian-tribal-governments/itg-faq-1-answer-when-are-casinos-considered-to-be-financial-institutions-subject-to-requirements-of-the-bank-secrecy-act-title-31.

393 American Gaming Association, "State of The States 2023", (May 2023), https://www.americangaming.org/wp-content/uploads/2023/05/AGA-State-of-the-States-2023.pdf.

394 American Gaming Association, "State of The States 2023", (May 2023), https://www.americangaming.org/wp-content/uploads/2023/05/AGA-State-of-the-States-2023.pdf.

395 FinCEN, SAR Filings by Industry, (July 2023), https://www.fincen.gov/sites/default/files/shared/Section percent201 percent20-percent20Casino percent20and percent20Card percent20Club percent20SARs.xlsx

396 See 31 CFR Part 1021, Subpart B, https://www.ecfr.gov/current/title-31/subtitle-B/chapter-X/part-1021.

397 See 31 CFR Part 1021, Subparts C and D, https://www.ecfr.gov/current/title-31/subtitle-B/chapter-X/part-1021.

The risks in this sector involve not only compliance issues by casinos and card clubs regarding their respective AML/CFT obligations under the BSA, but also the misuse of casinos by foreign illicit actors (especially CMLOs and Junket Operators) and uneven supervision. CMLO threat actors have used "mirror trades" (See CMLO section) as a feature of casino junkets.[398] Casino junkets attract high-net-worth individuals, such as those who want to move money out of mainland China and enable large transfers of funds between different jurisdictions. We discuss the risks associated with online gaming activities, including sports betting and offshore gaming platforms in the subsequent special focus section on those issues.

Law enforcement reporting and criminal prosecutions suggest continuing money laundering risks associated with placing illicit proceeds in casinos. These are often earned from illegal gambling, fraud, CMLO-related activity, and the proceeds of drug, arms, and human trafficking. Recent SAR filing data suggests this activity may involve chip walking, structuring, and the large deposit or withdrawal of funds with minimal gaming activity. For example, in 2022 casinos and card clubs filed a record number of SARs relating to chip walking and a six-year record of SARs relating to structuring and minimal gaming with large transactions.[399] Other methodologies may include the use of money-mule networks, the misuse of line-of-credit services to avoid CTR filings, the misuse of private gaming salons, and chip-walking in dominations lower than what casinos generally track (*i.e.,* using chips valued at less than $5,000).

According to federal and state law enforcement sources, some foreign illicit actors engage in intra-property transfers, wherein they deposit funds at a foreign branch of a U.S.-based casino property and then access an equivalent amount of funds at a U.S. branch of that same casino property - either in cash, chips, or through a line-of-credit vehicle. Using this arrangement, actors may ultimately withdraw the funds (plus any additional gambling winnings) at either the United States or the foreign branch of the casino, potentially bypassing both foreign currency controls and BSA reporting obligations.

There are continuing concerns regarding covered casinos' and card clubs' compliance with relevant AML/CFT obligations. Federal and state law enforcement underscored the extent to which covered casinos and card clubs may be fulfilling their required obligations, including SAR and CTR filing, but not taking other forms of proactive risk-based action against suspected money laundering. This approach may be indicative of casinos and card clubs seeking to attract, retain, and accommodate wealthy patrons, which may include illicit actors, despite money laundering concerns or their inability to determine sources of funds. Nonetheless, such practices can facilitate money laundering and other illicit activities occurring through licensed U.S. casinos. The sophistication and resourcing of regulatory and supervisory regimes for casinos varies considerably across federal, state, tribal, and territorial levels. This variation may create opportunities for jurisdictional arbitrage in the casino sector.

Case Examples

- In October 2022, six individuals were indicted for drug, gun, and money laundering crimes by a federal grand jury. According to the indictment, the drug conspiracy occurred between August 2020 and June 2022 and involved more than 400 grams of fentanyl and 500 grams of methamphetamine. The charged money laundering offenses included the transportation of large amounts of cash, the purchase of casino chips and placement of sportsbook bets, buying expensive jewelry, and leasing

398 See FinCEN, Frequently Asked Questions on Casino Recordkeeping, Reporting, and Compliance Program Requirements, https://www.fincen.gov/resources/statutes-regulations/guidance/frequently-asked-questions-casino-recordkeeping-reporting.

399 FinCEN, SAR Filings by Industry, (July 2023), https://www.fincen.gov/sites/default/files/shared/Section percent201 percent20-percent20Casino percent20and percent20Card percent20Club percent20SARs.xlsx.

a luxury apartment and vehicle, all using the proceeds of drug trafficking. The indictment alleges, among other transactions, that $51,000 in cash was seized from a checked bag belonging to one individual; that two other individuals purchased casino chips and placed sportsbook bets totaling over $540,000 and later cashed out more than $445,000; and that members of the group spent tens of thousands of dollars on Rolex and Audemars Piguet watches and a diamond and gold chain.[400]

- In July 2022, Demetrius Burt Catching was sentenced to 93 months in federal prison after pleading guilty to the distribution of marijuana and money laundering. According to the plea agreement, Catching admitted to distributing marijuana in the Lexington area and then taking the proceeds from the marijuana sales and placing large sports bets and wagers at various Indiana casinos. According to the plea, after Catching was banned from one of the casinos, he recruited others to go in his place to make his wagers and bets. Cash from the wagers was deposited in bank accounts in his name. Catching was also ordered to forfeit approximately $215,000 in proceeds from his drug trafficking and money laundering offenses, and ordered to serve an additional, consecutive term of 55 months for supervised release violations on previous convictions.[401]
- In May 2022, the California Gambling Control Commission issued a stipulated settlement decision and order for Lucky Chances Casino, located in Colma, California. As part of the settlement decision, the commission required the Casino to perform the following actions, among others: (1) fully comply with the BSA and its implementing regulations, (2) report to the Bureau of Gambling Control any examination by FinCEN and IRS any examination regarding the Casino's compliance with the implementation of the BSA (3) implement and maintain an effective AML program; (4) employ a compliance officer to ensure compliance with the BSA; (5) and hire a qualified independent consultant to review the effectiveness of the Casino's AML program.[402]

1. Special Focus: Online Gaming

In recent years, legal and technological developments have led to substantial growth in online gaming activity in the United States. While online gaming can take a number of forms, of particular illicit finance concern are the emergent money laundering risks associated with sports betting, offshore sports betting, and virtual asset gambling. These activities bear many of the same risks associated with traditional gaming at brick-and-mortar casinos. However, there are unique risks stemming from the size and rapid growth of these sectors, uneven or inadequate regulation, and anonymity afforded by online gaming.

a) Sports Betting

Since the U.S. Supreme Court overturned a broad prohibition on regulated sports betting in 2018, U.S.-based persons have collectively wagered more than $220 billion in legal sports bets as of 2023, nearly half of which occurred between 2022 and 2023.[403] Legal sports betting in the United States occurs across numerous settings, including at in-person sportsbooks (which can be co-located on casino premises)

400 IRS-CI, October 27, 2022, Six Detroiters charged with drug, gun, and money laundering crimes, https://www.irs.gov/compliance/criminal-investigation/six-detroiters-charged-with-drug-gun-and-money-laundering-crimes.

