# National Money Laundering Risk Assessment

February 2022

Department of the Treasury

# National Money Laundering Risk Assessment

# Table of Contents

# EXECUTIVE SUMMARY

This is the third publication of the National Money Laundering Risk Assessment (NMLRA) since the inaugural publication in 2015. The Department of the Treasury is publishing it during a transformative time for crime with increasing cybercrime complaints from the public exceeding $4.1 billion in 2020, a proliferation of ransomware attacks holding hostage sensitive information and demanding payment from U.S. citizens and businesses, and a growing overdose crisis that has killed over 100,000 citizens in a one-year period, quadrupling over the last decade, largely driven by synthetic opioids like fentanyl.

Fundamentally, money laundering is a necessary consequence of almost all profit-generating crimes. Money laundering remains a significant concern because it facilitates and conceals crime and can distort markets and the broader financial system. The United States is particularly vulnerable to all forms of illicit finance because of the size of the U.S. financial system and the centrality of the U.S. dollar in the payment infrastructure supporting global trade. Criminals and professional money launderers continue to use a wide variety of methods and techniques, including traditional ones, to place, move, and attempt to conceal illicit proceeds. These range from the traditional use of cash to the purchase of luxury or high-value goods, to the ever-evolving world of virtual assets and related service providers, including decentralized finance and the growing use of anonymity-enhancement technologies.

Fraud dwarfs all other proceed-generating crimes that are laundered in or through the United States. The exploitation of data, mainly personal identifiable information that is stolen, hacked, or compromised, remains one of the most common methods fraudsters, launderers, and other criminals use to set up bank accounts and conceal fraudulent activity. Drug trafficking, cybercrime, human trafficking and smuggling, and corruption also generate significant volumes of illicit proceeds within the United States or through the U.S. financial sector.

The COVID-19 pandemic affects almost every aspect of social interaction and human activity globally, to include how criminals earn money and launder their proceeds. Criminals have exploited government-led economic support programs during the pandemic. The pandemic has led to an increase in fraud risk for online financial services and general commerce, resulting in a dramatic spike in the number of stimulus, healthcare, bank, elder, and government fraud schemes and scams. Cybercriminals and malicious foreign state actors have and are continuing to exploit the COVID-19 pandemic through phishing schemes, exploitation of remote applications, ransomware, and business email compromise (BEC) fraud.

While many regulated U.S. financial institutions have adequate anti-money laundering (AML) programs, compliance deficiencies at some institutions continue to be a money laundering vulnerability, particularly considering the size and global reach of the industry. Additionally, certain financial intermediaries, such as investment advisers and third-party payment processors, are not subject to comprehensive AML/countering financing of terrorism (CFT) regulations and the NMLRA analyzes these intermediaries for their vulnerability to money laundering.

Key weaknesses within the U.S. AML/CFT regulatory regime include a lack of timely access to beneficial ownership information of legal entities and lack of transparency in non-financed real estate transactions. The deliberate misuse of legal entities and arrangements, including limited liability companies and other corporate vehicles, trusts, partnerships, and the use of nominees, continue to be significant tools for facilitating money laundering and other illicit financial activity in the U.S. financial system.

The 2022 NMLRA's purpose is to inform the understanding of risk by governmental and private sector actors, risk mitigation strategies of financial institutions, and policy deliberations by the U.S. government. In addition to identifying the most significant money laundering risks to the United States, the 2022 NMLRA includes "special focus" snapshots on topics that have not been identified or fully addressed in previous risk assessments. These specialized topics include COVID-19-related fraud and scams, synthetic identify fraud, Chinese Money Laundering

Organizations, wildlife trafficking, trusts, the art industry, and non-federally chartered Puerto Rican financial entities.

The many case studies included in the 2022 NMLRA ultimately reflect instances where money laundering was uncovered and mitigated because of the strength of our existing AML/CFT regime. However, some sectors and money laundering vulnerabilities require further attention from both the public and private sectors especially in response to the evolving threat environment.

This risk assessment along with the 2022 National Terrorist Financing and Proliferation Financing Risk Assessments serve as a prologue to the 2022 National Strategy to Combat Terrorist and Other Illicit Financing (2022 Strategy). The 2022 Strategy provides a detailed roadmap of the actions that the United States should take to further strengthen our AML/CFT regime and address its long-standing vulnerabilities. Once implemented, these actions will make the United States safer and better positioned to identify and disrupt illicit finance. To achieve these goals, the federal government must partner with state and local governments, the private sector, and foreign governments.

# INTRODUCTION

This report identifies the most significant money laundering threats, vulnerabilities, and risks faced by the United States. It is based on a review of federal and state public sector analysis, enforcement actions, and guidance, as well as interviews with U.S. Department of the Treasury (Treasury) staff, intelligence analysts, law enforcement agents, and prosecutors. The NMLRA uses all available information to identify the current money laundering environment within the United States. Relevant component agencies, bureaus, and offices of the Treasury, the U.S. Department of Justice (DOJ), and the U.S. Department of Homeland Security (DHS), as well as U.S. regulatory agencies, participated in the development of the risk assessment. Data collected are current as of December 31, 2021. However, we also highlighted Treasury's study on the Facilitation of Money Laundering and Terror Finance Through the Trade in Works of Art published in February 2022.

Money laundering continues to be a significant concern because it facilitates and conceals crime and can distort markets and the broader financial system. The United States is particularly vulnerable to all forms of illicit finance because of the size of the U.S. financial system and the centrality of the U.S. dollar in the payment infrastructure supporting global trade.

# Participants

This report incorporates published and unpublished research and the analysis, insights, and observations of managers and staff from U.S. government agencies, which also reviewed this report. In drafting this assessment, the Treasury's Office of Terrorist Financing and Financial Crimes (TFFC) 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)
  - 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**
  - Immigration and Customs Enforcement (ICE)
  - 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**[1]

Given the COVID-19 pandemic, the primary authors of this report did not have many face-to-face meetings with U.S. government operational agencies when seeking input for this year's assessment. However, as in previous versions, the 2022 NMLRA relies on open-source reporting from the DOJ, the use of publicly available court documentation,[2] and meetings with law enforcement via videoconference. In addition, this assessment includes feedback received directly from several U.S. Attorney Offices (USAOs) in the field, which provided additional insight beyond the expertise provided by many units of DOJ's Criminal Division in Washington and others at DOJ.

1 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.

2 The charges contained in an indictment are merely allegations. All defendants are presumed innocent unless, and until, proven guilty beyond a reasonable doubt in a court of law.

# Methodology

The terminology and methodology of the NMLRA are based in part on the guidance of the Financial Action Task Force (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 specific 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, taking into consideration the effect of mitigating measures including regulation, supervision, and enforcement.

# SECTION I. THREATS

In the context of the NMLRA, money laundering threats are the predicate crimes that generate illicit proceeds for laundering in, from, or through the United States. 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. This year's risk assessment identifies the most significant money laundering threats to the United States and includes "special focus" snapshots on emerging threats that were not identified or fully addressed in previous risk assessments. The findings related to money laundering threats within this risk assessment (and related risk assessments on terrorist financing and proliferation financing) align with the 2021 National AML/CFT Priorities issued by FinCEN.[3]

This section 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 harms 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.

## FRAUD

Fraud,[4] 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 magnitude of illicit proceeds, generating billions of dollars annually. Some individual investment fraud or Ponzi schemes can generate a billion dollars in proceeds alone.[5] For example, in the Bernard Madoff securities fraud case, the DOJ has distributed almost $3.7 billion in forfeited funds to nearly 40,000 victims, including many older victims.[6] Romance scams, considered one of the fastest growing fraud trends, are also seeing vast increases in illicit proceeds generated. For example, from January 1, 2021 to July 31, 2021, the FBI's Internet Crime Complaint Center (IC3) received over 1,800 complaints related to online romance scams, resulting in losses of approximately $133 million.[7] Scams which involved the use of social media, to include online shopping, romance scams, and supposed economic relief or income opportunities, have been rising steadily over the past few years. For example, reports that people lost money to scams that started on social media more than tripled in the past year, with a sharp increase in the second quarter of 2020.[8]

---

3 FinCEN, *Anti-Money Laundering and Countering the Financing of Terrorism National Priorities* (FinCEN, *AML/CFT Priorities)*, (Jun. 30, 2021), https://www.fincen.gov/sites/default/files/shared/AML_CFT Priorities (June 30%2C 2021).pdf. As required by Section 5318(h)(4)(C) of the Bank Secrecy Act (BSA), the Priorities are consistent with Treasury's 2018 and 2020 National Strategy for Combating Terrorist and Other Illicit Financing (the "National Strategy"), which are informed and supported by underpinning risk assessments on money laundering, terrorist financing, and proliferation financing.

4 Fraud is also considered one of the eight national AML/CFT priorities.

5 DOJ, "Two Remaining Defendants of $1.3 Billion Investment Fraud (Ponzi) Scheme – One of the Largest Ever Charged in South Florida – Plead Guilty to Mail and Wire Fraud Conspiracy," (Jul. 13, 2021), https://www.justice.gov/usao-sdfl/pr/two-remaining-defendants-13-billion-investment-fraud-ponzi-scheme-one-largest-ever; DOJ, "DC Solar Owner Sentenced to 30 Years in Prison for Billion Dollar Ponzi Scheme," (Nov. 9, 2021), https://www.justice.gov/usao-edca/pr/dc-solar-owner-sentenced-30-years-prison-billion-dollar-ponzi-scheme.

6 DOJ, "Acting Manhattan U.S. Attorney Announces Additional Distribution Of More Than $488 Million To Victims Of Madoff Ponzi Scheme," (Dec. 10, 2020), https://www.justice.gov/usao-sdny/pr/acting-manhattan-us-attorney-announces-additional-distribution-more-488-million-victims.

7 FBI Public Service Announcement, "Scammers Defraud Victims of Millions of Dollars in New Trend in Romance Scams," (Sep. 26, 2021), https://www.ic3.gov/Media/Y2021/PSA210916.

8 Federal Trade Commission (FTC), "Consumer Protection Data Spotlight: Scams starting on social media proliferate in early 2020," (Oct. 20, 2020), https://www.ftc.gov/news-events/blogs/data-spotlight/2020/10/scams-starting-social-media-proliferate-early-2020.

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, insurance companies); (2) by victim (e.g., elders, investors, taxpayers); or (3) by how fraud is perpetrated (e.g., identity theft/fraud, BEC, account takeover, check fraud, loan fraud, wire fraud, credit/debit card fraud, securities fraud); however there can be significant overlap in these classifications. At the broadest level, financial fraud distorts U.S. markets, harms national security, and undermines public confidence in the financial sector and government benefits and emergency relief programs. This is especially the case because of the vast and increasing numbers of citizens who are victimized and the billions of dollars stolen from government programs and private companies at the hands of sophisticated criminal actors and transnational criminal organizations (TCOs).[9] Fraud also has the capacity to disrupt economic activity and put legitimate businesses at a distinct competitive disadvantage.

The exploitation of data, mainly personal identifiable information (PII) that is stolen, hacked, or compromised, remains one of the most common methods fraudsters, launderers, and other criminals use to set up bank accounts and conceal fraudulent activity.[10] As noted in the 2018 NMLRA, large organized fraud groups use vast money mule networks as third-party money laundering mechanisms to launder illicit proceeds from fraud and other financial crimes (e.g., romance scams, employment scams, work-from-home scams).[11] A money mule is someone who, either wittingly or unwittingly, transfers or moves illegally acquired money on behalf of someone else.[12] In 2021, during the 10-week Money Mule Initiative campaign, agencies took action against approximately 4,750 individuals suspected of being money mules.[13] Law enforcement has also observed that organized fraud rings are increasingly using credit cards[14] and stored value gift cards[15] to launder money.

Online scams are designed to defraud victims into sending money to bank accounts, debit cards, and virtual wallets controlled by criminals. For example, in romance scams, a criminal adopts a fake online identity to gain a fraud victim's affection and trust. The scammer then uses the illusion of a romantic or close relationship to manipulate or steal from the fraud victim. To carry out the schemes, the criminals often use fake passports with numerous aliases or in the name of other accountholders to open bank accounts to collect and launder the proceeds of the romance scams. The criminals then make large cash withdrawals from those accounts, often multiple times in a single day and generally structured in amounts less than $10,000 to evade detection and reporting requirements. These transfers are often authorized by, and conducted in the names of, account holders, despite warnings from law enforcement or the fraud departments of financial institutions.

9 While considered a separate AML/CFT priority, TCOs are referenced throughout this document based on the type of money laundering threat they are associated with, rather than the regional or national basis of that group (e.g., Asian, African, Russian).

10 See Section on Synthetic Identity Theft for further information.

11 The FATF defines third-party money laundering as the laundering of proceeds by a person who was not involved in the commission of the predicate offence. See FATF, *Professional Money Laundering*, (2018), https://www.fatf-gafi.org/media/fatf/documents/Professional-Money-Laundering.pdf.

12 FBI, *Money Mule Awareness*, (n.d.), https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/money-mules.

13 FBI, *Money Mule Initiative*, (2021), https://www.justice.gov/civil/consumer-protection-branch/money-mule-initiative.

14 DOJ, "Two Architects Of Fraudulent Scheme Sentenced For Processing Over $150 Million Through U.S. Financial Institutions," (Jun. 21, 2021), https://www.justice.gov/usao-sdny/pr/two-architects-fraudulent-scheme-sentenced-processing-over-150-million-through-us.

15 DOJ, "Federal Grand Jury Indicts 4 SoCal Defendants in Scheme to Launder Target Gift Cards Purchased by Victims of Scams," (Sep. 28, 2021), https://www.justice.gov/usao-cdca/pr/federal-grand-jury-indicts-4-socal-defendants-scheme-launder-target-gift-cards.

## 1. Special Focus: COVID-19-Related Fraud and Scams

The global COVID-19 pandemic, the largest public health crisis in modern times, has significantly accelerated the transition from in-person financial activities to online account opening, payments, and lending. This has increased the fraud risk for online financial services and commerce in general and led to a dramatic spike in the number of stimulus, healthcare,[16] bank, elder, and government fraud schemes and scams exploiting the COVID-19 pandemic.[17] It remains to be seen if this trend is transitory or represents a permanent shift in consumer behavior. What is clear is that the pandemic provided an opportunity for fraudsters to exploit PII stolen through the large-scale data breaches that have occurred over the past few years. Some cases demonstrate repeat offenders who were engaged in other types of fraud prior to the pandemic.[18] Law enforcement suspects that large fraud groups were looking for new fraud schemes to exploit this stolen data in a more efficient manner and found it with the shift to the use of online financial transactions by both government and private sector actors.

As of October 25, 2021, the DOJ publicly charged 984 defendants with criminal offenses in 682 cases based on fraud schemes connected to the COVID-19 pandemic. These cases involved attempts to obtain over $753 million from the U.S. government and unsuspecting individuals. Criminals and bad actors have exploited the increased use of remote access to online accounts and stimulus programs. Many of the schemes observed during the pandemic mirror the kinds of illicit finance activity seen prior to the pandemic. However, criminals have been leveraging COVID-19 themes as lures, targeting vulnerable individuals and companies that are seeking healthcare information and products or contributing to relief efforts, as well as individuals who lost work during the pandemic and are seeking new employment. Individual scammers and complex TCOs (e.g., Nigerian fraud rings) have been taking advantage of the pandemic for their own profit. Below are two of the largest categories of pandemic-related fraud, but there are a number of other COVID-19-related schemes not included in this section.

### *a) Exploiting Stimulus Measures*

Beginning in the initial phases of the pandemic, fraudsters focused on various government stimulus programs aimed at relieving the negative economic impact of COVID-19, provided under the Coronavirus Aid, Relief, and Economic Security (CARES) Act,[19] including the Paycheck Protection Program (PPP),[20] unemployment insurance

16 DOJ, "DOJ Announces Coordinated Law Enforcement Action to Combat Health Care Fraud Related to COVID-19," (May 26, 2021), https://www.justice.gov/opa/pr/doj-announces-coordinated-law-enforcement-action-combat-health-care-fraud-related-covid-19.

17 For example, from March through October 2020, a total of 5,344 financial institutions filed 118,625 suspicious activity reports (SARs) associated with the CARES Act programs. Examples of suspicious activity identified by financial institutions included rapid movement of funds, identity theft, and forgeries. As of December 2020, FinCEN has shared over 3,000 COVID-19-related referrals with the DOJ SAR Review Team and other task forces. U.S. Government Accountability Office, *COVID-19: Critical Vaccine Distribution, Supply Chain, Program Integrity, and Other Challenges Require Focused Federal Attention* (GAO-21-265), (Jan. 28, 2021), https://files.gao.gov/reports/GAO-21-265/index.html.

18 DOJ, "Repeat Fraudster Sentenced for COVID-19 Loan Fraud Scheme," (Mar. 11, 2020), https://www.justice.gov/usao-edva/pr/repeat-fraudster-sentenced-covid-19-loan-fraud-scheme. For additional information, see the significant number of FinCEN advisories and notices to financial institutions detailing money laundering risks arising from the COVID-19 pandemic, available at https://www.fincen.gov/coronavirus.

19 FinCEN, "Advisory on Financial Crimes Targeting COVID-19 Economic Impact Payments," (Feb. 24, 2021), https://www.fincen.gov/sites/default/files/advisory/2021-02-25/Advisory%20EIP%20FINAL%20508.pdf; see also FinCEN, "Advisory on Imposter Scams and Money Mule Schemes Related to Coronavirus Disease 2019 (COVID-19)," (Jul. 7, 2020), https://www.fincen.gov/sites/default/files/advisory/2020-07-07/Advisory_Imposter_and_Money_Mule_COVID_19_508_FINAL.pdf.