401 IRS-CI, July 25, 2022, Jessamine County man sentenced to 93 months for distribution of marijuana and money laundering, https://www.irs.gov/compliance/criminal-investigation/jessamine-county-man-sentenced-to-93-months-for-distribution-of-marijuana-and-money-laundering.

402 CGCB, "Stipulated Settlement, Decision and Order in the Matter of Lucky Chances Inc.," Case No.: CGCC 2022-0210-14, (May 31, 2022), http://www.cgcc.ca.gov/documents/adminactions/decision/Lucky_Chances_Stipulated_Settlement_App-32323.pdf.

403 American Gaming Association, Assessing Shifts in the Sports Betting Market 5 Years Post-PASPA, (May 9, 2023), https://www.americangaming.org/wp-content/uploads/2023/05/AGA_PASPA_LSBResearch.pdf.

and at sporting events, such as stadiums and racetracks. However, most sports betting activity in the United States occurs via online or mobile gaming platforms. These platforms generally operate either (1) as third-party operators through licensing arrangements with BSA-covered casinos that are licensed at the state, tribal, or territorial level; or (2) by acquiring online gaming operator licenses or permits directly from relevant authorities without an affiliation with a brick-and-mortar, BSA-covered casino.

Both models create AML/CFT compliance challenges and opportunities to launder illicit proceeds. For example, online gaming platforms may not have robust AML/CFT controls; they may not be affiliated with a BSA-covered casino or entity; they may be unaware of any BSA obligations to which they may be subject as an extension of any licensing arrangement with a casino; and a BSA-covered casino could have limited visibility into potential criminal activity occurring on its third-party operator's services. In some instances, casinos and gaming operators that do not meet the BSA's definition of a casino (often due to a licensing requirement) may be operating as money transmitters.[404] These factors, in addition to the volume of the betting activity, the rapid growth of the sector, and the lack of uniform requirements or regulations of these services across state, territorial, and tribal jurisdictions, present significant and increasing money laundering risks.

There are numerous types of money laundering methodologies and schemes associated with sports betting, many of which resemble traditional casino-based criminal schemes. For example, users may deposit the proceeds of crime into betting accounts and subsequently withdraw funds after minimal betting activity, disguising the illicit funds as betting earnings. These schemes also demonstrate how criminal actors abuse U.S. financial institutions. Confederates can also collude on one or a series of bets, working together to hide the illicit origin of the source of funds.

In August 2023, a Georgia man was charged with money laundering and other crimes for a scheme to misdirect more than $30 million from faith-based charities and individual donors, originally intended for religious causes, for personal gain.[405] In his misuse of the funds, the man deposited approximately $1 million of the misdirected funds into an online sports gambling website. In 2021, New Jersey state authorities arrested a man for a fraudulent scheme involving his alleged use of stolen identities to create and fund more than 1,800 online gambling accounts through Atlantic City's online gaming providers.[406] As part of the scheme, he also allegedly created fraudulent bank accounts using the victims' stolen identities. He transferred funds from fraudulent unemployment benefits claims to those accounts, later making cash withdrawals.[407]

404 See 31 CFR 1010.100(t)(5)(i) and 31 CFR 1010.100(ff)(5)(i)(A).

405 DOJ, Fugitive charged in scheme that misdirected millions in charitable donations intended for Christian outreach in China, (August 1, 2023), https://www.justice.gov/usao-sdga/pr/fugitive-charged-scheme-misdirected-millions-charitable-donations-intended-christian.

406 State of New Jersey, State Police Arrest Man Who Stole Identities to Fund Online Gambling Accounts, (June 8, 2021), https://www.nj.gov/njsp/news/2021/20210608.shtml.

407 State of New Jersey, State Police Arrest Man Who Stole Identities to Fund Online Gambling Accounts, (June 8, 2021), https://www.nj.gov/njsp/news/2021/20210608.shtml.

b) Offshore Online Gaming

There is also a significant amount of online gaming activity occurring through offshore operators. Industry reporting suggests that Americans wager an estimated $64 billion annually on illegal or offshore gaming platforms, accounting for roughly 40 percent of the U.S. sports betting market.[408] Many illegal sports betting platforms are based in foreign jurisdictions with deficient regulatory frameworks yet actively advertise to U.S. consumers and markets.

There is evidence that U.S. persons have used offshore gaming platforms to engage in illicit activity. For example, in January 2023, eleven defendants were charged in a multi-million-dollar scheme relating to the operation of an illegal sports betting organization.[409] The scheme, which included the evasion of excise tax totaling nearly $20 million between 2019 and 2021, involved betting activities occurring online via an offshore server located in Costa Rica.

Some offshore gaming platforms use virtual assets as forms of payment, presenting additional risk factors. Large, transnational virtual asset gambling firms have grown rapidly since 2020, driven by increases in the adoption of virtual assets as well as the anonymity provided by the technology.[410] In 2019 guidance, FinCEN clarified that gaming operators and internet casinos that are not covered by the regulatory definition of casino, gambling casino, or card club but that accept and transmit virtual assets may still be regulated under the BSA as a money transmitter.[411]

Many large virtual asset gambling services screen for users' locations and deny access to users located in the United States in accordance with U.S. law. However, virtual private networks can allow U.S.-based users to, with relative ease, fraudulently circumvent these location-screening protocols by obfuscating or misreporting their locations. This obfuscation may also inhibit the ability of virtual asset gambling firms to conduct due diligence into U.S.-based users and understand sources of funds.

Entities Not Fully Covered by AML/CFT Requirements

1. Investment Advisers

The investment adviser (IA) industry in the United States consists of a wide range of business models that provide a variety of financial services to retail investors, high-net-worth individuals, private institutions, and governmental entities (including but not limited to local, state, and foreign government funds). The assets managed by different types of IAs—including IAs registered with the SEC (referred to as Registered Investment Advisers, or "RIAs"), IAs exempt from SEC registration (also known as Exempt Reporting

408 American Gaming Association, Sizing the Illegal and Unregulated Gaming Markets in the U.S., (November 30, 2022), https://www.americangaming.org/resources/sizing-the-illegal-and-unregulated-gaming-markets-in-the-u-s/#:~:text=AGA percent27s percent20report percent2C percent20Sizing percent20the percent20Illegal,billion percent20in percent20lost percent20tax percent20revenue.

409 DOJ, Eleven Indicted in Multi-Million Dollar Excise Tax Evasion and Money Laundering Scheme Involving Illegal Sports-Betting Organization, (January 6, 2023), https://www.justice.gov/usao-ndal/pr/eleven-indicted-multi-million-dollar-excise-tax-evasion-and-money-laundering-scheme.

410 DOJ, Report of the Attorney General's Cyber Digital Task Force: Cryptocurrency Enforcement Framework, see p. 39,. (October 2020), https://www.justice.gov/archives/ag/page/file/1326061/download.

411 See FinCEN, "Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies," (May 9, 2019), https://www.fincen.gov/sites/default/files/2019-05/FinCEN percent20Guidance percent20CVC percent20FINAL percent20508.pdf.

Advisers, or "ERAs"), and state-registered IAs (who are prohibited from registering with the SEC)—vastly exceed the holdings of U.S. banks.

As of July 31, 2023, there were approximately 15,000 RIAs reporting approximately $125 trillion in assets under management (AUM) for their clients.[412] There are also approximately 5,800 ERAs that report certain information to the SEC but are not required to register. According to the SEC, ERAs manage approximately $5 trillion in assets.[413] Finally, there are approximately 17,000 investment advisers who are required to register with state securities regulators. As of December 31, 2022, these state-registered investment advisers managed approximately $420 billion in assets.[414]

Oversight of the investment adviser industry by federal and state securities regulators is generally focused on protecting investors and the overall securities market from fraud and manipulation. However, the IA sector is not uniformly subject to comprehensive AML/CFT regulations and is not typically examined for AML/CFT compliance. Some RIAs may implement an AML/CFT program as the entity may also be a registered broker-dealer (*i.e.,* a dual registrant) or bank; other RIAs that are subsidiaries of a financial holding company may implement an enterprise-wide AML/CFT program. Additionally, some IAs may perform certain AML/CFT measures through contractual obligations for a joint customer of a regulated financial institution or as a voluntary best practice.[415] But these arrangements are not uniform across the IA industry, and the IAs' implementation of these measures is not subject to comprehensive enforcement and examination.

A review of law enforcement cases and BSA reporting identified several illicit finance threats involving IAs. First, IAs have served as an entry point into the U.S. market for illicit proceeds associated with foreign corruption, fraud, and tax evasion. Second, certain investment advisers (or entities required to register as investment advisers) have managed billions of dollars ultimately controlled by designated Russian oligarchs and their associates. Separately, numerous fraud cases involving smaller IAs (both SEC and state-registered) where they defrauded their clients and stole their funds.[416]

IAs may be vulnerable to these threats, at least in part, for several reasons. First, the lack of comprehensive AML/CFT regulation for the IA sector may create arbitrage opportunities for illicit actors by allowing them to more easily find IAs with weaker or non-existent client due diligence practices as they seek to access the U.S. financial system. Second, IAs' business activities may be segmented across intermediaries (and potentially national borders), possibly creating information asymmetries. Obligated entities (such as custodian banks or broker-dealers) working with an IA may not necessarily have a direct

412 The number of RIAs and AUM, and the number of ERAs are based on a Treasury review of Form ADV information filed as of July 31, 2023. This Form ADV data is available at Frequently Requested FOIA Document: *Information About Registered Investment Advisers and Exempt Reporting Advisers*, http://www.sec.gov/foia/docs/invafoia.htm. The $125 trillion in AUM includes approximately $22 trillion in assets managed by mutual funds, which are advised by RIAs and are subject to AML/CFT obligations under the BSA and its implementing regulations.

413 88 Fed. Reg. 63206, 63304 (Sept. 14, 2023).

414 North American Security Administrators Association, *NASAA Investment Adviser Section 2023 Annual Report*, p.3, https://www.nasaa.org/wp-content/uploads/2023/09/2023-IA-Section-Report-FINAL.pdf.

415 See, for example, SEC, Letter to Mr. Bernard V. Canepa, Associate General Counsel, Securities Industry and Financial Markets Association, Request for No-Action Relief Under Broker-Dealer Customer Identification Program Rule (31 CFR 1023.220) and Beneficial Ownership Requirements for Legal Entity Customers (31 CFR 1010.230) (Dec. 9, 2022), https://www.sec.gov/divisions/marketreg/mr-noaction/2020/sifma-120920-17a8.pdf.

416 In most of the identified cases, authorities pursued civil or criminal enforcement for violations of the federal securities laws against the investment adviser or other associated individuals.

relationship with the client (or, in the case of private funds, the ultimate investor). They may be unable to require an IA to disclose relevant information. At the same time, entities that can obtain information about ultimate clients and investors (typically the IA and certain service providers for the advised fund) are not required to do so, nor are they required to report potentially suspicious activity. Third, certain business practices often promote the secrecy of client/ or investor identity and information and the outsourcing of key compliance responsibilities.

The entities in the investment adviser sector that pose the highest risks are ERAs, RIAs who are not dually registered as, or affiliated with, a bank or broker dealer, and IAs who manage private funds.

Private funds advised by investment advisers, such as hedge and private equity funds and, venture capital funds, hold over $20 trillion in assets, and have limited reporting obligations. Advisers managing these funds may also routinely invest assets from foreign legal entities that are generally not required to disclose their ultimate beneficial owners. As of Q4 2022, private funds managed by RIAs represented $284 billion in equity beneficially owned by non-U.S. investors where the RIA did not know, and could not reasonably obtain information about, the non-U.S. beneficial ownership because the beneficial interest was held through a chain involving one or more third-party intermediaries.[417]

Case examples

- In December 2021, a founder of a New York financial advisory and investment company was charged with wire fraud, IA fraud, and money laundering in connection with a scheme to misappropriate more than $1 million from current and prospective clients. As alleged in the indictment, the former investment adviser executed a calculated scheme in which he repeatedly lied to his current and prospective clients about putting their money into legitimate investments, when, in reality, he stole their money to fund his lavish lifestyle. As noted in the indictment, the victims sent multiple wire transfers to the private bank account of the IA's investment firm. The IA then misappropriated the funds into his personal banking account, among other things.[418]
- In November 2019, Mark Scott, a former equity partner at the law firm Locke Lord LLP, was convicted of one count of conspiracy to commit money laundering and one count of conspiracy to commit bank fraud. Beginning in 2016, Scott established fake private equity investment funds in the British Virgin Islands, known as the "Fenero Funds" to launder approximately $400 million in proceeds from a large international pyramid fraud scheme called OneCoin. Scott claimed that the investments were from "wealthy European families," when in fact the money represented proceeds of the OneCoin fraud scheme. Scott layered the money through Fenero Fund bank accounts in the Cayman Islands and the Republic of Ireland. As part of the scheme, Scott and his co-conspirators lied to banks, including U.S. banks and other financial institutions, to cause those institutions to make transfers of OneCoin proceeds and evade AML procedures.[419]

417 SEC, "Private Fund Statistics, Fourth Calendar Quarter 2022", (July 18, 2023), https://www.sec.gov/files/investment/private-funds-statistics-2022-q4.pdf.