20 DOJ, "Man Sentenced for Covid-19 Relief Fraud," (Jul. 30, 2021), https://www.justice.gov/opa/pr/man-sentenced-covid-19-relief-fraud; DOJ, "Texas Man Sentenced for $24 Million COVID-19 Relief Fraud Scheme," (Jul. 28, 2021), https://www.justice.gov/opa/pr/texas-man-sentenced-24-million-covid-19-relief-fraud-scheme; DOJ, "Los Angeles Man Arrested for $27 Million PPP Fraud Scheme," (Jul. 22, 2021), https://www.justice.gov/opa/pr/los-angeles-man-arrested-27-million-ppp-fraud-scheme.

(UI),[21] and Economic Injury Disaster Loan (EIDL).[22]

Criminals have often relied on the use of false documents and statements to exploit the use of previously hacked PII to illegally apply for benefits to the programs noted above and to open various types of accounts online (e.g., bank, investment) to deposit these funds. Money mule networks have often moved proceeds generated by fraudsters using multiple Automated Clearinghouse (ACH) payments disbursed to a single bank account held by a suspected money mule not named as a payment beneficiary. Law enforcement also identified the use of funnel accounts in these schemes, which involve multiple deposits sent to a single account.[23] The misuse of a large portion of PPP/EIDL loan funds involved purchasing real estate, luxury vehicles, travel, and merchant purchases. The USSS notes that banks and investment firms have been used to receive the proceeds of the loans and that various online investment platforms have also been used to launder funds obtained from these programs.

Law enforcement and government oversight mechanisms have identified several vulnerabilities presented by the online EIDL application processes, which criminals exploited. These include the lack of trustworthy online access identity proofing and appropriate eligibility determinations for the loan programs. For example, criminals have often used multiple synthetic emails with the same Internet Protocol (IP) address to submit numerous applications for benefits across many claims. This vulnerability could be addressed by more robust identity proofing of applicants and authentication of eligible beneficiaries for payments of benefits and loan distribution. Several EIDL/PPP cases also involved bank fraud. In just one example, individuals allegedly created 12 fictitious business entities that were used to fraudulently apply for PPP loans, and then sent multiple applications for the same businesses to more than 10 different banks, without disclosing to those banks that they were submitting duplicative applications.[24]

Criminal actors ranging from domestic low-level criminals to TCOs have targeted UI program funds by using stolen identities to file for benefits. Given that applications are made through each state, individuals have stolen identities of people who have not yet applied and applied in their names. After account holders received payments, they moved some or all of the money, often to a third party, using a variety of methods, including wire transfers, cash withdrawals, money orders, virtual assets, gift cards, and mobile payment systems. Several UI-related cases have involved imprisoned individuals who applied for benefits under their own name or who used the PII of other inmates to submit fraudulent claims.[25] In an example of the former, the inmates used jail phones or other inmate communications to direct or assist persons outside the prison to file claims online using the inmate's

21 AP News, "California's unemployment fraud reaches at least $20 billion," (Oct. 26, 2021), https://apnews.com/article/business-california-5ec16ebe5b5982a9531a7a3d5a45e93c; see also FinCEN, "FinCEN Advisory on Unemployment Insurance Fraud During the Coronavirus Disease 2019 (COVID-19) Pandemic, (Oct. 13, 2020), https://www.fincen.gov/sites/default/files/advisory/2020-10-13/Advisory%20Unemployment%20Insurance%20COVID%2019%20508%20Final.pdf.

22 DOJ, "Berwick Man Pleads Guilty To Committing Over $400,000 In Covid-Relief Fraud," (Oct. 20, 2021), https://www.justice.gov/usao-mdpa/pr/berwick-man-pleads-guilty-committing-over-400000-covid-relief-fraud.

23 For more on funnel account activity see FinCEN, "FinCEN Advisory FIN-2014-A005," (May 28, 2014), https://www.fincen.gov/resources/advisories/fincen-advisory-fin-2014-a005; FinCEN, "FinCEN Advisory FIN-2012-A006." (Jul. 18, 2012), https://www.fincen.gov/resources/advisories/fincen-advisory-fin-2012-a006.

24 DOJ, "Tulsa Couple Plead Guilty to Bank Fraud After Applying for Paycheck Protection Program Loans under False Pretenses," (Mar. 12, 2021), https://www.justice.gov/usao-ndok/pr/tulsa-couple-plead-guilty-bank-fraud-after-applying-paycheck-protection-program-loans.

25 DOJ, "Two Plead Guilty in COVID-19 Unemployment Benefit Fraud Scheme," (Mar. 12, 2021), https://www.justice.gov/usao-edca/pr/two-plead-guilty-covid-19-unemployment-benefit-fraud-scheme; DOJ, "18 Pennsylvania Prison Inmates and Accomplices Charged with Fraudulently Obtaining Pandemic Unemployment Assistance Funds," (Oct. 10, 2020), https://www.justice.gov/usao-edpa/pr/18-pennsylvania-prison-inmates-and-accomplices-charged-fraudulently-obtaining-pandemic; DOJ, "33 Inmates and Accomplices Charged with Illegally Obtaining Coronavirus Unemployment Benefits," (Aug. 20, 2020), https://www.justice.gov/usao-wdpa/pr/33-inmates-and-accomplices-charged-illegally-obtaining-coronavirus-unemployment.

accurate PII, including their full name, date of birth, and social security number, but falsely asserting that the inmate was available to work and unemployed as a result of the COVID-19 pandemic.

Additionally, the CARES Act included a foreclosure moratorium, whereby servicers of federally backed mortgage loans were required to grant borrowers loan forbearances for up to 12 months, including extension requests, without the accrual of additional interest or fees.[26] According to federal and state law enforcement sources, criminals took advantage of this program by setting up fraudulent loan modification and debt relief services targeting mortgagers suffering financial hardships caused by the COVID-19 pandemic.[27] The fraudsters collected up-front fees for loan modification or aid, and then disappeared with the fees mortgagers paid them. Sometimes criminals directed homeowners to make monthly mortgage payments to the fraudulent loan modification companies, while the bank holding the mortgage was led to believe the homeowner had chosen to go into forbearance.

### *b) Vaccine Fraud, Fake Cures, and Fraudulent Vaccine Cards*

The COVID-19 Consumer Protection Act, passed by Congress in December 2020, prohibits deceptive acts or practices associated with the treatment, cure, prevention, mitigation, or diagnosis of COVID-19.[28] COVID-19 vaccine fraud may include the sale of unapproved and illegally marketed purported vaccines, the sale of counterfeit versions of approved vaccines, and the illegal diversion of legitimate vaccines. In the early days of the pandemic, fraudsters offered, for a fee, to provide potential victims with a vaccine sooner than permitted under the applicable vaccine distribution plan. Scammers around the world have also been attempting to sell fake and unlawful cures,[29] treatments, and personal protective equipment (PPE).[30] This includes instances of major fraud against the United States[31] dealing with hoarding or price gouging of PPE and nondelivery scams.[32] Criminals have preyed on the public's fear of COVID-19 to overcharge for, or defraud them into purchasing, counterfeit PPE[33] and vaccines. Cases have demonstrated a variety of payment mechanisms used to move illicit proceeds within criminal networks to include peer-to-peer (P2P) mobile payment apps to transfer money among the co-conspirators. With the recent implementation of regulations and guidelines requiring vaccination cards and identification to enter certain venues (e.g., restaurants, theaters, etc.), the FBI has also witnessed an increase in the manufacturing and sale of

26 NCUA, "Navigating and Understanding the End of Pandemic-Era Homeowner Protection Programs," (Sep. 2021), https://www.ncua.gov/regulation-supervision/letters-credit-unions-other-guidance/navigating-and-understanding-end-pandemic-era-homeowner-protection-programs.

27 New Jersey Division of Consumer Affairs, "AG Grewal, Banking and Insurance Commissioner Caride Announce Action to Stop Sham Mortgage Relief Scheme Targeting Financially Struggling Homeowners. State Obtains Temporary Restraints to Halt Defendants' Ongoing Business Activities and Freeze Assets," (Jan. 5, 2020), https://www.njconsumeraffairs.gov/News/Pages/01052021x.aspx.

28 DOJ, "Justice Department and FTC Announce Action to Stop Deceptive Marketing of Purported COVID-19 Treatments," (Apr. 15, 2021), https://www.justice.gov/opa/pr/justice-department-and-ftc-announce-action-stop-deceptive-marketing-purported-covid-19.

29 DOJ, "Department of Justice Acts To Stop Sale Of 'Nano Silver' Product As Treatment For Covid-19," (Nov. 13, 2020), https://www.justice.gov/opa/pr/department-justice-acts-stop-sale-nano-silver-product-treatment-covid-19.

30 DOJ, "Georgia Man Pleads Guilty in New York Federal Court on Charges Related to Ponzi and COVID-19 Fraud Schemes," (Aug. 10, 2021), https://www.justice.gov/opa/pr/georgia-man-pleads-guilty-new-york-federal-court-charges-related-ponzi-and-covid-19-fraud.

31 18 U.S. Code § 1031.

32 FinCEN, "2020 Advisory on Medical Scams Related to the Coronavirus Disease 2019 (COVID-19), (May 18, 2020), https://www.fincen.gov/sites/default/files/advisory/2020-05-18/Advisory%20Medical%20Fraud%20Covid%2019%20FINAL%20508.pdf.

33 DOJ, "Chinese Manufacturer Charged with Exporting Misbranded and Defective Masks Falsely Purporting to be N95 Respirators," (Jun. 5, 2020), https://www.justice.gov/usao-nj/pr/chinese-manufacturer-charged-exporting-misbranded-and-defective-masks-falsely-purporting.

fraudulent vaccine cards.[34]

In addition, cybercriminals,[35] including ransomware operators, have exploited the COVID-19 pandemic.[36] The websites of legitimate medical and biotechnology companies have been spoofed to trick the public into purchasing vaccines which do not exist. Fraudsters are adapting their techniques based on the timing of the vaccine rollouts. By using traditional phishing techniques, they have created fraudulent COVID-19 vaccine surveys for consumers to fill out with the promise of a prize or cash at the conclusion of the survey when, in fact, the surveys are used to steal money from consumers and unlawfully capture consumers' personal information.[37]

During the pandemic, illicit actors have taken advantage of several COVID-19-related measures, including the increased use of remote applications, virtual environments, and remote identity processes, to steal information and credentials and disrupt operations. Cybercriminals and state actors have also conducted phishing campaigns, often via email and using COVID-19-related themes, to lure victims. In these schemes, phishing scammers often reference payments related to the CARES Act or advertise ways to make money, such as through investing in virtual assets. Cybercriminals leverage accesses from these campaigns to conduct ransomware attacks, BEC scams, and other illicit activity.

## 2. Special Focus: Synthetic Identity Fraud

In 2021, the Federal Reserve System announced an industry-recommended definition of Synthetic Identity Fraud (SIF), which was developed by a focus group of fraud experts.[38] SIF is the use of a combination of real and fake PII to fabricate a person or entity in order to commit a dishonest act for personal or financial gain.[39] The FBI identifies synthetic identity theft, a term which falls within SIF, as the fastest growing financial crime in the United States. It targets some of society's most vulnerable citizens: children and the elderly.[40] Synthetic identity theft is different from traditional identity theft in that both real and fictitious information is used to create a new identity. While SIF is not new, inconsistent definitions made it difficult to identify and address this type of fraud.

Traditional identity theft involves a victim's actual identity being used without their knowledge (e.g., applying for a credit card or other loan, using the victim's real name, date of birth, address, and social security number [or SSN]).[41] According to the Federal Trade Commission (FTC), in 2020, nearly 1.4 million reports of identity theft were received through the FTC's IdentityTheft.gov website, about twice as many as in 2019.[42] For both traditional and

34 DOJ, "Woman Arrested for Fake COVID-19 Immunization and Vaccination Card Scheme," (Jul. 14, 2021), https://www.justice.gov/opa/pr/woman-arrested-fake-covid-19-immunization-and-vaccination-card-scheme.

35 See Cybercrime Section for further information about these scams.

36 FinCEN, "FinCEN Asks Financial Institutions to Stay Alert to COVID-19 Vaccine-Related Scams and Cyberattacks, (Dec. 20, 2020), https://www.fincen.gov/sites/default/files/shared/COVID-19 Vaccine Notice 508.pdf; FinCEN, "FinCEN Advisory on Cybercrime and Cyber-Enabled Crime Exploiting the Coronavirus Disease 2019 (COVID-19) Pandemic," (Jul. 30, 2020), https://www.fincen.gov/resources/advisories/fincen-advisory-fin-2020-a005.

37 DOJ, "Justice Department Warns About Fake Post-Vaccine Survey Scams," (Apr. 1, 2021), https://www.justice.gov/opa/pr/justice-department-warns-about-fake-post-vaccine-survey-scams.

38 While use of this definition throughout the industry is encouraged, adoption of the definition is voluntary at the discretion of each individual entity. Absent written consent, this definition may not be used in a manner that suggests the Federal Reserve endorses a third-party product or service.

39 The Federal Reserve, Fedpayments Improvement, "Synthetic Identity Fraud Defined," (n.d.), https://fedpaymentsimprovement.org/strategic-initiatives/payments-security/synthetic-identity-payments-fraud/synthetic-identity-fraud-defined/.

40 FBI, "Synthetic Identity Theft," (Jan. 2, 2020), https://www.fbi.gov/audio-repository/ftw-podcast-synthetic-ids-010220.mp3/view.

41 Social Security Administration (SSA), "Identity Theft and Your Social Security Number," (Jul. 2021), https://www.ssa.gov/pubs/EN-05-10064.pdf.

42 FTC, "New Data Shows FTC Received 2.2 Million Fraud Reports from Consumers in 2020," (Feb. 4, 2021), https://www.ftc.gov/

synthetic identity theft, criminals use various tactics to gain access to PII of their victims. Such methods include malware that can be distributed using malicious social media ads, phishing emails, and other channels, such as caller identity document spoofing to trick victims into giving criminals sensitive data. Another common source for PII is data breaches. Criminals can purchase compromised PII data via the internet or darknet marketplaces where hackers monetize stolen data. Moreover, the randomization of issuing SSNs by the Social Security Administration (SSA)[43] since 2011 has made it more difficult to detect fraud as it is no longer easy to associate an individual's age and geography to an application.

In July 2019, the Federal Reserve System issued a white paper highlighting vulnerabilities that are inherent in the credit process in the United States and allow fraudsters to create synthetic identities.[44] For fraudsters to create a synthetic identity, they must create a credit profile of record with the major credit bureaus that is generated when the criminal applies for credit (e.g., typically a credit card, using a fabricated set of PII derived from actual and fake PII). Regardless of the disposition of the credit application, the credit bureaus automatically create a "new" credit profile, which can then be used by the criminal to apply for credit at a different financial institution and pass identity verification processes.

Synthetic identities are used to establish bank accounts, open credit card accounts, make fraudulent purchases, but also to gain access to the U.S. financial sector anomalously. For example, a synthetic identity may be created for an individual who might otherwise be unable to access the U.S. financial system (e.g., Specially Designated Nationals[45] or individuals with a criminal record). There have been recent efforts to identify criminal schemes in which perpetrators create synthetic identities and use them to defraud financial institutions out of millions of dollars, harming individual victims in the process.[46] One of the main fraud tactics for the "buy now, pay later" (BNPL)[47] payment method recently reported is SIF. This has happened when fraudsters have signed up for a BNPL account using a real identity that has been constructed from multiple data points combined with false information (e.g., name, surname, shipping address).[48]

### 3. Healthcare Fraud

Healthcare fraud continues to be an area of focus, with DOJ estimating that it accounts for the loss of billions of dollars every year.[49] The often high cost of pharmaceuticals, medical procedures, and related devices can make detecting suspicious financial transactions more difficult.

---

news-events/press-releases/2021/02/new-data-shows-ftc-received-2-2-million-fraud-reports-consumers.

43 SSA, "Social Security Number Randomization, (n.d.), https://www.ssa.gov/employer/randomization.html.

44 FRB, "Synthetic Identity Fraud in the U.S. Payment System," (July 2019), https://fedpaymentsimprovement.org/wp-content/uploads/frs-synthetic-identity-payments-fraud-white-paper-july-2019.pdf.

45 As part of its enforcement efforts, OFAC publishes a list of individuals and companies owned or controlled by, or acting for or on behalf of, targeted countries. It also lists individuals, groups, and entities, such as terrorists and narcotics traffickers designated under programs that are not country specific. Collectively, such individuals and companies are called "Specially Designated Nationals" or "SDNs." Their assets are blocked, and U.S. persons are generally prohibited from dealing with them.

46 Suffolk County District Attorney, "13 Individuals and 3 Corporations Indicted for Alleged Nation-Wide Synthetic Identity Scheme," (Sep. 23, 2020), https://suffolkcountyny.gov/da/News-and-Public-Information/Press-Releases/13-individuals-and-3-corporations-indicted-for-alleged-nation-wide-synthetic-identity-scheme.

47 Nerdwallet, "What Is Buy Now, Pay Later?" (Oct. 18, 2021), https://www.nerdwallet.com/article/loans/personal-loans/buy-now-pay-later; see also CNET, "'Buy now, pay later': How Affirm, Afterpay, PayPal's Pay in 4 and Klarna work," (Dec. 9, 2021), https://www.cnet.com/personal-finance/loans/affirm-klarna-afterpay-and-more-buy-now-pay-later-plans-explained/.

48 The Paypers, "The most common fraud threats for individual payment methods," (Oct. 26, 2021), https://thepaypers.com/expert-opinion/the-most-common-fraud-threats-for-individual-payment-methods--1252350.