418 DOJ, "Founder of Investment Advisory Firm Charged with Wire Fraud, Investment Adviser Fraud and Money Laundering", (December 6, 2021), https://www.justice.gov/usao-edny/pr/founder-investment-advisory-firm-charged-wire-fraud-investment-adviser-fraud-and-money; *United States v. Slothower* (Indictment) Case 2:21-cr-00602 (E.D.N.Y), December 1, 2021.

419 DOJ, "Former Partner Of Locke Lord LLP Convicted In Manhattan Federal Court Of Conspiracy To Commit Money Laundering And Bank Fraud In Connection With Scheme To Launder $400 Million Of OneCoin Fraud Proceeds," (Nov. 21, 2019), https://www.justice.gov/usao-sdny/pr/former-partner-locke-lord-llp-convicted-manhattan-federal-court-conspiracy-commit-money.

2. Third-Party Payment Processors

Third-party payment processors (TPPPs or payment processors) are services that enable merchants and other business entities to accept card and other non-cash payments from consumers without having to maintain their own merchant account with a financial institution. TPPPs simplify payment processing for merchants by using their own commercial bank accounts to process merchants' payments, often aggregating all of their clients' transactions into a single merchant account or, in some cases, opening an account at a financial institution in the merchant's name. Merchant transactions primarily include credit card payments but can also include Automated Clearing House (ACH) transactions, remotely created checks (RCC), digital wallet payments, and debit and prepaid card transactions. Payment processors traditionally contracted primarily with retailers with physical locations; however, retail borders have been eliminated with the expansion of the Internet and e-commerce.[420]

As described in the 2022 NMLRA, TPPPs generally are not subject to AML/CFT regulatory requirements, and the scope of BSA coverage depends on the company's unique circumstances. However, only those payment processors that meet very specific conditions outlined in FinCEN guidance are exempt from BSA obligations.[421] These conditions are as follows: (1) the company must facilitate the purchase of goods or services, or the payment of bills for goods or services (other than money transmission itself); (2) it must operate through clearance and settlement systems that admit only BSA-regulated financial institutions (*e.g.,* the Automated Clearing House); (3) it must provide the service pursuant to a formal agreement; and (4) the entity's agreement must be at a minimum with the seller or creditor that provided the goods or services and receives the funds from the entity.

The FDIC, OCC, and FinCEN each issued guidance in the early 2010s regarding the risks, including the AML/CFT risks, associated with banking third-party processors. In 2023, the FDIC, OCC, and the FRB issued joint guidance for banking organizations regarding managing third-party relationships, as such relationships can reduce a bank's direct control over activities and may introduce new risks.[422] Banks may face heightened ML/TF risks when dealing with a processor account, similar to risks from other activities in which the bank's customer conducts transactions through the bank on behalf of the customer's clients. Some higher-risk merchants routinely use payment processors to process their transactions because they do not have a direct bank relationship. Criminals can use payment processors to mask illegal or suspicious transactions and launder proceeds of crime, especially if the processor does not have an effective means of verifying their merchant clients' identities and business practices. In addition, payment processors have been used to place illegal funds directly into a financial institution using ACH credit transactions originating from foreign sources.[423]

420 Federal Financial Institutions Examination Council (FFIEC) Manual, "Risks Associated with Money Laundering and Terrorist Financing, Third-Party Payment Processors—Overview," https://bsaaml.ffiec.gov/manual/RisksAssociatedWithMoneyLaunderingAndTerroristFinancing/10.

421 FinCEN, "Application of Money Services Business Regulations to a Company Acting as an Independent Sales Organization and Payment Processor," (FIN-2014-R009), (August 24, 2014), https://www.fincen.gov/sites/default/files/administrative_ruling/FIN-2014-R009.pdf.

422 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.

423 FinCEN Advisory, "Risk Associated with Third-Party Payment Processors," FIN-2012-A010, (October 22, 2012), https://www.fincen.gov/sites/default/files/advisory/FIN-2012-A010.pdf.

A review of cases, including criminal cases and civil enforcement actions, over the last three years involving TPPPs revealed several patterns of fraudulent behavior. The most common typology, present in eight of the cases, involved complicit TPPPs. As a primary gateway to the legitimate financial system, payment processors are in a unique position to facilitate high volumes of fraud by working together with fraudulent merchants or failing to address suspicious activity. In some cases, payment processors ignored red flags indicating fraudulent activity by merchants, such as a high rate of chargebacks, which can indicate unlawful debiting; in other cases, payment processors actively worked to disguise merchant activity, misrepresenting the types of transactions merchants were processing to banks or even creating shell companies or designing fake websites.

In six of the cases, the payment processors were taken advantage of by merchants and used to process transactions. These cases often involve merchants misrepresenting the nature of their transactions to payment processors. In other instances, the defendant made micro-debits from victims' accounts, which often went unnoticed and lowered the merchant's chargeback rate. Finally, four cases involved TPPPs that were themselves defrauding either merchants or consumers.

These and other recent cases indicate that the use of TPPPs for money laundering and fraud is on the rise. This vulnerability seems to be largely driven by TPPPs themselves, which can take advantage of the exemption from BSA requirements and the access they have to the financial system to facilitate money laundering.

Case Examples

- In May 2023, Stephen Short was sentenced in federal court to 78 months in prison for conspiracy to commit wire and bank fraud in connection to a scheme to obtain credit card processing services for his telemarketing operation through a third-party credit card processing network. Between 2012 and 2015, Short targeted customers with outstanding credit card debt to offer services, including debt consolidation and interest-rate reduction, to generate over $19 million in fraud proceeds. The scheme involved collaboration between Short's company and CardReady, with the latter keeping one-third of credit card sale transactions in exchange for access to the credit card processing network and concealment of the underlying merchant.[424]
- In July 2022, the executives of Electronic Transactions Systems Corporation were indicted for defrauding approximately 7,000 merchant clients out of millions of dollars. Between 2012 and 2019, the defendants intentionally disguised a portion of processing fees for clients, embedding hidden markups and failing to disclose the true fee structure in billing and account statements. Specifically, the company altered the Interchange fees to include hidden markups by accessing software on computer systems belonging to a third-party company.[425] This action facilitated the over-valuing of the company during its acquisition in 2018.[426]

424 DOJ, "Head Of Telemarketing Operation Sentenced To 78 Months In Prison For $19 Million Credit Card Laundering Scheme," (May 2, 2023), https://www.justice.gov/usao-sdny/pr/head-telemarketing-operation-sentenced-78-months-prison-19-million-credit-card#:~:text=U.S.%20Attorney%20Damian%20Williams%20said,more%20than%2019%2C000%20victims%20nationwide.

425 DOJ, "Executives of Card Payment Processing Company Indicted in East Texas for Nationwide Multimillion Dollar Fraud Scheme," (July 27, 2022), https://www.justice.gov/usao-edtx/pr/executives-card-payment-processing-company-indicted-east-texas-nationwide-multimillion.

426 Id.

3. Attorneys

There are over 1.3 million attorneys in the United States whose practices encompass a broad range of client services.[427] Certain legal practice areas or services such as representing clients in disputes and mediations, providing advice concerning childhood custody proceedings, and providing regulatory advisory services, may pose lower inherent money laundering or illicit finance risk than others. On the other hand, where attorneys advise on real estate transactions, assist in the formation and administration of legal entities and trusts, and transfer and manage client assets, they may be more vulnerable because these attorneys may act as intermediaries between a client and the U.S. financial system (*i.e.,* a gatekeeper).[428] These practice areas are at higher risk because the associated services are typically essential to the specific transactions undertaken, and, because of the involvement of attorneys, the underlying transactions may acquire a veneer of respectability and integrity.

Similarly, the involvement of attorneys may effectively shield the illicit actors' identities from financial institutions processing transactions involving those clients. This issue may occur due to misapplication of attorney-client privilege, the duty of confidentiality, and the lack of AML/CFT obligations covering the legal profession. As a result, attorneys may be attractive to illicit actors intending to launder the proceeds of crime.

Common threads running through these vulnerable or high-risk practice areas include the movement of funds and the level of beneficial ownership information available to financial institutions. Two possible examples might be escrow accounts and the IOLTAs required to be maintained by lawyers and their firms, primarily for the collection and disbursement of settlement and other funds payable to their clients. These are pooled bank accounts in which attorneys deposit client funds to keep them separate from the attorneys' funds, as legal ethics require.[429] An IOLTA functions as a standard bank account, except that the bank has no direct relationship with or knowledge of the beneficial owners of the client funds in these accounts. The bank transfers the interest earned by these accounts to a state IOLTA program, which uses this money to fund charitable causes, including the delivery of legal services to indigent clients.[430]

These IOLTA and other attorney-client trust accounts, including escrow accounts, are not titled in the name of any underlying client, causing banks to find it difficult to identify suspicious transactions effectively. Without comprehensive AML/CFT regulations covering attorneys, the obligation to report suspicious transactions involving IOLTAs falls on the financial institution that serves them. Even where neither privilege nor legal ethics prohibit reporting client identities or facts of a transaction, financial

427 2022 ABA National Lawyer Population Survey, *available at* https://www.americanbar.org/content/dam/aba/administrative/market_research/2022-national-lawyer-population-survey.pdf; *see also* The American Bar Association's 2022 Profile of the Legal Profession Report, which contains state-by-state demographic details of the legal profession. Given that one quarter of all attorneys are subject to ethics rules and disciplinary procedures in two jurisdictions (New York and/or California), reform efforts focused on these states may have a disproportionate affect in bringing the U.S. legal profession in line with international standards.

428 *See supra* note [375] (Section II, covering BSA/AML compliance deficiencies and complicit professionals, explaining the definition and origin of the term "gatekeeper").

429 According to the American Bar Association (ABA), before state and Supreme Court rules created the IOLTA framework, attorneys typically placed client deposits into combined, or pooled, trust accounts that contained other nominal or short-term client funds. Trust funds pooled in this manner earned no interest because trust accounts typically are checking accounts (to allow easy access to the funds) and, until the early 1980s when the IOLTA framework was crafted, checking accounts did not earn interest. In addition, these trust funds earned no interest because it is unethical for attorneys to derive any financial benefit from funds that belong to their clients.

430 FFIEC, "Bank Secrecy Act/Anti-Money Laundering InfoBase, *Professional Service Providers – Overview*," https://bsaaml.ffiec.gov/manual/RisksAssociatedWithMoneyLaunderingAndTerroristFinancing/26.

institutions are not well placed to detect such transactions. They do not have a relationship with the attorney's client or effective means to dispute a lawyer's claim of privilege, which results in vulnerabilities in the U.S. financial system. The Treasury assesses complicit attorneys may misuse IOLTA and other lawyer trust accounts to launder criminal proceeds into and out of the United States, as reflected in its review of case examples.

The vulnerability stems from the ability of the attorney to direct transfers into and out of the account without necessarily raising red flags at the bank where the account is held. Banks may not be able to successfully identify the transaction pattern for the account since they do not have insight into the ultimate source of funds or beneficial ownership information. This can be challenge exacerbated when attorneys use one account to facilitate transactions on behalf of multiple clients, as the commingled funds make the expected activity murkier. For example, two Beverly Hills attorneys assisted the son of the President of Equatorial Guinea to circumvent AML and PEP controls at U.S. financial institutions by allowing him to use IOLTAs as conduits for over $100 million and without alerting the bank to his use of those accounts. When a bank uncovered the illicit actor's use of an account and closed it, the attorneys helped him open another account, thus allowing the IOLTAs to accept millions of dollars in wire transfers from Equatorial Guinea, moving those funds into other related accounts, and using them to pay bills and expenses. Both attorneys declined to testify before the U.S. Senate Select Committee on Intelligence hearing, citing the Fifth Amendment, and the California Bar disciplined neither of them.[431]

A resonant example that reflects the complexity of attorneys' involvement in money laundering and other illicit activity was detailed in the 2022 NMLRA. The DOJ identified a prominent global law firm in a series of civil forfeiture actions as having provided a trust account through which they illicitly siphoned hundreds of millions of dollars belonging to Malaysia's 1MDB fund.[432]

Despite these well-understood risks the United States has no uniform national regulation of attorneys. Instead, attorneys are self-regulated by state bar associations, although not for AML/CFT. Across the country, attorneys are not subject to comprehensive AML/CFT measures. Like any person in any trade or business, they are obligated to file Form 8300 for cash transactions exceeding $10,000 and may choose to use Form 8300 under certain circumstances for cash transactions of $10,000 or less. Attorneys, like any other person, may be subject to penalties for failures to file a correct and complete Form 8300, including a minimum penalty of $31,520 that may be imposed if the failure is due to an intentional or willful disregard of the cash reporting requirements.[433] The Treasury assesses IOLTA accounts and other lawyer

431 United State Senate Permanent Subcommittee on Investigation, "Keeping Foreign Corruption out of the United States: Four Case Histories," (February 04, 2010), https://www.hsgac.senate.gov/wp-content/uploads/imo/media/doc/FOREIGNCORRUPTIONREPORTFINAL710.pdf. *See also* DOJ, "Second Vice President of Equatorial Guinea Agrees to Relinquish More Than $30 Million of Assets Purchased with Corruption Proceeds," (October 10, 2014), https://www.justice.gov/opa/pr/second-vice-president-equatorial-guinea-agrees-relinquish-more-30-million-assets-purchased.