49 DOJ, Criminal Fraud, "Facts and Statistics," https://www.justice.gov/criminal-fraud/facts-statistics.

As healthcare fraud schemes can be complex and have involved complicit doctors, pharmacists, and other medical professionals, the money flows can mimic legitimate transactions from insurers to healthcare providers. In some cases, complicit healthcare providers and other companies in the healthcare field have incentivized patients to purchase their services or products by illegally offering to pay for co-pay charges.[50] For example, in one scheme, a pharmaceutical company allegedly used a charitable foundation as a conduit to pay the co-pays of thousands of Medicare patients taking the company's product.[51]

In 2020, in the largest healthcare fraud and opioid enforcement action in DOJ's history, 345 defendants, including more than 100 doctors, nurses, and other licensed medical professionals, were charged in related healthcare fraud schemes involving more than $6 billion in alleged fraud losses. The largest amount of alleged fraud loss charged in connection with the cases—$4.5 billion in allegedly false and fraudulent claims—related to schemes involving telemedicine: the use of telecommunications technology to provide health care services remotely.[52]

The outbreak of the COVID-19 pandemic ushered in an era of unprecedented opportunity for criminals to defraud healthcare benefit programs, stimulus programs, and individual consumers searching for legitimate sources of medical aid. Early fraud schemes during the pandemic abused federal stimulus programs and increased exploitation of Medicare, Medicaid, and TRICARE, as well as healthcare programs provided through the Departments of Labor and Veterans Affairs and private health insurance companies.[53] Fraudsters have also targeted COVID-19 relief funds for healthcare providers, such as those provided under the PPP and Health Care Enhancement Act.[54]

## DRUG TRAFFICKING

Drug trafficking, which continues to pose a threat to public health in the United States, generates significant proceeds for the criminal organizations that supply the U.S. and global markets. Drug Trafficking Organizations (DTOs),[55] engaged in the trafficking of a variety of drugs into the United States, use numerous methods to launder proceeds, which remain predominantly cash based. DEA estimates that DTOs continue to generate billions of dollars in illicit proceeds every year.[56]

The movement and laundering of proceeds associated with the illicit drug market in the United States continue

50 DOJ, "Gilead Agrees To Pay $97 Million To Resolve Alleged False Claims Act Liability For Paying Kickbacks," (Sep. 23, 2020), https://www.justice.gov/opa/pr/gilead-agrees-pay-97-million-resolve-alleged-false-claims-act-liability-paying-kickbacks; DOJ, "Former Pittsburgh-area Doctor Pleads Guilty to Unlawfully Prescribing Opioids Health Care Fraud and Money Laundering," (Jul. 13, 2021), https://www.justice.gov/usao-wdpa/pr/former-pittsburgh-area-doctor-pleads-guilty-unlawfully-prescribing-opioids-health-care.

51 DOJ, "Actelion Pharmaceuticals Agrees to Pay $360 Million to Resolve Allegations that it Paid Kickbacks Through a Co-Pay Assistance Foundation," (Dec. 6, 2018), https://www.justice.gov/usao-ma/pr/actelion-pharmaceuticals-agrees-pay-360-million-resolve-allegations-it-paid-kickbacks.

52 DOJ, "2020 National Health Care Fraud and Opioid Takedown," (Sep. 30, 2020), https://www.justice.gov/criminal-fraud/hcf-2020-takedown/press-release.

53 DOJ, "Two Owners of New York Pharmacies Charged in a $30 Million COVID-19 Health Care Fraud and Money Laundering Case," (Dec. 21, 2020), https://www.justice.gov/usao-edny/pr/two-owners-new-york-pharmacies-charged-30-million-covid-19-health-care-fraud-and-money; DOJ, "Florida Man Charged with COVID Relief Fraud, Health Care Fraud and Money Laundering," (Jul. 29, 2020), https://www.justice.gov/opa/pr/florida-man-charged-covid-relief-fraud-health-care-fraud-and-money-laundering.

54 FinCEN, "Advisory on COVID-19 Health Insurance-and Health Care-Related Fraud," (Feb. 2, 2021), https://www.fincen.gov/sites/default/files/advisory/2021-02-02/COVID-19%20Health%20Care%20508%20Final.pdf.

55 A national AML/CFT priority.

56 DEA, *2020 National Drug Threat Assessment* (DEA NDTA), (May 2, 2021), https://www.dea.gov/sites/default/files/2021-02/DIR-008-21%202020%20National%20Drug%20Threat%20Assessment_WEB.pdf, pp.67, 84.

to include traditional methods and techniques, such as bulk cash smuggling (BCS) and trade-based money laundering (TBML), although the COVID-19 pandemic caused some initial disruptions to DTOs using those methods due to travel restrictions and a slower global economy. Financial institutions, including banks and money services businesses (MSBs), remain vulnerable to exploitation by DTOs that use front and shell companies and third parties (including money mules) to wire proceeds from the United States to their base of operations. Another popular way to launder drug proceeds in the United States is through the purchase of real estate as an investment, to use as stash houses, or to grow, manufacture, or distribute illicit narcotics. The role of professional money launderers, particularly Chinese money laundering organizations (CMLOs),[57] is also frequently cited as a growing and significant challenge to law enforcement tracing the movement of drug proceeds.

DTOs are growing more comfortable with darknet markets and the use of virtual assets to launder funds, although the size and scope of drug proceeds generated on the darknet and laundered via virtual assets remain low in comparison to cash-based retail street sales.[58] Worldwide sales on major darknet markets appear to have remained modest when compared to overall illicit drug sales. For example, during 2017–2020, drug-related darknet market sales amounted to approximately $315 million annually, or about 0.2 percent of the combined estimated illicit annual retail drug sales in the United States and European Union.[59]

## 1. Main Drug Types

### *a) Illicit Opioids and Heroin*

Opioids are a class of drugs that include the illegal drug heroin, synthetic opioids such as fentanyl, and pain relievers available legally by prescription, such as oxycodone (OxyContin®), hydrocodone (Vicodin®), codeine, morphine, and many others.[60] The dramatic spike in the abuse of prescription drugs, heroin, and synthetic opioids such as fentanyl and its analogues has accelerated over the past three years. Pharmaceutical fentanyl is a synthetic opioid, approved for treating severe pain, typically advanced cancer pain. It is 50 to 100 times more potent than morphine. However, illegally made fentanyl is sold through illicit drug markets for its heroin-like effect, and it is often mixed with heroin or other drugs, such as cocaine, or pressed into counterfeit prescription pills.[61] Fentanyl and related synthetic opioids are among a category of synthetic drugs that, when diverted or used outside of prescribed medical parameters, challenge current trafficking policy responses. This is because pharmaceutical applications of these drugs, their analogues (which can be chemically altered to avoid international controls), and precursors often have or were developed for legitimate medical uses, which can make the diversion harder for investigators to detect or interdict. Provisional data from the Centers for Disease Control and Prevention's (CDC's) National Center for Health Statistics indicates that there were an estimated 100,306 drug overdose deaths in the United States during the 12-month period ending in April 2021.[62] The new data documents that estimated overdose deaths from opioids increased to 75,673 in the 12-month period ending in April 2021, up from 56,064 the year before. Synthetic opioids (other than methadone) are currently the main driver of drug

57 See Chinese Money Laundering Organization Section for further information.

58 DOJ, "International Law Enforcement Operation Targeting Opioid Traffickers on the Darknet Results in 150 Arrests Worldwide and the Seizure of Weapons, Drugs, and over $31 Million," (Oct. 26, 2021), https://www.justice.gov/opa/pr/international-law-enforcement-operation-targeting-opioid-traffickers-darknet-results-150.

59 United Nations Office on Drugs and Crime (UNODC), *World Drug Report*, (Jun. 2021), https://www.unodc.org/res/wdr2021/field/WDR21_Booklet_2.pdf, p.76.

60 DEA, "Drug Fact Sheet," (April 2020), https://www.dea.gov/sites/default/files/2020-06/Narcotics-2020.pdf.

61 CDC, "Commonly Used Terms," https://www.cdc.gov/opioids/basics/terms.html.

62 CDC, "Drug Overdose Deaths in the U.S. Top 100,000 Annually," (November 2021), https://www.cdc.gov/nchs/pressroom/nchs_press_releases/2021/20211117.htm.

overdose deaths.[63]

The COVID-19 pandemic did not appear to significantly disrupt the use of illicit fentanyl in the United States, which the National Drug Threat Assessment (NDTA) has ascribed to the small number of pills needed to generate high revenue and to induce the intended effect in users.[64] While direct shipments of fentanyl from China to the United States have decreased substantially since China began controlling all forms of fentanyl as a class of drugs in 2019, Chinese companies and individuals continue to export precursor chemicals to Mexico for use by DTOs there to manufacture fentanyl before it is shipped to the United States. Labs and pill presses are present throughout Mexico, and cartels traffic their finished product to the United States alongside other drugs like heroin and cocaine. These DTOs are prioritizing building indigenous production capacities to reduce their reliance on foreign-sourced precursor chemicals.

While fentanyl's availability has risen in many parts of the United States, heroin, which is primarily sourced from Mexico, also continues to be readily available. Seizure data shows that the southwest border area of the United States remains a critical entry point for heroin from Mexico. The markets for fentanyl and heroin are substantially intertwined, as distributors often lace heroin with fentanyl to increase their profits while maintaining the potency of their product.

In addition to the illicit trafficking of fentanyl by DTOs, there have been numerous cases of medical professionals, such as doctors and pharmacists, prescribing or filling prescriptions for opioid painkillers even though their patients had no medical need for them.[65] While many complicit professionals took cash fees up front to arrange for these prescriptions, others adopted more sophisticated money laundering techniques, including the use of shell companies to hide the proceeds from law enforcement scrutiny.[66] In 2019, FinCEN issued an advisory to financial institutions that describes the schemes and methods that illicit actors use to conceal financial flows related to the trafficking of fentanyl and other synthetic opioids.[67]

### *b) Cocaine*

Cocaine, produced almost entirely in Latin America (particularly Bolivia, Colombia, and Peru) and trafficked through Mexico, continues to maintain a significant share of the U.S. drug market and remains one of the primary drugs that DTOs export to this country. Colombian and Mexican DTOs control the supply chain of cocaine, with Mexican DTOs controlling distribution within the United States.[68]

### *c) Methamphetamine*

According to the DEA, the pandemic did not significantly disrupt methamphetamine production, and high purity methamphetamine remains prevalent throughout the United States. As with many other illicit drugs, the southwest border area remains the principal transport point for methamphetamine produced in Mexico at scale

63 CDC, "Drug Overdose Deaths," https://www.cdc.gov/drugoverdose/deaths/index.html.

64 DEA NDTA.

65 DOJ, "CEO Sentenced to Prison in $150 Million Health Care Fraud, Opioid Distribution, and Money Laundering Scheme," (Mar. 3, 2021), https://www.justice.gov/opa/pr/ceo-sentenced-prison-150-million-health-care-fraud-opioid-distribution-and-money-laundering.

66 DEA, "Cumberland County man admits conspiring to distribute opioids, launder millions of dollars in drug proceeds," (Dec. 15, 2020), https://www.dea.gov/press-releases/2020/12/15/cumberland-county-man-admits-conspiring-distribute-opioids-launder.

67 FinCEN, "Advisory to Financial Institutions on Illicit Financial Schemes and Methods Related to the Trafficking of Fentanyl and Other Synthetic Opioids." (Aug. 21, 2019), https://www.fincen.gov/sites/default/files/advisory/2019-08-21/Fentanyl%20Advisory%20FINAL%20508.pdf.

68 DEA NDTA, p. 33.

for the U.S. market. As with the illicit production of fentanyl, DTOs have adapted to restrictions on the availability of precursor chemicals (in this instance, put in place by the Mexican government) by importing them from other countries, including China and India.

*d) Marijuana*

As referenced in the 2018 NMLRA, marijuana continues to be the most widely consumed illicit drug in the United States. While it remains illegal under federal law, U.S. states are expanding a trend of decriminalizing possession and consumption, or in some cases making whole categories of marijuana-related products legal to sell under state law. While Mexico remains the largest source of imported marijuana according to the DEA, its market share has steadily eroded as domestic production, which occurs in all 50 states, has increased.[69]

## 2. Priority DTO Threat Actors

According to the 2021 Annual Threat Assessment of the U.S. Intelligence Community, sophisticated DTOs were able to adapt to the disruptions brought on by the COVID-19 pandemic.[70] In its 2020 NDTA, the DEA similarly concluded that, despite fluctuations in pricing and disruptions to distribution methods arising from travel restrictions and depressed economic activity, DTOs were able to continue the majority of their operations.[71]

The Sinaloa Cartel and the Cártel Jalisco Nueva Generación (CJNG) are the two largest and most sophisticated DTOs, controlling transportation and distribution routes throughout Mexico and the United States, although multiple Mexican DTOs maintain a significant presence in the United States.[72] In addition to their traditional control of heroin, cocaine, and marijuana trafficking, Mexican DTOs have embraced the growing fentanyl market.

Mexican DTOs use a variety of money laundering methods, including BCS, misuse of MSBs and banks, and TBML. Of the major money laundering methods, COVID-19 may have temporarily affected BCS and TBML the most, as decreased traffic across the border generated larger seizures of cash or products tied to DTO activity.[73]

In November 2020,[74] the DEA and HSI arrested three Mexican nationals associated with the Sinaloa Cartel and seized $3.5 million, 685 kilograms of cocaine, and 24 kilograms of fentanyl at a truck yard in the border crossing of Otay Mesa, California. The DEA believes it to be one of the largest seizures of cash, narcotics, and ammunition ever in southern California. It was part of a five-year OCDETF investigation into the Sinaloa Cartel's operations in the region, which resulted in the seizure of over $27 million in narcotics proceeds.

Laundering through cross-border wire transfers remains a popular method for Mexican DTOs as well. In February 2021,[75] for example, the former owner and operator of a Virginia business used to launder more than $4.3 million in profits for CJNG was sentenced to 96 months in federal prison. The woman owned and operated a market that

69 DEA NDTA, p. 47.

70 Office of the Director of National Intelligence, *Annual Threat Assessment of the U.S. Intelligence Community*, (Apr. 9, 2021), https://www.dni.gov/files/ODNI/documents/assessments/ATA-2021-Unclassified-Report.pdf.

71 DEA NDTA.

72 The DEA's NDTA identifies nine Mexican DTOs as having the greatest drug trafficking impact on the United States. The remaining seven are Beltran-Leyva Organization, Cartel del Noreste and Los Zetas, Guerreros Unidos, Gulf Cartel, Juarez Cartel and La Linea, La Familia Michoacana, and Los Rojos.

73 See Cash Section in the Vulnerabilities Section of the report for a description of smuggling trends related to the pandemic.

74 DEA, "Agents Seize $3.5 Million in U.S. Currency and Massive Quantities of Cocaine, Fentanyl, and .50 Caliber Ammunition in Otay Mesa," (Nov. 24, 2020), https://www.dea.gov/press-releases/2020/11/24/agents-seize-35-million-us-currency-and-massive-quantities-cocaine.

75 DOJ, "Cartel Money Launderer Sentenced to 96 Months in Federal Prison," (Feb. 10, 2021), https://www.justice.gov/usao-wdva/pr/cartel-money-launderer-sentenced-96-months-federal-prison.

contracted with Intermex Wire Transfer, LLC, the leading provider of money transfer services in Latin America. She admitted that from 2016 through 2018, she used the business to launder the drug trafficking proceeds on behalf of CJNG. Her role was to receive U.S. currency, which she knew was drug trafficking proceeds and derived from a criminal offense, from multiple individuals working for the CJNG. She then wired that money to individuals in Mexico. The defendant conducted wire transfers in small amounts and falsified and fabricated the names and addresses of the senders in order to conceal the nature, location, source, ownership, and control of the funds.

## Cybercrime

Incidents of cybercrime[76] have significantly increased since the 2018 NMLRA, particularly as cybercriminals and malicious foreign state actors have taken advantage of the COVID-19 pandemic through phishing schemes and exploitation of remote applications to conduct ransomware attacks and BEC fraud. Other cybercriminal groups have deployed malware to harvest data, which they have monetized through online marketplaces or direct exploitation. Cybercrime presents a significant illicit finance threat: The size, reach, speed, and accessibility of the U.S. financial system make U.S. financial institutions attractive targets to traditional criminals, cybercriminals, terrorists, and foreign state actors. Among other critical infrastructure targets, these actors target financial institutions' websites, systems, and employees to steal customer and commercial credentials and proprietary information, defraud institutions and their customers, and disrupt business functions.[77]

The FBI's IC3 in 2020 received 791,790 complaints from the public citing suspected criminal activity facilitated by the internet, representing an increase of more than 69 percent from the previous year.[78] Self-reported losses exceeded $4.1 billion, although complaints received by IC3 are likely only a fraction of the cybercrime occurring in the United States. Law enforcement and supervisory assessments, as well as reports from financial institutions, confirm the assessment that cybercrime is a larger and growing share of the overall money laundering threat in the United States. Ransomware attacks, in particular, have seen significant growth in scale and sophistication over the past few years.

### 1. Ransomware

The severity and sophistication of ransomware attacks[79] have risen throughout the pandemic. Ransomware is a national security priority and an area of significant concern to the U.S. government in terms of potential loss of life, financial impact, and critical infrastructure vulnerability.[80]

FinCEN analysis of suspicious activity report (SAR) data found a 42 percent increase in ransomware-related SARs in the first six months of 2021 compared to all of 2020. Ransomware actors have increasingly targeted larger enterprises to demand larger payouts,[81] with the median average ransomware-related payment amount based on SAR analysis of $100,000; the majority of payments from the same analysis were under $250,000.[82]

76 Cybercrime is identified as a national AML/CFT priority.

77 FinCEN, *AML/CFT Priorities*.

78 FBI, IC3, *2020 Internet Crime Annual Report*, https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf.

79 A ransomware attack occurs when a specific type of malware encrypts data on a victim's systems in the interest of extorting a ransom payment from victims in exchange for decrypting the information and returning access to systems.

80 Treasury, "Treasury Continues Campaign to Combat Ransomware As Part of Whole-of-Government Effort," (Oct. 15, 2021), https://home.treasury.gov/news/press-releases/jy0410; DOJ, "U.S. Government Launches First One-Stop Ransomware Resource at StopRansomware.gov," (Jul. 15, 2021), https://www.justice.gov/opa/pr/us-government-launches-first-one-stop-ransomware-resource-stopransomwaregov.

81 DOJ, "Department of Justice Seizes $2.3 Million in Cryptocurrency Paid to the Ransomware Extortionists Darkside," (Jun. 7, 2021), https://www.justice.gov/opa/pr/department-justice-seizes-23-million-cryptocurrency-paid-ransomware-extortionists-darkside.

82 FinCEN, *Ransomware Trends in Bank Secrecy Act Data Between January 2021 and June 2021*, (October 2021), https://www.fincen.gov/sites/default/files/2021-10/Financial%20Trend%20Analysis_Ransomware%20508%20FINAL.pdf.

Cybercriminals often use remote desktop protocol endpoints and phishing campaigns to harvest credentials or otherwise gain access to a victim's computer network. Ransomware actors have also shared resources, such as exploit kits,[83] or formed partnerships with other cybercriminals to enhance the effectiveness of their attacks. Some ransomware developers sell access to their malware to affiliates in a "ransomware-as-a-service" model,[84] thereby decreasing the barrier to entry and level of technical expertise required to conduct ransomware attacks. In addition, ransomware actors increasingly employ double extortion tactics, where criminals steal confidential data before encrypting it and threaten to publish the data if the victim does not pay the ransom.

During the pandemic, attacks on small municipalities[85] and healthcare institutions have become more common, likely based on an expectation that the need to resume operations, in particular during a pandemic, may make hospitals more likely to pay a ransom. Criminals often require ransomware-related extortion payments to be made in virtual assets, frequently in bitcoin.[86] FinCEN SAR analysis indicates that some ransomware actors have demanded payment in anonymity-enhanced cryptocurrencies (AECs), requiring an additional fee for payment in bitcoin or only accepting payment in bitcoin after negotiation. SAR data also indicates that virtual wallets associated with top ransomware variants most commonly send funds to virtual asset service providers (VASPs), in particular exchanges.[87] The same data indicates that threat actors use foreign virtual asset service providers for ransomware-related deposits, which frequently have weak or nonexistent AML/CFT controls, before the perpetrator launders and cashes out the funds. To further obfuscate the laundering of ransomware proceeds, threat actors avoid using the same wallet addresses and use chain hopping,[88] mixing services,[89] and decentralized exchanges.[90]

The U.S. government continues to strongly discourage the payment of cyber ransom or extortion demands, which can be used to finance future attacks or other illicit activity. In some cases, the attackers simply refuse to honor the payment and the victim is unable to restore data and operations. Timely victim notification to and coordination with U.S. government agencies, including law enforcement, have proven instrumental in identifying and disrupting ransomware networks.

Ransomware attacks also frequently stem from jurisdictions with elevated sanctions risk. Notably a number of ransomware networks have been linked to sanctioned groups or jurisdictions with high sanctions risks, including

83 Exploit kits are toolkits that automate the identification and exploitation of client-side vulnerabilities.

84 *Ransomware-as-a-service* refers to a business model in which ransomware developers sell or otherwise deliver ransomware software to individuals or groups that have separately gained illicit access to the victim network often in exchange for a percentage of any ransom paid by the victim. See FinCEN, "Advisory on Ransomware and the Use of the Financial System to Facilitate Ransom Payments," (Nov. 8, 2021), https://www.fincen.gov/sites/default/files/2021-11/FinCEN Ransomware Advisory_FINAL_508_.pdf.

85 The White House, "Readout of Deputy National Security Advisor for Cyber Anne Neuberger Meeting with the Bipartisan National Association of Attorneys General," (Jun. 11, 2021), https://www.whitehouse.gov/briefing-room/statements-releases/2021/06/11/readout-of-deputy-national-security-advisor-for-cyber-anne-neuberger-meeting-with-the-bipartisan-national-association-of-attorneys-general/.

86 FinCEN, "Advisory on Ransomware."

87 FinCEN, *Ransomware Trends*.

88 Chain hopping refers to the practice of converting one virtual asset into a different virtual asset at least once before moving the funds to another service or platform.

89 *Mixers* are websites or software designed to conceal or obfuscate the source or owner of virtual assets.

90 FinCEN, *Ransomware Trends*.

Russia,[91] Democratic People's Republic of Korea,[92] and Iran.[93] For example, in December 2019, OFAC designated Evil Corp, the Russia-based cybercriminal organization responsible for the development and distribution of the Dridex malware, as well as core cyber operators, multiple businesses associated with a group member, and financial facilitators used by the group.[94] Ransomware payments may therefore not only fund activities that harm U.S. national security but also risk violating OFAC regulations.[95] OFAC considers victims' notification to and coordination with the government to be a "mitigating factor" in enforcement actions associated with ransomware payments.

TCOs are often the perpetrators of ransomware crimes, leveraging global infrastructure and money laundering networks to carry out their attacks. The U.S. government is pursuing a focused, integrated effort to counter ransomware, including working with the private sector to modernize their cyber defenses and with international partners to address the global nature of the threat.[96] For example, in January 2021, the DOJ and international law enforcement partners coordinated global action to disrupt a sophisticated form of ransomware known as NetWalker.[97] The action included charges against a Canadian national in relation to NetWalker ransomware attacks in which tens of millions of dollars were allegedly obtained, the seizure of approximately $454,530 in virtual assets from ransom payments, and the disablement of a darknet hidden service used to communicate with NetWalker ransomware victims.

Additionally, in November 2021, the DOJ announced that it had charged a Ukrainian national and a Russian national with accessing internal computer networks of several victim companies and deploying ransomware. The DOJ also seized $6.1 million in funds traceable to alleged ransom payments received by one of the individuals. In parallel with the arrest of the Ukrainian national in Poland, interviews and searches were carried out in multiple countries.[98] OFAC also designated the two individuals for their part in perpetuating ransomware incidents against the United States.[99] Simultaneously, OFAC designated a virtual asset service provider (VASP),[100] and its associated support network, for facilitating financial transactions for ransomware actors, an action which built upon OFAC's first sanctions designation of a VASP in September 2021. Latvia and Estonia also took action against the VASP and its associated support network.

---

91 DOJ, "Six Russian GRU Officers Charged in Connection with Worldwide Deployment of Destructive Malware and Other Disruptive Actions in Cyberspace," (Oct. 19, 2020), https://www.justice.gov/opa/pr/six-russian-gru-officers-charged-connection-worldwide-deployment-destructive-malware-and.

92 DOJ, "3 North Korean Military Hackers Indicted in Wide-Ranging Scheme to Commit Cyberattacks and Financial Crimes Across the Globe," (Feb. 17, 2021), https://www.justice.gov/usao-cdca/pr/3-north-korean-military-hackers-indicted-wide-ranging-scheme-commit-cyberattacks-and.

93 DOJ, "Two Iranian Men Indicted for Deploying Ransomware to Extort Hospitals, Municipalities, and Public Institutions, Causing Over $30 Million in Losses," (Nov. 28, 2018), https://www.justice.gov/opa/pr/two-iranian-men-indicted-deploying-ransomware-extort-hospitals-municipalities-and-public.

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

95 OFAC, "Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments," (Oct. 1, 2020), https://home.treasury.gov/system/files/126/ofac_ransomware_advisory_10012020_1.pdf.

96 The White House, "FACT SHEET: Ongoing Public U.S. Efforts to Counter Ransomware," (Oct. 13, 2021), https://www.whitehouse.gov/briefing-room/statements-releases/2021/10/13/fact-sheet-ongoing-public-u-s-efforts-to-counter-ransomware/.

97 DOJ, "Department of Justice Launches Global Action Against NetWalker Ransomware," (Jan. 27, 2021), https://www.justice.gov/opa/pr/department-justice-launches-global-action-against-netwalker-ransomware.

98 DOJ, "Ukrainian Arrested and Charged with Ransomware Attack on Kaseya," (Nov. 8, 2021), https://www.justice.gov/opa/pr/ukrainian-arrested-and-charged-ransomware-attack-kaseya.

99 Treasury, "Treasury Continues Campaign to Combat Ransomware As Part of Whole-of-Government Effort," (Oct. 15, 2021), https://home.treasury.gov/news/press-releases/jy0410.

100 See Section II. C. on Virtual Assets for a fuller description of the term VASP and how it is used in this report.

## 2. Business Email Compromise

BEC schemes, which are considered cyber-enabled fraud, accounted for $1.8 billion in losses in 2020, over 40 percent of all victim losses from cybercrime for the year, according to IC3 estimates. Cybercriminals have increasingly exploited the COVID-19 pandemic by using BEC schemes, particularly targeting municipalities and the healthcare industry supply chain.[101] In addition, the FBI has witnessed a rise in BEC schemes targeting the real estate, entertainment, and commercial food sectors.[102] For example, remote closings for real estate were widespread during the pandemic, and BEC scammers can generate significant illicit proceeds when they convince those buying real estate to wire down payments to illegitimate accounts. The USSS recently reported intercepting a potential $21 million real estate BEC scheme and warns of a sharp rise in BEC incidents specific to the real estate sector.[103]

In BEC schemes, criminals use compromised or spoofed accounts, often those actually or purportedly belonging to company leadership, vendors, or lawyers, to target employees with access to a company's finances to induce them to transfer funds to bank accounts thought to belong to trusted partners. During the pandemic, criminals have exploited pandemic-related changes in business operations, the high demand for critical pandemic-related supplies, and remote work operations to convince victims to make payments.[104] Criminals have often made last-minute and urgent demands for a change in recipient account information and the timeline for payment. Additionally, IC3 observed an increase in schemes in which BEC criminals used stolen identities to set up bank accounts, into which they received funds from BEC schemes. The criminals then exchanged the funds into virtual assets.

## 3. Compromise and Sale of Financial Information

Some cybercriminal groups[105] develop and deploy malware to harvest and monetize financial data on an industrial scale from businesses around the world. Some groups use botnets, or networks of compromised computers that can include hundreds of devices, which they can command and control to launch attacks against a large number of computers at once to extract information, including banking passwords and login credentials.[106] Criminals can traffic the harvested data through marketplaces that specialize in the sale of compromised debit and credit cards, PII, financial and banking information, and other contraband. For example, the criminal organization FIN7 used malware and other tools to breach the computer networks of businesses in all 50 U.S. states in addition to international victims, stealing more than 20 million customer card records from over 6,500 individual point-of-sale

101 FBI, "FBI Anticipates Rise in Business Email Compromise Schemes Related to the COVID-19 Pandemic," (Apr. 6, 2020), https://www.fbi.gov/news/pressrel/press-releases/fbi-anticipates-rise-in-business-email-compromise-schemes-related-to-the-covid-19-pandemic; FinCEN, "FinCEN Advisory on Cybercrime and Cyber-Enabled Crime Exploiting the Coronavirus Disease 2019 (COVID-19) Pandemic," (Jul. 30, 2020), https://www.fincen.gov/resources/advisories/fincen-advisory-fin-2020-a005.

102 DOJ, "Two Defendants Posing as Booking Agents for Famous Entertainers Arrested for Fraudulent Scheme," (Jan. 9, 2020), https://www.justice.gov/usao-edny/pr/two-defendants-posing-booking-agents-famous-entertainers-arrested-fraudulent-scheme-0.

103 USSS, "U.S Secret Service Thwarts Loan Scam Totaling More Than $21 Million," (Sep. 1, 2021), https://www.secretservice.gov/newsroom/releases/2021/09/us-secret-service-thwarts-loan-scam-totaling-more-21-million.

104 FinCEN, FinCEN Updated Advisory on Email Compromise Fraud Schemes Targeting Vulnerable Business Processes," (Jul. 16, 2019), https://www.fincen.gov/resources/advisories/fincen-advisory-fin-2019-a005.

105 DOJ, "Russian National Pleads Guilty for Role in Transnational Cybercrime Organization Responsible for more than $568 Million in Losses," (Jun. 6, 2020), https://www.justice.gov/opa/pr/russian-national-pleads-guilty-role-transnational-cybercrime-organization-responsible-more.

106 DOJ, "Emotet Botnet Disrupted in International Cyber Operation," (Jan. 28, 2021), https://www.justice.gov/opa/pr/emotet-botnet-disrupted-international-cyber-operation.

terminals at more than 3,600 separate business locations.[107]

Criminals, like those associated with FIN7, can traffic harvested data through marketplaces that specialize in the sale of compromised debit and credit cards, PII, financial and banking information, and other contraband. Such marketplaces may be established by other cybercriminals using turnkey online storefront design and hosting platforms. For example, in May 2021, a Russian national was sentenced to months in custody for his role as the administrator of an online platform that catered to cyber criminals by virtually selling items such as stolen credit card information, other personal information, and services to be used for criminal activity. The platform as of March 2020 had approximately 3,000 shops with sales exceeding $17 million.[108] Purchasers of harvested data may attempt to use credentials and other PII to access victims' accounts at financial institutions to conduct unauthorized financial transactions, create synthetic identifies, or commit identity theft, among other crimes. Based on victim reports regarding one online marketplace disrupted through international law enforcement cooperation in June 2021, stolen login credentials sold over the marketplace were used to cause over $200 million in losses in the United States.[109]

## PROFESSIONAL MONEY LAUNDERING

The use of professional money laundering organizations (PMLOs), networks, and third-party money launderers has not abated since our previous risk assessments.[110] These groups are considered in the Threats section given that it is focused on criminal actors (e.g., money brokers). PMLOs, for example, have recently worked to launder funds on behalf of organized criminal enterprises operating in several countries around the world.[111] Many investigations have also demonstrated that each year PMLOs launder tens of millions of dollars on behalf of DTOs selling illegal narcotics throughout the United States. Some of these international PMLOs have focused on laundering the proceeds of cybercrime.[112] PMLOs carry out several activities, including conducting money pickups of drug proceeds in the United States, transporting the cash, depositing the money into the retail banking system, and/or transferring the money to different individuals or entities. PMLOs use casinos, front companies, foreign and domestic bank accounts, and BCS to launder money on behalf of transnational DTOs.[113]

---

107 DOJ, "High-level organizer of notorious hacking group FIN7 sentenced to ten years in prison for scheme that compromised tens of millions of debit and credit cards," (Apr. 16, 2021), https://www.justice.gov/usao-wdwa/pr/high-level-organizer-notorious-hacking-group-fin7-sentenced-ten-years-prison-scheme.

108 DOJ, "Russian Hacker Pleads Guilty to Administering a Website that Catered to Criminals," (Jan. 21, 2021), https://www.justice.gov/usao-sdca/pr/russian-hacker-pleads-guilty-administering-website-catered-criminals; DOJ, "Russian Hacker Sentenced to 30 Months for Running a Website Selling Stolen, Counterfeit, and Hacked Accounts," (May 24, 2021), https://www.justice.gov/usao-sdca/pr/russian-hacker-sentenced-30-months-running-website-selling-stolen-counterfeit-and.

109 DOJ, "Slipp Marketplace Disrupted in International Cyber Operation," (Jun. 10, 2021), https://www.justice.gov/opa/pr/slilpp-marketplace-disrupted-international-cyber-operation.

110 Professional money laundering can be placed in three categories: (1) individuals, (2) organized groups of people, and (3) networks of associates and contacts. See FATF, *Professional Money Laundering Report,* (2018), https://www.fatf-gafi.org/media/fatf/documents/Professional-Money-Laundering.pdf, pp.12-13.

111 DOJ, "Three Defendants Charged In Organized Crime Money Laundering Scheme," ( Jul. 14, 2021), https://www.justice.gov/usao-sdny/pr/three-defendants-charged-organized-crime-money-laundering-scheme.

112 DOJ, "Officials Announce International Operation Targeting Transnational Criminal Organization QQAAZZ that Provided Money Laundering Services to High-Level Cybercriminals," (Oct. 15, 2020), https://www.justice.gov/opa/pr/officials-announce-international-operation-targeting-transnational-criminal-organization; DOJ, "Foreign Nationals Sentenced for Roles in Transnational Cybercrime Enterprise, (Mar. 19, 2021), https://www.justice.gov/opa/pr/foreign-nationals-sentenced-roles-transnational-cybercrime-enterprise#:~:text=Two%20foreign%20nationals%20%E2%80%94%20one%20Russian,credit%20card%20data%2C%20computer%20malware%2C.

113 DOJ, "Three Members of Transnational Money Laundering Network Pleaded Guilty to Aiding Foreign Drug Trafficking Organizations," (Apr. 14, 2021), https://www.justice.gov/usao-edva/pr/three-members-transnational-money-laundering-network-pleaded-guilty-aiding-foreign-drug.

Criminal groups and TCOs have offered professional money laundering services through online advertisements. For example, in 2020 and 2021, 14 members of the Infraud Organization were convicted of racketeering charges including money laundering offenses. Operating under the slogan "In Fraud We Trust," traders on international, members-only clear and darknet sites could engage in the large-scale sales of stolen identities, financial and banking information, and computer malware and post advertisements offering illegal money laundering services.[114]

Law enforcement has observed new trends with respect to PMLOs. For example, the FBI noted that these networks have co-opted unwitting and witting third parties (e.g., law firms, real estate agents, accountants, etc.) to bypass domestic regulatory AML/CFT controls and have used legal privilege as a method to hide illicit activity. A "special focus" on the increased use of CMLOs is included in this section.

## 1. Money Brokers

As discussed in the 2015 and 2018 NMLRAs, TBML is the process of disguising the origin of criminal proceeds through the import or export of merchandise and trade-related financial transactions. There are various TBML methods that can be employed by professional launderers to include the use of money brokers. Money (or peso) brokers are third parties that seek to purchase drug proceeds in the location where illicit proceeds are earned by drug cartels (e.g., Colombia, Mexico) at a discounted rate. Money brokers often employ many individuals responsible for collecting narcotics proceeds and disposing of those proceeds, as directed by either the DTO or the money brokers who serve as PMLOs.[115]

Money brokers often act as unregulated or "black market" money exchangers, using unwitting and complicit businesses to accept cash and move merchandise across international borders instead of cash.[116] These money brokers use contracts between different parties to facilitate the laundering process. Common customs fraud techniques such as over-and under-invoicing and the Black Market Peso Exchange (BMPE)[117] remain effective, and the increase in CMLOs continues to further compartmentalize and disguise this activity (see next section).