432 *See* Treasury, National Money Laundering Risk Assessment, February 2022. *See also* Complaint at 42, *U.S. v. One Drawing Entitled "Self-Portrait" by Jean-Michel Basquiat*, (C.D. Cal. 2020) (No. e 2:20-cv-05910) ("Between approximately October 21, 2009, and October 13, 2010, eleven wires totaling approximately $368 million were sent …to an Interest on Lawyer Account held by the law firm Shearman & Sterling LLP in the United States.") *See also* Press Release, U.S. Repatriates $300 Million to Malaysia in Proceeds of Funds Misappropriated from 1Malaysia Development Berhad (Apr. 14, 2020), *available at* https://www.justice.gov/opa/pr/us-repatriates-300-million-malaysia-proceeds-funds-misappropriated-1malaysia-development. One notable example is the 1MDB case where hundreds of millions of dollars were siphoned out of Malaysia's sovereign wealth fund. These funds passed through pooled accounts held at law firms in the U.S. Law firms authorized transfers that were used to pay for luxury U.S. real estate, jewelry, and yacht and jet rentals.

433 IRS Form 8300 Reference Guide, https://www.irs.gov/businesses/small-businesses-self-employed/irs-form-8300-reference-guide#penalties.

trust accounts that complicit attorneys are using to launder criminal proceeds into and out of the United States.

The American Bar Association (ABA), a voluntary, member-led organization, publishes Model Rules of Professional Conduct ("Model Rules") that have substantially influenced nearly every state jurisdiction's standards of conduct, ethics, and discipline for attorneys. Accordingly, in most states, the professional discipline of attorneys is conducted pursuant to regulations contained in codes that have been approved by the highest court in the jurisdiction in which the attorney is admitted. The ABA revised its Model Rules of Professional Conduct on August 8, 2023, in an effort to better protect the legal profession and U.S. financial system from money laundering and terrorist financing risks.[434] To date, no state bar association has adopted these amendments.

The revision to these codes by states leaves attorneys substantial discretion to determine whether to accept or continue representation under the facts and circumstances of a particular case. These state codes are permissive rather than mandatory because they generally leave final decision-making and authority over the conduct of attorneys to a state court or a specially designated grievance or discipline committee within the state. These entities generally lack the resources or authority to conduct systematic audits, examinations, or other regulatory measures for AML/CFT purposes. At the same time, unscrupulous attorneys continue to be involved in complex money laundering, sanctions evasion, and other illicit finance schemes.

Case Examples

- In March 2023, Jack Stephen Pursley, a Texas attorney pleaded guilty to conspiring with a former client to repatriate more than $18 million in untaxed income from offshore accounts held in the Isle of Man that the client had earned through his company. Pursley was aware that his client had never paid taxes on these funds. He designed and implemented a scheme whereby fund transfers from an Isle of Man bank account to the United States were disguised as stock purchases in U.S. corporations Pursley and his client owned and controlled. The attorney received more than $4.8 million and a 25 percent ownership interest in his client's business for his role in the fraudulent scheme.[435]
- In 2022, an Illinois attorney named Hassan Abbas was sentenced for his role in a scheme to defraud victims in multiple states, many of whom thought they were closing real estate transactions or sending money to romantic partners. Once the attorney received the funds, he sent large sums to fellow fraudsters overseas and took a cut, which he used to spend on luxury items and an international lifestyle. When approached by financial institutions about his account activity, the attorney disguised the purposes of wire transfers to bank investigators, claiming that certain transfers were for non-existent "clients" and, in one instance, insisting that information about the wires was protected by the attorney-client privilege.[436]

434 The changes create a duty to "inquire into and assess the facts and circumstances of each representation to determine whether the lawyer may accept or continue each representation," and to decline to represent or withdraw from representing a client who "seeks to use or persists in using the lawyer's services to commit or further a crime or fraud." *See* ABA Model Rules of Professional Conduct 1.16 (a)(4).

435 DOJ, "Houston Attorney Pleads Guilty to Offshore Tax Evasion Scheme," (March 28, 2023), https://www.justice.gov/opa/pr/houston-attorney-pleads-guilty-offshore-tax-evasion-scheme.

436 DOJ, "Illinois Lawyer Sentenced to Nine Years in Prison for Sophisticated Wire Fraud and Money Laundering Scheme," (October 28, 2022), https://www.justice.gov/usao-ma/pr/illinois-lawyer-sentenced-nine-years-prison-sophisticated-wire-fraud-and-money-laundering.

4. Accountants

The U.S. accounting sector includes approximately three million individuals who provide a wide range of services. These include (but are not limited to) Certified Public Accountants (CPAs); non-licensed public and private accountants; internal and external auditors; and bookkeeping, accounting and auditing clerks (who do not require professional licenses or four-year college degrees). Accountants in the United States are regulated through a complex framework at the federal, state, and local levels, including several private sector bodies that promulgate professional and ethical standards. State accountancy boards also supervise CPAs. The U.S. accounting sector is generally not subject to comprehensive requirements under the BSA for the purposes of AML/CFT, and oversight of the accounting industry is largely aimed at protecting the market and the public from fraud and manipulation.[437] Additionally, as U.S. persons, accountants are subject to sanctions regulations issued by OFAC concerning prohibitions on providing financial services to sanctioned persons or entities.

A review of this sector for ML/TF risks finds that licensed and unlicensed accountants face a lower to medium-low level of ML/TF risk largely because U.S. accountants generally provide financial record keeping or advice services rather than managing or holding client funds, purchasing real estate, or establishing companies. For example, even a CPA certification does not grant an accountant special access to form accounts or manage financial transactions.

While accountants are not financial service providers in the United States, there is some concern about an accountant's ability to act as financial facilitators for criminal or terrorist organizations due to their knowledge of the legal and financial system. For example, an accountant's knowledge on creating and structuring shell companies, bank accounts, wire transfers, and financial statements could be attractive to those looking to conceal financial transactions or launder money. However, an accounting background does not afford an individual any ability to register companies, open bank accounts, or authorize financial transactions beyond what an ordinary citizen can do. When accountants do commit ML offenses, their status as accountants does not allow them special access or privileges to mechanisms for hiding or transferring money. While a complicit accountant could perform these services for a criminal or terrorist organization, professional accountants or CPAs are not routinely involved in organized crime or major narcotics investigations. A criminal organization may have a "money person" that they call a "bookkeeper" or "accountant" but this may be a person with no professional training but who is entrusted by the criminal organization to coordinate payments throughout the criminal enterprise.