The main objective of the money broker is to evade foreign exchange restrictions. This enables DTOs with cash located in the United States to transfer the value of that cash to other countries, principally Colombia and Mexico (depending on the location of the DTO), without having to physically transport U.S. currency across an international border. Furthermore, the use of a money broker allows all the participants to receive funds in their own currencies. In a traditional TBML model, dollars in the U.S. are sold by the DTO and paid for in Colombia or Mexico by the money broker to the DTO. Dollars are purchased in Colombia or Mexico by the Colombian/Mexican Importer, paid for in Colombia or Mexico to the money broker, and remitted in the United States by the money broker.

To effectuate these schemes, money brokers, operating primarily in Colombia or Mexico, facilitate both the pickup of bulk cash drug proceeds from couriers located throughout the United States and the receipt of incoming wire

114 See *United States v. Bondarenko*, 2019 WL 2450923 (D. Nev. 2019); *United States v. Chiochiu*, 2019 WL 3307546 (D. Nev. 2019).

115 FATF, *Professional Money Laundering*, (July 2018), https://www.fatf-gafi.org/media/fatf/documents/Professional-Money-Laundering.pdf, p. 30.

116 DOJ, "Los Angeles Fashion District Company Owner Sentenced to One Year in Prison for Committing Customs Violations and Tax Offenses," (Dec. 6, 2021), https://www.justice.gov/usao-cdca/pr/los-angeles-fashion-district-company-owner-sentenced-one-year-prison-committing-customs.

117 See 2015 and 2018 NMLRA for further detail about BMPE schemes, available at https://www.treasury.gov/resource-center/terrorist-illicit-finance/Documents/National%20Money%20Laundering%20Risk%20Assessment%20%E2%80%93%2006-12-2015.pdf and https://home.treasury.gov/system/files/136/2018NMLRA_12-18.pdf.

transfers (e.g., from U.S. funnel accounts).[118] Typically, as part of these schemes, the funds collected in the United States pursuant to contracts offered by money brokers are deposited in bank accounts located in the United States and then transferred to the bank account of the U.S-based exporter (e.g., electronics). Upon receiving confirmation that funds collected pursuant to a money broker contract are available for deposit into the bank account of the U.S. exporter, the business will arrange for the export of a roughly equivalent value of consumer electronics products to certain consumer product suppliers located in Colombia or Mexico. These suppliers, in turn, arranged to pay for the products by delivering pesos to an individual in Colombia or Mexico, who then delivered those funds to the money brokers.[119] To settle the imbalance that would otherwise accrue with a peso outflow and U.S. dollar inflow, a combination of money mules (often the courier) and complicit merchants are used to obtain goods for export, such as electronics from Colombia or Mexico. There are also examples of merchants who are unwitting participants in these schemes and are merely wholesalers enlisted by brokers, sometimes on a one-off basis, for a shipment abroad.

## 2. Special Focus: Chinese Money Laundering Organizations

Law enforcement is seeing an increase in DTOs' use of CMLOs seeking to repatriate funds outside the United States.[120] CMLO schemes use "underground banking" or "black market foreign exchange" to facilitate the exchange of foreign currency.[121] These methods can be described as a black market foreign exchange that relies on basic principles of supply and demand of currency and matches individuals that have a supply of U.S. dollars with those in the market that have a demand for U.S. dollars. In some cases, CMLOs also take advantage of the traditional TBML techniques. What makes CMLOs unique is their ability to offer services at lower fees than traditional money brokers, to exploit Chinese currency controls, and to use communication technology effectively. These organizations are often compartmentalized, and they disguise themselves behind legitimate business activity to reduce their risk of exposure.[122] CMLOs will also provide insurance against losses, in that they will still pay out even if the funds are lost due to theft or interdiction by law enforcement. These money laundering schemes are designed to remedy two separate problems: DTOs' desire to repatriate drug proceeds into the Mexican banking system and wealthy Chinese nationals restricted by China's capital flight laws from transferring large sums of money held in Chinese bank accounts for use abroad.[123] In order to address these problems, CMLOs seek out U.S. dollars held by Mexican DTOs as a means to supply their ultimate customers.

---

118 FinCEN, "Update on U.S. Currency Restrictions in Mexico: Funnel Accounts and TBML," (May 28, 2014), https://www.fincen.gov/sites/default/files/advisory/FIN-2014-A005.pdf.

119 DOJ, "6 Colombian Nationals And Owner Of Consumer Electronics Business Charged For Their Roles In Money Laundering And Unlicensed Money Transmission Business Offenses," (Jan. 17, 2020), https://www.justice.gov/usao-sdny/pr/6-colombian-nationals-and-owner-consumer-electronics-business-charged-their-roles-money.

120 DOJ, "United States Unseals Superseding Indictment Charging Nationwide Money Laundering Network," (Oct. 15, 2020), https://www.justice.gov/usao-edva/pr/united-states-unseals-superseding-indictment-charging-nationwide-money-laundering; DOJ, "7 Defendants In Nationwide Money Laundering Organization Charged For Laundering Over $28 Million For Drug Trafficking Organizations," (Jul. 21, 2021), https://www.justice.gov/usao-sdny/pr/7-defendants-nationwide-money-laundering-organization-charged-laundering-over-28.

121 DOJ, "Owners of Underground, International Financial Institutions Sentenced for Operating Unlicensed Money Transmitting Business," (Jun. 3, 2021), https://www.justice.gov/usao-sdca/pr/owners-underground-international-financial-institutions-sentenced-operating-unlicensed.

122 DOJ, "Chinese National Sentenced to 14 Years in Prison for Laundering Drug Proceeds on Behalf of Traffickers in Mexico," (Apr. 27, 2021), https://www.justice.gov/usao-ndil/pr/chinese-national-sentenced-14-years-prison-laundering-drug-proceeds-behalf-traffickers.

123 DOJ, "Three Indicted for International Money Laundering Scheme Pairing Mexican Drug Traffickers and Chinese Nationals," (Oct. 18, 2019), https://www.justice.gov/usao-or/pr/three-indicted-international-money-laundering-scheme-pairing-mexican-drug-traffickers-and.

CMLO schemes generally begin via a contract with a DTO and a CMLO negotiating a price for bringing U.S. drug proceeds back to the DTO's point of origin. These agreements have taken place between CMLO heads and foreign-based TCO leaders in countries such as Mexico, Colombia, China, and the United States. For example, a Mexican DTO will coordinate the delivery of bulk U.S. dollars through couriers in the United States to a Chinese money broker in the United States. Once the drug cash proceeds are received by the money broker in the United States, the money broker in Mexico pays the Mexican DTO in pesos.

According to open-source reporting, information provided by law enforcement and court records, the WeChat messaging application (which offers end-to-end encryption) appears to be a key method used to communicate the transfer of funds among various participants in the scheme. Chinese money brokers transfer the drug proceeds in U.S. dollars to a processor in the United States. The processor is responsible for advertising and selling the bulk U.S. dollars to Chinese nationals in the United States. The processor identifies customers by posting advertisements on internet bulletin boards or private WeChat forums online. The processor then sells the bulk U.S. dollars in exchange for mobile China-to-China bank transfers to Chinese bank accounts controlled by the CMLO.[124]

Chinese customers in the United States who purchase the bulk U.S. dollars from the processor in the United States then use the U.S. dollars to purchase assets and support their lifestyle in the United States, which Chinese capital flight restrictions would otherwise limit. With the Chinese currency that it has received, the CMLO may sell to either Mexican importers or Chinese expatriates who have a business in Mexico and want to repatriate their profit. Those goods are then sold at retail in Mexico for pesos and the broker in Mexico receives the funds to complete the money laundering cycle.

The example below demonstrates CMLOs' involvement in illegal money transmitting businesses. In this case, a CMLO accepted cash from various third parties in the United States and delivered that cash to a customer, typically a high-roller gambler from China who could not readily access cash in the United States due to capital controls. Members of the CMLO were introduced to customers by casino hosts, who sought to increase the gambling play of the casino's customers. By connecting cash-starved gamblers in the United States with illicit money transmitting businesses, like those operated by CMLOs, casinos increased the domestic cash play of their China-based customers. All a gambler needed to obtain funds was a mobile device with remote access to a China-based bank account. As a result, CMLOs transmitted and converted electronic funds in China into hard currency in the United States, all while circumventing the obstacles imposed both by China's capital controls and the AML/CFT scrutiny imposed on U.S. financial institutions and casinos. According to public reporting, the casino hosts often received a cut of the CMLOs' commission.[125] The FBI has also noted the sale of cash by CMLOs to Chinese university students who then use the cash to pay their tuitions.

## CORRUPTION[126]

Corruption takes on many forms and is used to further various illicit behaviors. Types of corruption include grand corruption, administrative corruption, kleptocracy, state capture, and strategic corruption.[127] Public corruption within the United States involves the corruption of local, state, and federal government officials. The proceeds of

124 See United States District Court (USDC), District of Oregon, U.S. v. SHEFENG SU, Case 3:19-cr-00190-MO; See also USDC, Eastern District of Virginia, U.S. V. XIZHI LI, Case 1:19-cr-00334, https://www.justice.gov/opa/press-release/file/1328016/download.

125 DOJ, "Owners of Underground, International Financial Institutions Pleaded Guilty to Operating Unlicensed Money Transmitting Business," (Feb. 3, 2020), https://www.justice.gov/usao-sdca/pr/owners-underground-international-financial-institutions-plead-guilty-operating.

126 Corruption is a national AML/CFT priority.

127 The White House, "United States Strategy on Countering Corruption," (December 2021), https://www.whitehouse.gov/wp-content/uploads/2021/12/United-States-Strategy-on-Countering-Corruption.pdf, see illustrative types of corruption, p. 6.

foreign corruption affect the United States when foreign corrupt officials seek to invest their illicit proceeds in or through the U.S. economy and markets. These crimes are generally committed for private gain and often rely on money laundering to conceal or hide the source and ownership of the illicit proceeds. Common money laundering methods rely on opaque foreign financial systems and the misuse of professional service providers, nominees, and legal entities and other corporate vehicles, including anonymous shell companies, and limited liability companies.[128]

Corruption can prevent citizens at home and abroad from receiving what they are due, from relief payments to social services. It can manifest as citizens, especially the wealthy, evade payments they owe, including tax obligations and other fees. Corruption is major impediment to economic fairness and growth in many countries and a detriment to good governance.

The 2015 and 2018 NMLRAs identified corruption as a priority money laundering threat and President Joseph Biden in December 2021 signaled a redoubled emphasis on anti-corruption as a national security priority via the issuance of a U.S. Strategy on Countering Corruption, which includes curbing illicit finance as one of its key pillars.[129]

## 1. Foreign Corruption

The United States uses a number of legal authorities to combat foreign corruption. The Foreign Corrupt Practices Act (FCPA),[130] among other things, makes it unlawful for certain classes of persons and entities to offer or pay money or anything of value to foreign government officials in order to obtain or retain business.

In addition, the DOJ regularly prosecutes schemes involving money laundering that may involve proceeds of crimes under foreign law, such as foreign laws against bribery, misappropriation, and embezzlement of public funds by or for the benefit of a public official. In these and other types of cases, the DOJ may consider prosecuting corruption based on various types of fraudulent activity and associated violations, including foreign or domestic bank fraud, failure to disclose foreign bank accounts, and other disclosure obligations. The DOJ also uses criminal and civil forfeiture, where possible and appropriate, to forfeit proceeds of corruption involving money laundering and other offenses. The DOJ's Kleptocracy Asset Recovery Initiative focuses on investigation and litigation to recover the proceeds of foreign official corruption in the United States, or which used the U.S. financial system. As of 2021, the DOJ's Kleptocracy Asset Recovery Initiative had recovered and assisted in recovering and repatriating approximately $1.7 billion in assets and had an additional approximately $2.2 billion in assets restrained pending forfeiture litigation and forfeited pending return negotiations.

Many of the foreign corruption cases involve the assistance of agencies such as the Securities and Exchange Commission (SEC) and the Commodity Futures Trading Commission (CFTC), as well as parallel civil investigations and enforcement actions.[131] Given the FCPA's prohibitions on the payment of bribes by publicly traded companies and their affiliates to foreign officials to assist in obtaining or retaining business, the enforcement of this legislation continues to be a high priority area for the SEC. In 2010, the SEC's Enforcement Division created a specialized

128 The White House, "Memorandum on Establishing the Fight Against Corruption as a Core United States National Security Interest, (Jun. 2, 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/.

129 The White House, "Fact Sheet: U.S. Strategy on Countering Corruption," (Dec. 6, 2021), https://www.whitehouse.gov/briefing-room/statements-releases/2021/12/06/fact-sheet-u-s-strategy-on-countering-corruption/.

130 15 U.S.C. §§ 78dd-1, et seq.

131 DOJ and SEC, *A Resource Guide to the U.S. Foreign Corrupt Practices Act, Second Edition.* (July 2020), https://www.justice.gov/criminal-fraud/file/1306671/download.

unit[132] to further enhance its enforcement of the FCPA. Several recent DOJ and SEC enforcement actions demonstrate the enormous scope and magnitude of this threat.[133]

Proceeds from corruption cases can often be difficult to detect, as bad actors may use front and shell companies to pay or otherwise influence individuals and entities engaging in financial activity that is not necessarily discernible as illicit. Front and shell companies also mask the identities of those profiting from kickbacks, fraud, embezzlement, and bribery, sometimes making it difficult for law enforcement to identify the ultimate beneficial owners.[134] Complicit businesses that provide financial services may also play a role in concealing, profiting from, and moving corruption proceeds.[135] As a result, kleptocrats are able to integrate the proceeds into tangible property, real estate, investments, and other assets.[136]

The term politically exposed person (PEP) is commonly used in the financial industry to refer to foreign individuals who are or have been entrusted with a prominent public function, as well as to their immediate family members and close associates.[137] By virtue of their public position or relationships, some PEPs may have access to funds that may be the proceeds of corruption or other illicit activity; PEPs thus may present a risk higher than other customers. Some PEPs have used banks as conduits for their illegal activities, including corruption, bribery, money laundering/terrorist financing (ML/TF), and other illicit financial activity.[138]

## 2. Domestic Corruption

Prosecutable domestic corruption often involves money laundering activity as individuals seek to disguise bribes paid to and received by corrupt officials. DOJ's Public Integrity Section handles federal cases involving embezzlement, bribery, and related crimes. Like foreign corruption activity, domestic corruption often involves other crimes, ranging from tax evasion to contracting fraud.[139] Recent domestic corruption cases have also

132 SEC, "SEC Names New Specialized Unit Chiefs and Head of New Office of Market Intelligence," (Jan. 13, 2010), https://www.sec.gov/news/press/2010/2010-5.htm.

133 DOJ, "Businessman Sentenced for Foreign Bribery and Money Laundering Scheme Involving PetroEcuador Officials," (Jan. 28, 2021), https://www.justice.gov/opa/pr/businessman-sentenced-foreign-bribery-and-money-laundering-scheme-involving-petroecuador; DOJ, "Vitol Inc. Agrees to Pay over $135 Million to Resolve Foreign Bribery Case," (Dec. 03, 2020), https://www.justice.gov/opa/pr/vitol-inc-agrees-pay-over-135-million-resolve-foreign-bribery-case. See also "SEC Enforcement Actions: FCPA Cases," https://www.justice.gov/opa/pr/justice-department-seeks-forfeiture-third-commercial-property-purchased-funds-misappropriated.

134 DOJ, "Justice Department Seeks Forfeiture of Third Commercial Property Purchased with Funds Misappropriated from PrivatBank in Ukraine," (Dec. 30, 2020), https://www.justice.gov/opa/pr/justice-department-seeks-forfeiture-third-commercial-property-purchased-funds-misappropriated.

135 DOJ, "Two Individuals Indicted for Money Laundering Related to Odebrecht Bribery and Fraud Scheme," (May 25, 2021), https://www.justice.gov/usao-edny/pr/two-individuals-indicted-money-laundering-related-odebrecht-bribery-and-fraud-scheme.

136 DOJ, "Over $1 Billion in Misappropriated 1MDB Funds Now Repatriated to Malaysia," (Aug. 5, 2021), https://www.justice.gov/opa/pr/over-1-billion-misappropriated-1mdb-funds-now-repatriated-malaysia.

137 See "Joint Statement on Bank Secrecy Act Due Diligence Requirements for Customers Who May Be Considered Politically Exposed Persons," (Aug. 21, 2020) issued by the federal banking agencies (Federal Reserve, https://www.federalreserve.gov/supervisionreg/srletters/SR2021.htm; FDIC, https://www.fdic.gov/news/financial-institution-letters/2020/fil20078.html; NCUA, https://www.ncua.gov/newsroom/press-release/2020/agencies-issue-statement-bank-secrecy-act-due-diligence-requirements-customers-who-may-be-considered-peps/joint-statement; OCC, https://www.occ.treas.gov/news-issuances/bulletins/2020/bulletin-2020-77.html) and FinCEN, https://www.fincen.gov/news/news-releases/agencies-issue-statement-bank-secrecy-act-due-diligence-requirements-customers.

138 Federal Financial Institutions Examination Council (FFIEC), "Update to the BSA/AML Examination Manual, Politically Exposed Persons," (Dec. 1, 2021), https://www.ffiec.gov/press/PDF/Politically-Exposed-Persons.pdf.