In the limited cases since 2016 where accountants were charged with money laundering offenses, only a few cases involved accountants using their professional capacity to launder money. Accountants have not frequently come up in large-scale money laundering or illicit finance schemes.

437 AML/CFT requirements under the BSA do not apply to the accounting sector as accountants, or accounting firms, are not defined as one of the enumerated financial institution categories; however, as with any U.S. person, they are subject to BSA requirements for filing reports when receiving $10,000 or more in currency. See https://www.irs.gov/businesses/small-businesses-self-employed/form-8300-and-reporting-cash-payments-of-over-10000. Further, participants in the U.S. accounting sector may be subject to certain cash-based reporting requirements under the BSA applicable to non-financial businesses and trades. They may also be subject to other requirements under the BSA depending on whether sector participants meet other conditions, such as whether they meet the definition of a financial institution, such as a broker-dealer, already subject to BSA requirements.

Case examples

- In August 2023, Craig Clayton, the owner of a "virtual CFO" business, agreed to plead guilty to laundering tens of millions of dollars in proceeds from internet fraud schemes by creating shell companies and opening fraudulent business bank accounts.[438] According to the charging documents, from 2019 to 2021, Clayton and others used his accounting and "virtual CFO" business, Rochart Consulting, as a front to launder the proceeds of internet fraud schemes. As part of the conspiracy, Clayton founded shell companies to open business bank accounts in Rhode Island and Massachusetts, through which he laundered the proceeds of internet fraud schemes on behalf of his clients. In total, Clayton laundered more than $35 million.
- In October 2018, San Diego-based CPA Luke Fairfield, was sentenced to 21 months in prison for his role in the criminal enterprise led by former USC football player Owen Hanson – an international drug trafficking, gambling, and MLO known as "ODOG."[439] Hanson operated ODOG in the United States, Central and South America, and Australia from 2012 to 2016, trafficking in thousands of kilograms of cocaine, heroin, methamphetamine, MDMA (also known as "ecstasy"), and other illegal drugs in wholesale and retail quantities. The ODOG enterprise also operated a vast illegal gambling network focused on high-stakes wagers placed on sporting events. To carry out its gambling operation, the ODOG enterprise employed numerous bookies and money runners, and in the event a customer did not pay his gambling debt, the ODOG enterprise employed enforcers to threaten, intimidate, and injure its customers to force compliance. As Fairfield admitted when pleading guilty in March of 2017, his role in the ODOG enterprise included laundering money, aiding in the creation of shell companies to hide ODOG's criminal proceeds, and training ODOG money runners on methods and tactics to hide the enterprise's activities from law enforcement and banks. Because of this conviction, Fairfield is no longer licensed as a CPA.

Although accountants pose a lower ML/TF risk, a review of law enforcement cases and information available to the U.S. government finds that other illicit finance risks are present, especially regarding tax offenses, embezzlement, fraud, and crimes of professional misconduct. Additionally, accountants working as auditors warrant continued regulatory attention as they are guarantors of financial data prepared by businesses, companies, trusts, and other legal entities. However, these additional risks are outside the scope of this risk assessment. The U.S. government will continue to monitor the money laundering risks posed by accountants.

438 DOJ, "Rhode Island Business Owner to Plead Guilty to Money Laundering Conspiracy and Obstruction of Justice" (August 17, 2023), https://www.justice.gov/usao-ma/pr/rhode-island-business-owner-plead-guilty-money-laundering-conspiracy-and-obstruction.

439 DOJ, "CPA Sentenced for Role in Racketeering Enterprise", (October 2, 2018), https://www.justice.gov/usao-sdca/pr/cpa-sentenced-role-racketeering-enterprise.

CONCLUSION

While many of the U.S.' most significant money laundering risks have remained consistent in recent years, a range of new factors have emerged that are reshaping the risk landscape in the United States. As this National Money Laundering Risk Assessment identifies, crimes like fraud, drug and human trafficking, cybercrime, corruption, and human smuggling remain the most significant proceeds-generating activities associated with money laundering. However, in the aftermath of the COVID-19 pandemic, and, other recent geopolitical, technological, and financial developments, the broader illicit finance ecosystem in which these crimes occur has substantially evolved. The result, therefore, is an evolved 'landscape' for money laundering risk.

A number of recent money laundering threats and vulnerabilities have become more significant and pernicious over the past two years. For example, criminals, scammers, and illicit actors are increasingly using virtual assets and digital peer-to-peer payment systems to engage in fraud and other crimes. CMLOs are no longer just emerging threats but are now dominant across the professional money laundering market. The wide availability of illicit fentanyl throughout the United States is indicative of the reach and scale of the transnational illicit supply chains supporting the production of these deadly substance.

This 2024 NMLRA aims to highlight to the public and private sectors these and other high-level threats to the U.S. financial system, both the continuing challenges as well as emerging vulnerabilities and risks that the United States faces. Only by enumerating these challenges can the United States work to prioritize and address them effectively.

As the case examples within this report demonstrate, there is robust coordination between financial oversight entities and law enforcement agencies to identify, prosecute, and ultimately dismantle money laundering activity within the United States. Indeed, it is due to the integrity, reliability, and security of the U.S. financial system that individuals and businesses both within the United States and across the world continue to use and invest their funds in the U.S. financial system—it is the most secure and trusted in the world.

The findings of the 2024 NMLRA, taken in tandem with the findings of the proliferation finance risk assessment and the terrorist financing risk assessment, will inform the forthcoming 2024 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.

PARTICIPANTS

In drafting this assessment, the Department of the Treasury's Office of Terrorist Financing and Financial Crimes consulted with staff from the following U.S. government agencies, who also reviewed this report:

- **Department of the Treasury**
  - Internal Revenue Service - Criminal Investigation (IRS-CI)
  - Internal Revenue Service - Passthroughs & Special Industries
  - 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**
  - Criminal Division
    - Computer Crime and Intellectual Property Section
    - Fraud Section
    - Money Laundering and Asset Recovery Section
    - Narcotic and Dangerous Drugs Section
    - Organized Crime and Gang Section
  - Environment and Natural Resources Division
  - Executive Office for U.S. Attorneys
  - Drug Enforcement Administration (DEA)
  - Federal Bureau of Investigation (FBI)
  - Organized Crime Drug Enforcement Task Forces (OCDETF)
- **Department of Homeland Security**
  - Customs and Border Protection (CBP)
  - Homeland Security Investigations (HSI)
  - United States Secret Service (USSS)
- **Department of the Interior**
  - U.S. Fish and Wildlife Service
- **U.S. Postal Inspection Service (Inspection Service)**
- **Staff of the Federal functional regulators[440]**
- **Nevada Gaming Control Board**

440 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 is the largest self-regulatory organization for broker-dealers doing business with the public in the United States.