139 DOJ, "San Francisco Public Official And Contractors Charged With Crimes Related To Public Corruption And Money

involved unlawful campaign contributions, as both U.S. and foreign individuals have sought to illegally influence elections within the United States. Like foreign corruption cases, such activity can be difficult to detect as perpetrators of domestic corruption seek to conceal their involvement by obfuscating their identity. In one 2019 case, a federal grand jury indicted several individuals for their part in an elaborate scheme to make unlawful political contributions to influence the U.S. political process.[140] In March 2020, an executive of a multinational insurance company and a consultant were convicted for public corruption and bribery charges pertaining to a scheme to covertly direct illegal campaign contributions to a candidate for public office at the state level in North Carolina in return for a favorable action regarding the insurance company by the candidate. According to evidence presented at trial, between April 2017 and August 2018, the executive and the consultant sought to funnel millions of dollars in campaign contributions and other things of value in exchange for the Commissioner of the North Carolina Department of Insurance's removal of the deputy commissioner, who was responsible for regulating the executive's company. To conceal this scheme, the schemers set up two corporate entities to form an independent expenditure committee to anonymously funnel $1.5 million in contributions to the commissioner's re-election campaign. Another individual, chairman of a North Carolina state political party, who was part of the scheme, transferred $250,000 of monies contributed to the state party to go toward the commissioner's re-election campaign.[141]

## HUMAN TRAFFICKING AND HUMAN SMUGGLING [142]

Human trafficking crimes generally involve compelling or coercing a person's labor, services, or commercial sex acts, or causing a minor to engage in commercial sex.[143] Human trafficking does not require the crossing of an international border and is a crime distinct from the crime of human smuggling. Human smugglers engage in the crime of bringing people across international borders through deliberate evasion of immigration laws, often for financial benefit.[144] While human trafficking and human smuggling are distinct crimes, individuals who are smuggled are vulnerable to becoming victims of human trafficking and other serious crimes. Both human trafficking and human smuggling networks pose a serious criminal threat with devastating consequences as criminal organizations value profit over human life.[145]

### 1. Human Trafficking

Human trafficking is a financially motivated crime that harms the safety and security of those trafficked throughout the United States and the world. It is a misconception that human trafficking requires crossing a

Laundering Scheme," (Jun. 10, 2020), https://www.justice.gov/usao-ndca/pr/san-francisco-public-official-and-contractors-charged-crimes-related-public-corruption; DOJ, "Former Baltimore Mayor Catherine Pugh Sentenced to Three Years in Federal Prison for Fraud Conspiracy and Tax Charges," (Feb. 27, 2020), https://www.justice.gov/usao-md/pr/former-baltimore-mayor-catherine-pugh-sentenced-three-years-federal-prison-fraud.

140 DOJ, *Report to Congress on the Activities and Operations of the Public Integrity Section*, (2019), https://www.justice.gov/criminal-pin/file/1346061/download, see pp.19-20, *United States v. Khawaja, et al*.

141 DOJ, "Federal Jury Convicts Founder and Chairman of a Multinational Investment Company and a Company Consultant of Public Corruption and Bribery Charges," (Mar. 5, 2020), https://www.justice.gov/opa/pr/federal-jury-convicts-founder-and-chairman-multinational-investment-company-and-company.

142 Human Trafficking and Human Smuggling are considered national AML/CFT priorities.

143 See 18 U.S.C. §§ 1581 – 1588. See also DOJ, Human Trafficking Prosecution Unit (HTPU), https://www.justice.gov/crt/human-trafficking-prosecution-unit-htpu.

144 See 8 U.S.C. § 1324. See also U.S. Department of State, "Human Trafficking and Migrant Smuggling: Understanding the Difference," (Jun. 27, 2017), https://www.state.gov/wp-content/uploads/2019/02/272325.pdf.

145 DOJ, "Attorney General memoranda on joint task force against human smuggling and trafficking networks," (Jun. 7, 2021), https://www.justice.gov/opa/press-release/file/1401991/download; DHS, "DHS Announces Operation to Target Criminal Smuggling Organizations," (Apr. 27, 2021), https://www.dhs.gov/news/2021/04/27/dhs-announces-operation-target-criminal-smuggling-organizations.

border.[146] 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. Human traffickers take advantage of poverty, conflict, natural disaster, breakdowns in the rule of law, dislocation, disruption of social support systems, and other global crises that can intensify victims' vulnerabilities to recruitment and exploitation. Corrupt government officials also enable human traffickers (e.g., by accepting bribes from labor brokers engaged in deceptive practices).[147] Human trafficking is also one of the most profitable crimes and a predicate offense for money laundering.[148] In 2020, a total of 11,193 situations of human trafficking were identified through the U.S. National Human Trafficking Hotline,[149] and globally, an estimated 24.9 million people are subjected to human trafficking, generating an estimated $150 billion in illicit profits annually.[150]

Financial activity from human trafficking activities can intersect with the regulated financial system at any point during the recruitment, transportation, and exploitation stages. The illicit proceeds from human trafficking can include income associated with logistics, such as housing and transportation of victims, as well as earnings from the exploitation of victims.[151] In the United States, human trafficking occurs in a broad range of industries, including, hospitality, agriculture, janitorial services, construction, restaurants, care for persons with disabilities, salon services, massage parlors, retail, fairs and carnivals, peddling and begging, childcare, domestic work, and drug smuggling and distribution.[152] Illicit proceeds from human trafficking can be paid or transferred in cash, electronic funds transfers/remittance systems, credit card transactions, payment apps, or virtual assets.

Sex trafficking, in particular, may be perpetuated by TCOs[153] and facilitated through online platforms.[154] For example, in June 2020, U.S. law enforcement seized CityXGuide and its related websites. In August 2021, Wilhan Martono, the creator, owner, and operator of CityXGuide, pled guilty to promotion and facilitation of prostitution and reckless disregard of sex trafficking and conspiracy to engage in interstate and foreign travel and transportation in aid of racketeering enterprises. Martono created, owned, and operated a network of websites, including CityXGuide, that posted hundreds of thousand of prostitution advertisements in locations across the United States and around the world. CityXGuide allowed pimps, prostitutes, and brothels to post and pay for advertisements that featured an explicit list of "intimate activities," along with nude or partially nude photographs, a physical description, work hours, methods of payment, and contact information for the female

146 "DHS, Blue Campaign, Myths and Misconceptions," https://www.dhs.gov/blue-campaign/myths-and-misconceptions.

147 UNODC, *Issue Paper: The Role of Corruption in Trafficking in Persons*, (2011), https://www.unodc.org/documents/human-trafficking/2011/Issue_Paper_-_The_Role_of_Corruption_in_Trafficking_in_Persons.pdf. See also U.S. Department of State, *Trafficking in Persons Report*, (2020), https://www.state.gov/wp-content/uploads/2020/06/2020-TIP-Report-Complete-062420-FINAL.pdf.

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

149 Polaris, *2019 U.S. National Human Trafficking Hotline Data Report*, (2019), https://polarisproject.org/wp-content/uploads/2019/09/Polaris-2019-US-National-Human-Trafficking-Hotline-Data-Report.pdf.

150 State Department, Trafficking in Persons Report. (June 2021), https://www.state.gov/wp-content/uploads/2021/07/TIP_Report_Final_20210701.pdf.

151 The White House, *The National Action Plan to Combat Human Trafficking*. (December 2021), https://www.whitehouse.gov/wp-content/uploads/2021/12/National-Action-Plan-to-Combat-Human-Trafficking.pdf.

152 FinCEN, "Supplemental Advisory on Identifying and Reporting Human Trafficking and Related Activity," (Oct. 15, 2020), https://www.fincen.gov/sites/default/files/advisory/2020-10-15/Advisory%20Human%20Trafficking%20508%20FINAL_0.pdf. This advisory is a supplement to FinCEN's 2014 advisory on Human Trafficking and Smuggling, and highlights financial and behavioral red flags and typologies related to human trafficking.

153 DOJ, "Five Defendants Convicted of Sex Trafficking, Alien Smuggling and Money Laundering," (Mar. 14, 2020), https://www.justice.gov/usao-edny/pr/five-defendants-convicted-sex-trafficking-alien-smuggling-and-money-laundering.

154 DOJ, "U.S. Attorney's Office Shuts Down Website Promoting Prostitution and Sex Trafficking, Indicts Owner," (Jun. 19, 2020), https://www.justice.gov/usao-ndtx/pr/us-attorney-s-office-shuts-down-website-promoting-prostitution-and-sex-trafficking.

being advertised.[155]

## 2. Human Smuggling

Human smuggling involves illegally transporting people, who have consented to their travel, into the United States and, potentially, the subsequent harboring of those individuals in the United States. Human smuggling is an inherently transnational crime, with smuggling routes across the southwest border remaining the most popular for entry into the United States.[156] Moving human beings as cargo pays in the billions of dollars for transnational criminal smuggling organizations.[157] Illegal smuggling fees can range from a few hundred dollars to over $10,000 to cross the border from Mexico to the United States,[158] while immigrants from China might pay tens of thousands dollars for their cross-Pacific journey.[159] Law enforcement has witnessed a significant spike in cross-border human smuggling over the past year and human smuggling on the southwest border of the U.S. is a daily occurrence.[160]

A 2019 RAND report prepared for the DHS estimates that the smuggling of unlawful migrants from the Northern Triangle region of Central America—Guatemala, Honduras, and El Salvador—to the United States generated between $200 million and $2.3 billion for human smugglers in 2017.[161] The wide range in estimated amounts reflects the uncertainty of underlying estimates related to unlawful migrant flows, the use of smugglers, and smuggling fees. The report also found that the illegal business of human smuggling includes independent operators, ad hoc groups, loose networks, and some more formally structured networks, such as TCOs.[162] TCOs that maintain control over drug smuggling territory profit from this illegal activity by charging smuggling organizations a fee or tax to pass through their territories.

## SPECIAL FOCUS: WILDLIFE TRAFFICKING

U.S. financial institutions are vulnerable to unwittingly processing transactions associated with wildlife trafficking given the importance of the U.S. dollar and financial system to international trade and finance, the difficulty of identifying underlying illicit connections, and a lack of financial intelligence on these types of crimes. More broadly, environmental crimes[163] threaten biodiversity, accelerate climate change, perpetuate forced labor, and increase risks for the spread of zoonotic diseases, which have national security implications.

The FATF recently noted that it is concerned about the lack of focus on the financial aspects of wildlife crimes.[164] While

155 DOJ, Northern District of Texas, *United States v. Wilhan Martono (CityXGuide)*, https://www.justice.gov/usao-ndtx/united-states-v-wilhan-martono-cityxguide.

156 DHS, "Snapshot: Using Data Analytics to Target Human Smugglers," (Aug. 14, 2018), https://www.dhs.gov/science-and-technology/news/2018/08/14/snapshot-using-data-analytics-target-human-smugglers.

157 ICE, Features, "Human Smuggling equals grave danger, big money," (updated Nov. 16, 2021), https://www.ice.gov/features/human-smuggling-danger.

158 Newsweek, "Customs and Border Protection (CBP) statement reporting prices range from a hundred to a few thousand dollars for Mexican nationals, from $8,000 to $10,000 for Central Americans, and from as high as $15,000 to more for people coming from Brazil or Ecuador," (Jun. 3, 2021), https://www.newsweek.com/human-smugglers-charging-15000-per-person-us-border-crossing-1597043.

159 DHS, "Snapshot: Using Data Analytics to Target Human Smugglers," (Aug. 14, 2018), https://www.dhs.gov/science-and-technology/news/2018/08/14/snapshot-using-data-analytics-target-human-smugglers.

160 ICE, Features, "Human Smuggling equals grave danger, big money," (updated Nov. 16, 2021), https://www.ice.gov/features/human-smuggling-danger.

161 RAND, "Human Smuggling and Associated Revenues," (2019), https://www.rand.org/pubs/research_reports/RR2852.html.

162 Id.

163 FinCEN, "FinCEN Calls Attention to Environmental Crimes and Related Financial Activity," (Nov. 18, 2021), https://www.fincen.gov/sites/default/files/2021-11/FinCEN%20Environmental%20Crimes%20Notice%20508%20FINAL.pdf.

164 FATF, *Money Laundering and the Illegal Wildlife Trade.* (2018), https://www.fatf-gafi.org/media/fatf/documents/Money-laundering-and-illegal-wildlife-trade.pdf.

the United States is at the international forefront of using law enforcement authorities to disrupt the financing of wildlife trafficking, the crime persists as a threat to the U.S. financial system. As the U.S. Fish and Wildlife Service has acknowledged, the United States is a major source and destination country for the illegal wildlife trade.[165]

FinCEN analysis of wildlife trafficking-related SARs filed through late 2021 indicates that wildlife trafficking affects the U.S. financial sector, but that financial institutions' current identification and reporting of potential wildlife trafficking may not reflect the totality of wildlife trafficking and associated illicit financial activity with a nexus to the United States. The number of wildlife trafficking-related SARs filed annually increased year over year between January 2018 and October 2021, with a total of 212 SARs filed in this period. SARs show that illicit financial activity related to potential wildlife trafficking is usually identified because of its connection to public or already known trafficking activity or because of a law enforcement referral related to wildlife trafficking.[166]

Between 2019 and 2021, numerous defendants were charged and convicted in dozens of wildlife trafficking cases in U.S. courts. The three dozen wildlife trafficking cases reviewed for this report, with total criminal proceeds exceeding $30 million over a period of two and a half years, represent a snapshot of the illegal wildlife trade in the United States. Several cases focused on turtles being shipped both to and from East Asia. Recently, a foreign national was sentenced for money laundering linked to financing a trafficking network that smuggled at least 1,500 protected turtles, valued at more than $2 million.[167] The financer sent money via online money transmitters, credit cards, or bank transfers to the United States to purchase turtles from sellers advertising on social media or reptile trade websites. Other wildlife cases involved smugglers facilitating the movement of illicit wildlife products and wildlife across the U.S.-Mexico border.[168] In many instances, wildlife traffickers have used the guise of legitimate businesses, including sales facilitated by online platforms, to sell illicit products and intermingle the proceeds with licit ones. The wildlife trafficking investigations with the largest amount of criminal proceeds, and the most likely to include money laundering components, involve defendants who are also affiliated with criminals or TCOs smuggling drugs, such as cocaine and heroin.[169] A recent ongoing investigation involved criminals who conspired to conduct large transactions via ocean freight, offering the buyer more than two tons of elephant ivory, one ton of pangolin scales, and multiple intact rhinoceros horns.[170]

Because the financial sector is less familiar with money laundering typologies in wildlife trafficking, and because of the difficulty in distinguishing financial transactions in illegal trade from large-scale legal trade, most criminal investigations in wildlife trafficking cases are the result of proactive law enforcement actions, rather than a follow-up to receiving financial intelligence. It is difficult to estimate the full scale of proceeds generated from this crime without more consistent financial reporting from the private and public sector.

165 U.S. Department of the Interior, Fish and Wildlife Service, "2020 Budget Justifications," https://www.fws.gov/budget/2020/FY2020-FWS-Budget-Justification.pdf.

166 FinCEN, *Illicit Finance Threat Involving Wildlife Trafficking and Related Trends in Bank Secrecy Act Data*. (Dec. 20, 2021), https://www.fincen.gov/sites/default/files/2021-12/Financial_Threat_Analysis_IWT_FINAL%20508_122021.pdf.

167 DOJ, "Foreign National Sentenced for Money Laundering Funds to Promote Turtle Trafficking," (Oct. 6, 2021), https://www.justice.gov/opa/pr/foreign-national-sentenced-money-laundering-funds-promote-turtle-trafficking.

168 DOJ, "Environmental Crimes Section Monthly Bulletin," (December 2020), https://www.justice.gov/enrd/page/file/1358886/download.

169 DOJ, "International money laundering, drug trafficking and illegal wildlife trade operation dismantled," (Sep. 3, 2020), https://www.justice.gov/usao-sdga/pr/international-money-laundering-drug-trafficking-and-illegal-wildlife-trade-operation.

170 DOJ, "Two Foreign Nationals Arrested for Trafficking Ivory and Rhinoceros Horn as Part of International Operation with the Democratic Republic of the Congo," (Nov. 8, 2021), https://www.justice.gov/opa/pr/two-foreign-nationals-arrested-trafficking-ivory-and-rhinoceros-horn.

# Section II: Vulnerabilities and Risk

In the context of the 2022 NMLRA, a money laundering vulnerability is what facilitates or creates the opportunity for money laundering. 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 most amount of money to be laundered quickly or with little risk of being caught present the greatest potential vulnerabilities. Residual risk is a function of threat and vulnerability and represents an overarching judgment, taking into consideration 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

The U.S. dollar has functioned as the world's dominant reserve currency since World War II. As of December 2020, central banks around the globe held about 60 percent of their foreign exchange reserves in U.S. dollars.[171] Most of this total was held in the form of U.S. Treasury securities. As of the end of the first quarter of 2021, about a third of the total of marketable Treasury securities outstanding, or $7 trillion, were held by foreign investors, with a little over 40 percent held by domestic private parties and the remaining quarter held by the Federal Reserve System itself.[172] In foreign exchange markets, where currencies are traded, U.S. dollars are involved in nearly 90 percent of all transactions. Individuals and banks in some countries continue to hold onto U.S. dollar banknotes as a store of value to hedge against political and economic uncertainty. Financial institutions around the world are taking advantage of improved international logistics and have been repatriating U.S. dollar banknote stockpiles accumulated during the pandemic.[173]

### 1. Bulk Cash Smuggling

COVID-19, at least temporarily, changed the money laundering landscape due to a dramatic decrease in commercial air travel, shipping delays, and border restrictions between the United States and Mexico during the height of global lockdowns. During that period, drug traffickers had difficulty transporting bulk currency from the United States across the southwest border into Mexico. This resulted in a stockpiling of large amounts of U.S. currency on the U.S. side. Although the pandemic led to a temporary decline in some BCS activity, it is believed that TCOs continue to repatriate a significant volume of illicit proceeds every year via BCS.

HSI's National Bulk Cash Smuggling Center conducted a comparative analysis of BCS activity observed during 2018, 2019, and 2020 to assess the impact of COVID-19 on BCS. As noted above, travel restrictions and border security caused a freeze in TCOs' financial supply chains in the United States, resulting in cash stockpiling from March to May 2020. TCOs appear to have adapted by partly abandoning the strategy of widely distributed small loads of bulk cash and switching BCS tactics toward fewer, larger cash loads over the spring and summer of 2020, based on DHS interdictions during this time. For example, instead of the long-standing median cash load of

171 Congressional Research Service, *The U.S. Dollar as the World's Dominant Reserve Currency*, (December 2020), https://crsreports.congress.gov/product/pdf/IF/IF11707.