METHODOLOGY

Treasury's Office of Terrorist Financing and Financial Crimes by statute is the AML/CFT policy coordination 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 though 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 s listed above, participated in the development of the risk assessment. This year, we engaged with several State agencies, particularly with respect to the Casino and Gaming Section (See list of Participants). Data collected is current as of January 31, 2024.

Section I on Threats is based on discussions with law enforcement and cites specific public charges that are intended to provide an example of the wider trends identified by investigators. The discussion of each threat category highlights their consequences, including the harm inflicted upon U.S. citizens and the effects on the U.S. economy. Understanding the threat environment is essential to understanding the vulnerabilities that create opportunities for laundering illicit proceeds.

Numerous federal agencies collect data on the outcomes of their illicit finance investigations at the agency, interagency, and government-wide levels. However, a single source of comprehensive, government-wide data on the full range of such outcomes does not exist. Therefore, identifying cases based solely on charges filed is challenging. For instance, although there are specific money laundering statutes, additional statutes might include relevant cases - such as tax evasion - but be overly broad for the purpose of conducting such searches. Furthermore, agencies may charge defendants under the predicate crime instead of under a money laundering-related statute or a prosecutor may drop a money laundering charge as part of a plea bargain. We have identified those cases (mainly citing DOJ or LEA Press Releases) that demonstrate some type of *ML activity* or how criminal actors 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. The case examples only cite the names of those found guilty. We have also utilized qualitative data, often provided by LEAs, 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 sources."

We have incorporated advisories, alerts and bulletins published by our LEAs, FinCEN, and consumer protection agencies (*e.g.,* the Consumer Trade Commission). Examples include public service announcements on various types of frauds/scams. From a drug perspective, we relied on national drug threat assessments and data provided by our health protection agencies (*e.g.,* Centers for Disease Control and Prevention). We also rely on top-down assessments or strategies produced at the national level, which the President of the United States issues. These have included national efforts to combat human

trafficking, ransomware, and corruption among other criminal threats with a financial nexus. We also use open-source documents from our Intelligence Community such as the "Annual Threat Assessment of the U.S. Intelligence Community."

From a vulnerability perspective, we rely on regulatory agencies who issue public advisories, such as on the role of the U.S. Dollar, data on financial products or services, or various types of frauds and scams. U.S. federal functional regulators (banks, securities, commodities) also issue annual supervisory insights and examination priorities which provides insight into areas of focus for compliance based on current or emerging shortcomings in AML/CFT compliance. We also utilize information from our FFIRAs, including the BSA/AML Manual issued by the Federal Financial Institutions Examination Council (FFIEC). Within the Treasury, we often conduct public (*e.g.,* Art, DeFi) and non-public sectoral (*e.g.,* DNFBPs) risk assessments which assist us in developing our understanding of ML risk and that we have incorporated into the NMLRA.

The Department of the 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.

LIST OF ACRONYMS

ACH	Automated Clearinghouse
ABA	American Bar Association
AEC	Anonymity-Enhanced Cryptocurrencies
AML/CFT	Anti-Money Laundering / Countering the Financing of Terrorism
ANPRM	Advance Notice of Proposed Rulemaking
ATM	Automated Teller Machine
AUM	Assets Under Management
BCS	Bulk Cash Smuggling
BEC	Business Email Compromise
BOI	Beneficial Ownership Information
BSA	Bank Secrecy Act
CBP	U.S. Customs and Border Protection (Department of Homeland Security)
CDD	Customer Due Diligence
CDG	Clan del Golfo
CEO	Chief Executive Officer
CFTC	Commodity Futures Trading Commission
CIB	Cash-Intensive Business
CIP	Customer Identification Program
CJNG	Cártel Jalisco Nueva Generación
CMLO	Chinese Money Laundering Organization
CTA	Corporate Transparency Act
CTR	Currency Transaction Report
CVC	Convertible Virtual Currency
DEA	Drug Enforcement Administration (U.S. Department of Justice)
DeFi	Decentralized Finance
DHS	Department of Homeland Security
DOJ	Department of Justice
DPRK	Democratic Republic of North Korea
DTO	Drug Trafficking Organization
EDD	Enhanced Due Diligence
EFE	Elder Financial Exploitation
EIDL	Economic Injury Disaster Loan
ERC	Employee Retention Credit
FAA	Federal Aviation Administration
FATF	Financial Action Task Force
FBI	Federal Bureau of Investigation

FCM	Futures Commission Merchant
FCPA	Foreign Corrupt Practices Act
FDIC	Federal Deposit Insurance Corporation
FFIEC	Federal Financial Institutions Examination Council
FFIRAs	Federal Financial Institution Regulatory Agencies
FinCEN	Financial Crimes Enforcement Network (U.S. Department of the Treasury)
FINRA	Financial Industry Regulatory Authority
FRB	Board of Governors of the Federal Reserve System (or "Federal Reserve Board")
FTC	Federal Trade Commission
FY	Fiscal Year
GTO	Geographic Targeting Order
ICE HSI	U.S. Immigration and Customs Enforcement Homeland Security Investigations (U.S. Department of Homeland Security)
IC3	Internet Crime Complaint Center (Federal Bureau of Investigation)
IOLTA	Interest on Lawyers' Trust Accounts
IPO	Initial Public Offering
IRS-CI	Internal Revenue Service-Criminal Investigation
IVTS	Informal Value Transfer Service
ML/TF	Money Laundering/Terrorist Financing
MLO	Money Laundering Organization
MSB	Money Services Business
NCUA	National Credit Union Administration
NDAA	National Defense Authorization Act
NDTA	National Drug Threat Assessment
NPRM	Notice of Proposed Rulemaking
OCC	Office of the Comptroller of the Currency
OCDETF	Organized Crime Drug Enforcement Task Forces (U.S. Department of Justice)
OFAC	Office of Foreign Assets Control (U.S. Department of the Treasury)
PII	Personally Identifiable Information
PML	Professional Money Laundering
PMSJs	Precious Metals, Stones, And Jewels
PEP	Politically Exposed Person
PMO	Postal Money Order
PPP	Paycheck Protection Program
PRC	People's Republic of China
P2P	Peer-To-Peer
RIA	Registered Investment Adviser
RMB	Chinese Renminbi

SAR	Suspicious Activity Report
SBA	Small Business Administration
SB/SE	Small Business/Self-Employed
SEC	Securities and Exchange Commission
SDN	Special Designated National
TBML	Trade-Based Money Laundering
TCO	Transnational Criminal Organization
TCSP	Trust and Company Service Provided
TPPP	Third-Party Payment Processor
USD	U.S. Dollar
USPIS	U.S. Postal Inspection Service
VAIS	Virtual Asset Investment Scheme
VASP	Virtual Asset Service Provider


THE DEPARTMENT OF THE TREASURY
1789