172 Federal Reserve System, FEDS Notes, "The International Role of the U.S. Dollar," (Oct. 06, 2021), https://www.federalreserve.gov/econres/notes/feds-notes/the-international-role-of-the-u-s-dollar-20211006.htm.

173 Reuters, "Fed quarantines U.S. dollars repatriated from Asia on coronavirus caution," (Mar. 6, 2020), https://www.reuters.com/article/us-health-coronavirus-fed-dollars/fed-quarantines-u-s-dollars-repatriated-from-asia-on-coronavirus-caution-idUSKBN20T1YT.

between $24,000 and $37,000, HSI and U.S. Customs and Border Protection (CBP) began to encounter loads that were 10 to 20 times larger.

According to law enforcement sources, decreases in outbound BCS activity took place between 2013 and 2018, which represented the "floor" with the lowest outbound BCS seizure totals (438 incidents, totaling just under $10 million). The year 2019 represented the highest outbound seizure activity (1,111 incidents, totaling $746 million) with activity slightly decreasing in 2020 (1,010 incidents, totaling $741 million). On a typical day during 2020, CBP seized $386,195 in illicit currency.[174] HSI attributed the recent changes from 2019-2020 to greater CBP operational focus and outbound inspections at the border (e.g., vehicles at southwest border) and a greater ability to target high-risk conveyances given the less frequent commercial and personal travel. For example, in 2019, Newark Liberty International Airport was the second-ranking port in the United States by seizure with 100 cash seizures. However, in 2020, Newark fell out of the top 10 ranking. Moving up the list were ports such as Laredo, Texas, and Eagle Pass, Texas, which both saw a doubling of their outbound cash seizures.

HSI also reported a significant rise in seizures of bulk cash from the Caribbean basin during June-August 2020, which suggests geographic and modal adaptations by TCOs to avoid exposure to the additional scrutiny along the southwest land border. For example, San Juan BCS seizures doubled in 2020 from 2019. U.S. Attorney's Offices in the U.S. Virgin Islands (USVI) and Puerto Rico have also noted an increase in BCS cargo shipments through their ports and an increase of cash couriers from these jurisdictions to the continental United States. The U.S. Attorney's Office for the USVI also noted the use of U.S. Postal Service (USPS) and other mail carriers to send cash (and money orders) from USVI to the mainland.

### Case examples

- In December 2020, a Texas man pleaded guilty to BCS after an outbound inspection of his vehicle from the United States into Mexico found $571,497 in bulk U.S. currency hidden in the spare tire. He acknowledged knowing he was concealing the money and that it was illegal to transport the currency from the United States to Mexico unreported.[175]
- In April 2021, three Puerto Rican men were caught smuggling over $3 million into the USVI using a private vessel. According to the affidavit, CBP Air and Marine (AMO) agents noticed a vessel approaching without its navigation lights illuminated and initiated a stop. After the AMO agents boarded the vessel and detained the three occupants, the agents recovered three duffel bags from the water that had been thrown overboard. A fourth duffel bag was discovered on the vessel. Agents estimate that the bags collectively contained at least $3 million. One of the duffel bags was equipped with a GPS tracker. The vessel, which is registered in Puerto Rico, was outfitted with five fuel tanks.[176]
- In June 2020, a Mexican man was convicted for attempting to smuggle $879,000 in alleged drug proceeds collected in the United States and consolidated in San Antonio, Texas to Mexico, including via private aircraft.[177]

174 CBP, "On a Typical Day in Fiscal Year 2020, CBP..." https://www.cbp.gov/newsroom/stats/typical-day-fy2020.

175 DOJ, "Texan admits to attempting to illegally take cash to Mexico," (Dec. 21, 2020), https://www.justice.gov/usao-sdtx/pr/texan-admits-attempting-illegally-take-cash-mexico.

176 DOJ, "Three Puerto Rican Men Caught Smuggling Over $3 Million Cash Into St. Thomas Onboard a Vessel Near Brewer's Bay," (Apr. 20, 2020), https://www.justice.gov/usao-vi/pr/three-puerto-rican-men-caught-smuggling-over-3-million-cash-st-thomas-onboard-vessel-near.

177 ICE, "A Mexican man sentenced for attempting to smuggle close to $900k in US currency into Mexico," (Jun. 11, 2020), https://www.ice.gov/news/releases/mexican-man-sentenced-attempting-smuggle-close-900k-us-currency-mexico.

## 2. Postal Money Orders

Money orders are negotiable financial instruments, which represent a convenient, widely accepted form of payment. They are more secure than cash, and unlike checks, money orders cannot bounce as the funds are prepaid at the time of purchase. Data provided by the Federal Reserve Board (FRB) indicates that in 2019, the Federal Reserve processed $21.4 billion in USPS money orders and in 2020, they processed $20.6 billion.[178] This data suggests that USPS money orders continue to be a popular form of payment utilized by the public.

USPS money orders also continue to be exploited by criminals and TCOs, as evidenced by Inspection Service investigations. Money orders are used in a wide variety of criminal activities ranging from fraud to narcotics trafficking to human trafficking. Money orders offer a vehicle to convert illicit proceeds to a monetary instrument that is not inherently suspicious in nature. Furthermore, individuals seek to launder their funds through a MSB (such as USPS) while also remaining relatively anonymous throughout a transaction. USPS money orders can be purchased using cash, debit cards, and traveler's checks payable in U.S. dollar (if the purchase is for at least 50 percent of the value of the traveler's checks). If a customer purchases USPS money orders with cash totaling $3,000 or more in a business day, they must complete PS Form 8105-A, Funds Transaction Report, and provide an acceptable form of identification and identifying information.[179]

USPS business records indicate there was a rising number of USPS money order sales that were deemed suspicious from 2018 through 2020, and those figures were in the billions of dollars. Inspection Service seizure data, however, indicates that Postal Inspectors were successful in seizing only a small fraction of USPS money orders (when compared to the number of money orders that were reported as suspicious). This exemplifies one of the many challenges of money order investigations, namely, that money orders are generally negotiated relatively soon after being purchased. As a result, law enforcement officers have a short window to develop the necessary probable cause to seize USPS money orders before they are cashed.

### Case examples

- In September 2021, two individuals who hacked into tax preparation firms and filed fraudulent unemployment benefit claims and tax returns using stolen PII, and then laundered the fraudulent assets, were sentenced to federal prison. Fraudulent funds from this unemployment benefits scheme and tax fraud scheme were deposited into bank accounts set up by co-conspirators. One defendant recruited Zambian nationals to travel to the United States on tourist visas to incorporate sham corporations in Georgia and open business bank accounts in the names of those corporations. After the fraudulent funds were deposited into those accounts, the defendant laundered the funds by cashing money orders purchased with debit cards linked to the accounts.[180]

## 3. Funnel Accounts

A funnel account involves an individual or business account in one geographic area that receives multiple cash deposits, often in amounts below the cash reporting threshold, and from which the funds are withdrawn in a different geographic area with little time elapsing between the deposits and withdrawals. They are typically seen in a variety of complex frauds and scams targeting the elderly or other victims and are also used by DTOs and fraud rings to get illicit cash proceeds out of the United States. They are used on a large scale with great effect by networks of money mules, who are often controlled by PMLOs or fraud rings. Cash activity occurs at financial

178 Federal Reserve, "Postal Money Orders Processed by the Federal Reserve—Quarterly Data," https://www.federalreserve.gov/paymentsystems/check_postalmosprocqtr.htm.

179 See 31 CFR § 1010.415(a)(2).

180 DOJ, "Nigerian hacker and a repeat offender sentenced to federal prison for unemployment fraud and tax fraud scheme," (Sep. 2, 2021), https://www.justice.gov/usao-ndga/pr/nigerian-hacker-and-repeat-offender-sentenced-federal-prison-unemployment-fraud-and-tax.

institution branches across the United States. The most frequent geographic locations visited by money mules to structure cash deposits reflect known consolidation points for bulk cash and illicit proceeds. As shown by recent case examples, owners of potential funnel accounts make cash withdrawals near the southwest border or send cross-border payments to Mexico.

### Case examples

- In November 2021, an indictment was partially unsealed in federal court charging 29 alleged members of a PMLO that is tied to the Sinaloa Cartel and CJNG Cartel in Mexico. According to the indictment and other public records, this PMLO laundered in excess of $32 million in drug proceeds from the United States to Mexico. The PMLO secured contracts with DTOs in Mexico to pick up drug proceeds in cities throughout the United States. The defendants allegedly served as either couriers and/or funnel bank account holders. After the illicit cash proceeds were deposited into the fictitious funnel bank accounts, the monies were wired to personal bank accounts in Mexico where the money was then dispersed to the DTOs.[181]
- In March 2020, 24 individuals were arrested for their involvement in a large-scale fraud and money laundering operation that targeted individuals and corporations, funneling $30 million in illicit proceeds into financial institutions throughout the United States. The defendants and co-conspirators facilitated BEC schemes, romance scams, and retirement account scams by receiving and distributing fraudulent funds. The defendants created multiple shell companies that did not have physical premises, earn legitimate income, or pay wages to employees. In turn, the defendants opened business bank accounts at multiple financial institutions to facilitate receipt of the fraudulent money. The defendants also opened personal bank accounts to receive fraudulent funds, often using false identities or victims' identities. After funds were deposited into the defendants' bank accounts, the money was quickly withdrawn from the accounts and circulated among the defendants.[182]
- In October 2019, Manuel Reynoso Garcia was sentenced for money laundering for his role as a leader in a PMLO that laundered more than $19 million in narcotics proceeds from the United States to Mexico. According to the plea agreement and other public records, the PMLO was composed of a network of co-conspirators who coordinated the pickup, deposit, laundering, and transfer of millions of dollars of narcotics proceeds to a Mexico-based DTO. The organization recruited individuals to serve as funnel account holders and transported them to bank branches on the southwest border to open personal bank accounts typically at domestic U.S. banks. The funnel account holders were primarily young adults between the ages of 18 and 23 who attended a university in Tijuana, Mexico.[183]

## 4. Cash-Intensive Businesses

The use of cash-intensive businesses is one of the oldest and most reliable methods to place and layer illicit funds, often through the use of a front company. Front companies are fully functioning companies, often having a physical location, with the characteristics of a legitimate business, and should not be confused with shell or shelf companies, which are discussed later in this report. 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.[184] Investigators and prosecutors often see illicit proceeds

181 DOJ, "Alleged Money Launderers for Mexican Cartels Indicted," (Nov. 16, 2021), https://www.justice.gov/usao-sdca/pr/alleged-money-launderers-mexican-cartels-indicted.

182 DOJ, "Dozens charged in Atlanta-based money laundering operation that funneled $30 million in proceeds from computer fraud schemes, romance scams, and retirement account fraud," (Mar. 11, 2020), https://www.justice.gov/usao-ndga/pr/dozens-charged-atlanta-based-money-laundering-operation-funneled-30-million-proceeds.

183 DOJ, "Eighth Member of International Money Laundering Organization Sentenced in $19 Million Dollar Scheme," (Oct. 29, 2019), https://www.justice.gov/usao-sdca/pr/eighth-member-international-money-laundering-organization-sentenced-19-million-dollar.

184 31 C.F.R. § 1010.330.

laundered through cash-intensive businesses, such as corner stores, small auto repair shops, and gas stations. In such examples, the cash deposits and subsequent activity in their bank accounts do not align with what a legitimate business would show. Business restrictions that were in place due to COVID-19 affected the cash flow of many businesses because of closures and customer service restrictions, making it more difficult to move suspiciously high volumes through businesses reliant on in-person, cash-based transactions.

An emerging trend in this area is the use of auto auctions to "clean" funds. For example, auto auction companies have set up accounts for individuals who deposited illicit proceeds but did not purchase any cars, and who then asked the auction company to issue them a refund. The auction company has typically issued a check for the refund to make the funds appear "clean." These companies have allowed individuals to store funds toward the purchase of vehicles and receive funds in their accounts with very few customer due diligence (CDD) requirements.

**Case examples**

- In 2020, three individuals were sentenced for their part in a money laundering conspiracy used to defraud financial institutions through an elaborate auto-financing scheme. All Auto Care had a license that permitted it to buy and sell vehicles at auto auctions in the state of Minnesota. As part of the scheme, the vehicles were "sold" by the co-conspirators through All Auto Care to an auto dealership located in Illinois, where other conspirators worked. The conspirators committed the fraud by applying for fraudulent vehicle financing using deceased buyers' names or stolen identities or by paying people for the use of their information to buy luxury vehicles. After receiving the loan proceeds, the conspirators made a nominal number of sham ("lulling") payments to make the loans appear legitimate when, in actuality, the conspirators laundered the funds through various bank accounts they controlled.[185]
- In another case, an individual took cash drug proceeds to a casino and gambled about $1.4 million over an 18-month span. To disguise drug proceeds as gambling winnings, the individual would exchange small bills for large bills. This individual and his co-conspirators also moved cash drug proceeds through legitimate businesses (i.e., a mechanic shop and discount used car dealership). They also had several jointly owned businesses that did no actual business (another car dealership, a construction company, and an LLC with no stated purpose). They deposited cash into the businesses' accounts, transferred smaller amounts to the other accounts, and then withdrew it. More than a million dollars in cash moved through the businesses over two years.[186]

## MISUSE OF LEGAL ENTITIES

While many legal entities are used for legitimate purposes, illicit actors frequently misuse these structures to obscure illegal activities, including money laundering. Malign actors and their financial facilitators take advantage of the anonymity and perceived legitimacy afforded to legal entities to disguise and convert the proceeds of crime before introducing them into the financial system. The deliberate misuse of legal entities, including limited liability companies and other corporate vehicles, trusts, partnerships, and the use of nominees continue to be significant tools for facilitating money laundering and other illicit financial activity in the U.S. financial system. Determining the true ownership of these structures requires time-consuming and resource-intensive processes by law enforcement when conducting financial investigations.[187]

As described in more detail below, the misuse of legal entities, both within the United States and abroad, remains

185 DOJ, "Three Men Sentenced In Money Laundering, Identity Theft Scheme, (Aug. 28, 2020), https://www.justice.gov/usao-mn/pr/three-men-sentenced-money-laundering-identity-theft-scheme.

186 Western District of Michigan, *United States v. James Moore et al.*, 1:20-cr-00189.

187 FBI, "Testimony of Steven M. D'Antuono, Section Chief, Criminal Investigative Division," (Nov. 29, 2018), https://www.fbi.gov/news/testimony/combating-money-laundering-and-other-forms-of-illicit-finance.

a major money laundering vulnerability in the U.S. financial system. These entities can facilitate money laundering involving domestic and foreign bribery and corruption schemes, sanctions evasion, tax evasion, drug trafficking, and fraud, among other types of offenses. Recent cases indicate that money laundering activity involving the misuse of legal entities remains complex and significant.

## 1. Status of Beneficial Ownership Requirements

As defined by the FATF, the global AML/CFT standard-setting body, a beneficial owner is the "natural person(s) who ultimately owns or controls a customer and/or the natural person on whose behalf a transaction is being conducted." FATF also considers as beneficial owners "those persons who exercise ultimate effective control over a legal person or arrangement."[188]

Within the United States, criminals have historically been able to take advantage of the lack of uniform laws and regulations pertaining to the disclosure of information detailing an entity's beneficial owners, or beneficial ownership. This has stemmed mainly from the different levels of information and the transparency required by states at the time of a legal entity's registration. Treasury, DOJ, and federal law enforcement agencies have generally supported stronger requirements around beneficial ownership.

Until recently, the United States had major gaps in its legal and regulatory framework for the collection of beneficial ownership information, both by financial institutions and the government, leading the FATF to give the United States the lowest possible ratings in 2016 for its lack of transparency of beneficial ownership information, limited law enforcement access to this information, and failing to prevent legal persons and arrangements from being used for criminal purposes.[189] Combating the misuse of legal entities is not a challenge only for the United States but for many jurisdictions across the globe. According to the FATF, out of more than 100 mutual evaluations, only one-third of countries have laws and regulations related to the transparency of legal persons and arrangements that comply with FATF standards. Only 10 percent of countries take effective measures to ensure the transparency of company and trust ownership.[190]

The United States has made significant progress since 2016 in addressing these gaps. FinCEN's CDD rules and beneficial ownership requirements, which became applicable in May 2018, help mitigate this vulnerability by requiring 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. The FATF has determined that due to FinCEN's CDD and beneficial ownership requirements, the United States now largely complies with the FATF standard on CDD.[191] With the recent enactment of the Corporate Transparency Act, part of the 2021 National Defense Authorization Act (NDAA), certain companies will be required to disclose to FinCEN their beneficial ownership information when they are formed (or for non-U.S. companies, when they register with a state to do business in the United States); they will also be required to report changes in beneficial owners.[192]

---

188 FATF, *The FATF Recommendations,* (June 2021), https://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf; SEC, Guide to Investing, see "Schedules 13D and 13G," https://www.investor.gov/introduction-investing/investing-basics/glossary/schedules-13d-and-13g.

189 FATF, *United States Mutual Evaluation*, (2016), https://www.fatf-gafi.org/media/fatf/documents/reports/mer4/MER-United-States-2016.pdf.

190 FATF, "Public Statement on the Pandora Papers," (Oct. 21, 2021), https://www.fatf-gafi.org/publications/fatfgeneral/documents/pandora-papers.html.

191 FATF, "United States 3rd Enhanced Follow-up Report & Technical Compliance Re-Rating," (March 2020), https://www.fatf-gafi.org/media/fatf/documents/reports/fur/Follow-Up-Report-United-States-March-2020.pdf.

192 FinCEN, "FinCEN Issues Proposed Rule for Beneficial Ownership Reporting to Counter Illicit Finance and Increase Transparency," (Dec. 7, 2021), https://www.fincen.gov/news/news-releases/fincen-issues-proposed-rule-beneficial-ownership-reporting-counter-illicit.

The new U.S. requirements for the disclosure of beneficial ownership information to the federal government, once fully implemented, are expected to help facilitate law enforcement investigations and make it more difficult for illicit actors to hide behind corporate entities registered in the United States or those foreign entities registered to do business in the United States. However, illicit actors can still take advantage of foreign legal structures lacking beneficial ownership disclosure requirements to obscure their illicit activity. For example, money launderers with a U.S. nexus, including those linked to foreign corrupt activity (e.g., PEPs), can continue to rely on the anonymity granted to beneficial owners of shell companies and other corporate vehicles that are not registered in the U.S. and that are within "black box" jurisdictions abroad that have strong corporate secrecy laws and lackluster legal frameworks that do not facilitate international cooperation.

## 2. Shell and Shelf Companies

As reported in previous risk assessments, bad actors consistently use a number of specific structures to disguise criminal proceeds, and U.S law enforcement agencies have had no consistent way to obtain information about the beneficial owners of these entities. The ease with which companies can be incorporated under state law and the lack of information generally required about the company's owners or activities lead to limited transparency. Bad actors take advantage of these lax requirements to set up shell companies, while those looking for ready-to-use legal entities can exploit legal entities that are "off the shelf," or incorporated in the past to make them appear "established" to outsiders.

### Case examples

- In September 2020, Richard Gaffey, a U.S. accountant was sentenced for wire fraud, tax fraud, money laundering, and aggravated identity theft pertaining to his involvement in a decades-long tax evasion scheme perpetrated by Panamanian law firm, Mossack Fonseca.[193] According to court documentation, Gaffey helped U.S. taxpayers avoid reporting income, including by obscuring his clients' beneficial ownership of offshore shell companies and setting up bank accounts for the shell companies. He also helped one of the owners of Mossack Fonseca conceal his assets and income from the IRS by providing personal identity information belonging to the owner's mother (a Guatemalan national not subject to U.S. taxes) to a U.S. bank purporting that she was the sole beneficial owner of the shell companies and bank accounts belonging to the law firm's owner.[194]
- In June 2020, DOJ announced a civil forfeiture complaint involving $20 million in funds implicated in an Iranian sanctions evasion scheme that used shell companies in the United States and abroad.[195] According to the complaint, three Iranian nationals and a U.S. national effectuated sham transactions to covertly move the equivalent of $1 billion in Iranian-held funds located in a South Korean financial institution. The defendants converted the funds, held in South Korean bank accounts, to U.S. dollars and then laundered them through shell companies registered in the United States, the United Arab Emirates, and South Korea. The Iranians then sought to use $20 million in the laundered funds to purchase a hotel in Tbilisi, Georgia, of which $7 million was ordered to be forfeited. The $7 million was to be allocated to the U.S. Victims of State Sponsored Terrorism Fund, which Congress established to provide compensation to certain individuals who were injured in acts of international state-sponsored terrorism.[196]

193 While based out of Panama, Mossack Fonseca provided global company formation services, operating out of popular company formation centers such as Nevada and Wyoming, which are also known for high levels of corporate secrecy.

194 DOJ, "U.S. Accountant in Panama Papers Investigation Sentenced to Prison," (Sep. 24, 2020), https://www.justice.gov/opa/pr/us-accountant-panama-papers-investigation-sentenced-prison.

195 DOJ, "Justice Department Seeks Forfeiture of More than $20 Million in Assets Relating to Unlawful Use of U.S. Financial System to Evade and Violate Iranian Sanctions," (Jun. 3, 2020), https://www.justice.gov/opa/pr/justice-department-seeks-forfeiture-more-20-million-assets-relating-unlawful-use-us-financial.

196 DOJ, "U.S. Government Collects $7 Million in Iranian Assets for Victims of Terrorism Fund," (Jan. 5, 2021), https://www.justice.gov/usao-ak/pr/us-government-collects-7-million-iranian-assets-victims-terrorism-fund.

- In March 2019, a Russian telecommunications company and its Uzbek subsidiary entered into a deferred prosecution agreement (DPA) with DOJ for bribing an Uzbek official, who then used legal entities to launder the bribes through the U.S. financial system. As detailed in the DPA, the Russian company and the Uzbek subsidiary paid approximately $420 million in bribes to an Uzbek official so the company could enter the Uzbek market through the acquisition of an Uzbek company and gain its valuable telecom assets. The companies structured and concealed bribes through payments to shell companies and charities controlled by the official.[197]

## 3. Special Focus: Trusts

The misuse of trusts for money laundering is recognized as a global problem by the FATF, which has identified characteristic AML/CFT vulnerabilities of trusts that include (1) problematic relationships among the settlor, trustee, and beneficiary of a trust; (2) use of specific trust provisions to obscure relevant facts; and (3) use of trusts to take advantage of jurisdictional differences.[198] In the United States, a trust is a legal arrangement created and governed under the state law (whether statutory or common law) of the jurisdiction in which it was formed. A trust is generally a relationship created by an arrangement between the grantor and the trustee, under which the trustee assumes fiduciary obligations to the trust's beneficiaries. The legal title to any property held in trust is controlled by the trustee, who is then charged with the responsibility of administering that property for the benefit of one or more beneficiaries. The beneficiaries of the trust may receive the economic benefits from the trust property, but generally have no power over the investment or distribution of that property. The duties, powers and responsibilities of these parties are determined by the law of the jurisdiction of formation of the trust and by the trust agreement.

Central to trust law is a set of fiduciary duties or obligations imposed on every trustee, one effect of which is to require that the trustee have and maintain information about other parties relevant to the trust, including co-trustees, the grantor, and the beneficiaries of the trust.[199] However, several states have recently enacted or proposed trust legislation that may run counter to conventional trust law in some ways. This includes the formation of a domestic asset protection trust (DAPT) similar to those in South Dakota and Wyoming.[200] A DAPT is an irrevocable, self-settled trust, of which the grantor is a permissible beneficiary; this framework is considered attractive because it purportedly protects any assets in trust from the creditors of the grantor, even if the grantor is also a beneficiary.[201] A DAPT allows for a grantor to retain access to the assets placed in the trust, while purportedly shielding those assets from the claims of most future creditors of the grantor. The drafters of the Uniform Trust

197 DOJ, "Mobile Telesystems Pjsc and Its Uzbek Subsidiary Enter into Resolutions of $850 Million with the Department of Justice for Paying Bribes in Uzbekistan," (Mar. 7, 2019), https://www.justice.gov/opa/pr/mobile-telesystems-pjsc-and-its-uzbek-subsidiary-enter-resolutions-850-million-department.

198 FATF, *Guidance on Transparency of Beneficial Ownership (Recommendations 24 & 25)*. (Oct. 2014), https://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-transparency-beneficial-ownership.pdf.

199 These duties appear in the Uniform Trust Code (UTC) in sections 801 through 813. These fiduciary duties are (1) a duty to administer the trust for the benefit of the beneficiaries, sometimes described as a duty of good faith, loyalty, and impartiality, (2) a duty to invest prudently, (3) a duty to act prudently, (4) a duty to maintain records, (5) a duty to identify and safeguard the assets of the trust, (vi6) the duty not to commingle the trust assets and the trustee's assets; and (7) the duty to inform and report to the beneficiaries. UTC Section 404 states, "a trust may be created only to the extent its purposes are lawful, not contrary to public policy, and possible to achieve." The comment to this section states, "a trust with a purpose that is unlawful or against public policy is invalid." A total of 31 U.S. States and the District of Columbia have adapted the UTC to codify and harmonize their trust laws, and where states have their own statutes regulating trusts, they typically have followed the basic principles outlined in the UTC with some key distinctions.

200 American College of Trust and Estate Counsel, *Twelfth Comparison of the DAPT Statutes*. (August 2019), https://www.actec.org/assets/1/6/Shaftel-Comparison-of-the-Domestic-Asset-Protection-Trust-Statutes.pdf?hssc=1.

201 JDSUPRA, "Asset Protection Trusts: 'Everybody Gets a DAPT!'" *(even those outside Connecticut)*. (Sep. 12, 2019), https://www.jdsupra.com/legalnews/asset-protection-trusts-everybody-gets-44243/.

Code (UTC) rejected the approach taken in states like Alaska, Delaware, South Dakota, and Wyoming and instead endorsed the common law rule that makes it impossible to create a trust for oneself that will be immune from the claims of the settlor's own creditors.[202]

Federal law does not regulate trusts. Rather, federal law applicable to trusts is primarily directed toward the taxation of trust income. U.S. trusts are taxed on U.S. and foreign source income, and foreign trusts are taxed only on U.S. source income. A trust with income generating a U.S. tax liability is required to file an annual income tax return with the IRS and may be required to file an income tax return with a state, if applicable. That return will disclose the identifying information and tax identification number of each beneficiary who received taxable income from the trust during that year. A foreign trust with no U.S. source income need not file an annual income tax return with the IRS and therefore need not disclose its beneficiaries to the IRS. A trust that is formed under U.S. law may be treated as a foreign trust for tax purposes if a non-U.S. person has control over one substantial decision of the trust (e.g., a non-U.S. protector with the authority to decide whether to replace a trustee). Under the reciprocal Foreign Account Tax Compliance Act intergovernmental agreements, the IRS is not required to automatically exchange information on accounts maintained by U.S. financial institutions—including accounts held by foreign trusts—if the account does not receive income during the year or receives only foreign source income.

The exact number of trustees in the United States is unknown as trusteed legal arrangements are not registered and generally any natural person may serve as a trustee. Over the years, the use of trusts has increased as settlors seek to protect family assets both from the claims of future creditors and divorcing spouses of trust beneficiaries (other than the settlor) and from transfer taxes by contributing assets to dynastic trusts for multiple generations of beneficiaries. As a result, the U.S. trust industry has steadily been growing. This appears to be true especially in states with DAPT statutes. For example, as of September 2021, South Dakota, a state of less than 900,000 persons, was home to more than 100 trust companies[203] with approximately $367 billion in assets reportedly held in 2020, which is an amount larger than the approximately $29 billion held by banks operating in the state.[204] In Wyoming, a state with a population of less than 600,000 people, the trust industry likewise is growing, with approximately $15 billion of assets under management, which is equivalent to approximately 30 percent of the state's GDP.[205] It appears that, particularly for assets coming from foreign jurisdictions where there is no existing connection or relationship with any U.S. state, the purported creditor protections offered to settlors by these statutes have attracted the assets to trusts in those states.

Trustees (except for trust companies) are not subject to the Bank Secrecy Act (BSA). When misused, trust and asset management accounts can conceal the sources and uses of funds, as well as the identity of beneficial owners.[206] Factors that can serve as indicia of a higher risk that the trust is being used for inappropriate purposes include unusual account relationships and circumstances, questionable assets and sources of assets, and other potential areas of risk, such as offshore accounts, private investment companies, and transfers of funds to or from offshore accounts.

---

202 UTC, Comments on p. 91.

203 South Dakota Department of Labor and Regulation, "Trust Licensed to Do Business in South Dakota as of Sep. 1, 2021," https://dlr.sd.gov/banking/licensed_providers/state_chartered_trust_companies.pdf.

204 South Dakota Department of Labor and Regulation, *2020 Annual Report*, https://dlr.sd.gov/publications/documents/annrpt20.pdf.

205 Oil City News, "Public trusts in Wyoming managing ~$15 billion; Legi. looking to lure foreign interest," (Jan. 27, 2021), https://oilcity.news/wyoming/legislature/2021/01/27/public-trusts-in-wyoming-managing-15-billion-legi-looking-to-lure-foreign-interest/.

206 FFIEC Manual, "Risk Associated with Money Laundering and Terrorist Financing, Trust and Asset Management Overview," https://bsaaml.ffiec.gov/manual/RisksAssociatedWithMoneyLaunderingAndTerroristFinancing/21.

To date, the available evidence does not indicate that trusts established within the United States are frequently used for money laundering purposes.[207] They are used for tax avoidance purposes by both U.S. and foreign persons. While that is distinct from money laundering, it still is of interest to the Treasury. Where trusts were identified as being used to launder money, they relied on strawman trustees (trustees willing to act illegally) to provide a clean name for the trust documents. The U.S. government is seeking to expand its understanding of whether and how U.S. trusts are misused for illicit purposes in the United States.

- In October 2021, six defendants were charged with conspiring to defraud the IRS and other fraud offenses from at least January 2015 through September 2018. According to the superseding indictment, as part of the tax fraud scheme, the conspirators allegedly filed fraudulent individual tax returns and other tax documents that reported false withholdings from mortgage lenders and then claimed substantial refunds from the IRS. After processing the false returns, the IRS allegedly issued refunds totaling over $1 million. To prevent the IRS from recovering the fraudulently obtained refunds, the conspirators allegedly created trusts, opened new bank accounts in the name of business entities and the trusts, and transferred the criminal proceeds between the accounts to conceal the funds from the IRS.[208]

## Virtual Assets

In the United States, digital assets[209] is a broad term that includes so-called digital currencies, stablecoins,[210] and other terms used in the industry. Depending on the circumstances, digital assets can be securities, commodities, derivatives, or something else. Public information on investigations often uses the terms virtual currency or cryptocurrency. This report uses the terms virtual asset and VASP, terms not contained explicitly in U.S. law or regulation, to align with the terminology defined by the FATF.[211] Virtual assets, as used in this report, include and non-sovereign-administered digital assets (such as convertible virtual currencies [CVCs], like bitcoin and stablecoins) but do not cover central bank-issued digital currencies (CBDCs), which are representations of fiat currency and treated the same as fiat currency by the FATF.[212]

Some virtual assets allow instantaneous transactions without the involvement of a financial institution with AML/CFT obligations. These transactions may also be transferred across jurisdictional boundaries and may be anonymous.[213] VASPs doing business wholly or in substantial part in the United States qualify as money

207 There are cases of complicit attorneys that intentionally misuse their client trust accounts to launder criminal proceeds, but these accounts are not trusts; rather, they are the equivalent of an escrow fund.

208 DOJ, "Six Defendants Charged with Conspiring to Defraud the IRS and Other Fraud Offenses," (Oct. 15, 2021), https://www.justice.gov/usao-hi/pr/six-defendants-charged-conspiring-defraud-irs-and-other-fraud-offenses.

209 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%20Joint%20Policy%20Statement_508%20FINAL_0.pdf.

210 Stablecoins are digital assets that are designed to maintain a stable value "pegged" to a national currency or other reference assets. As with all digital assets, stablecoins can present ML/TF risks. The magnitude of these risks depends on various factors, including the application of AML/CFT controls, the degree to which it is adopted by the public, and the design of the stablecoin arrangement. For additional information, see the President's Working Group on Financial Markets, the Federal Deposit Insurance Corporation, and the Office of the Comptroller of the Currency's *Report on Stablecoins* (November 2021), https://home.treasury.gov/system/files/136/StableCoinReport_Nov1_508.pdf.

211 FATF, "FATF's Focus on Virtual Assets," https://www.fatf-gafi.org/publications/virtualassets/documents/virtual-assets.html?hf=10&b=0&s=desc(fatf_releasedate).

212 CBDCs may have unique ML/TF risks compared with physical fiat currency, depending on their design, and such risks should be addressed prior to launch. CBDCs may also present opportunities to program AML/CFT controls into the CBDCs or related service providers, but these opportunities should also take in consideration data privacy and other concerns.

213 Lexis-Nexis, White Paper, *A Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers*, (December 2019), https://risk.lexisnexis.com/global/-/media/files/financial%20services/white-paper/lnrs-emea%20virtual%20assets%20wp-nxr14189-00-1119-en-us.pdf.

transmitters, which means they are required to comply with the BSA obligations that apply to MSBs, including registering with FinCEN; developing, implementing, and maintaining an effective AML program; filing SARs and currency transaction reports (CTRs); appointing a chief compliance officer; conducting training; and maintaining certain records. When operators of these VASPs violate the BSA or neglect regulatory requirements, such as failing to establish effective AML programs or report suspicious activities, their actions present a vulnerability to the financial system. Other financial institutions may offer services that trigger other AML/CFT regulatory obligations, such as those for securities-related businesses, and that can present similar risks if they fail to comply.

The number of users and market capitalization of virtual assets have risen sharply since the 2018 NMLRA, and virtual assets are being increasingly incorporated into services provided by the traditional financial sector. While VASPs based or operating in the United States have increased in number, the proportion of virtual assets transferred without VASPs and through P2P payments have likely increased substantially due to the growth of decentralized finance (DeFi) (see below) after remaining largely stable through 2020. Additionally, as of mid-2020, over half of mined bitcoin was held in addresses associated with VASPs, and over 87 percent had passed through a VASP at some point.[214] There has also been increasing adoption of virtual assets-related products or services by long-established or traditional financial service providers, including banks, credit card providers, and non-VASP MSBs, often in partnership with VASPs.

While the use of virtual assets for money laundering remains far below that of fiat currency and more traditional methods, as noted below, U.S. law enforcement agencies have detected an increase in the use of virtual assets to pay for online drugs[215] or to launder the proceeds of drug trafficking, fraud, and cybercrime, including ransomware attacks (see previous sections on threats), as well as other criminal activity, including sanctions evasion. In addition, a large number of VASPs operating abroad have substantially deficient AML programs, particularly in jurisdictions where international AML/CFT standards for VASPs are not effectively implemented, which affects the U.S. financial system. This is often the case, for instance, with VASPs that process ransomware-related payments which originated in the United States. Uneven and often inadequate regulation and supervision internationally allow VASPs and illicit cyber actors to engage in regulatory arbitrage and expose the U.S. financial system to risk from jurisdictions where regulatory standards and enforcement are less robust. While regulatory arbitrage is a problem with all financial services, it is of particular concern with VASPs given the ability to transfer virtual assets across borders nearly instantaneously. This could potentially expose the U.S. financial system to VASPs with deficient or nonexistent AML/CFT controls operating abroad. In some instances, noncompliant VASPs may operate as nested exchanges[216] to benefit from the liquidity and convenience offered by larger market players. However, VASPs doing business wholly or in substantial part in the United States generally have obligations under the BSA regardless of the jurisdiction in which they are located.[217]

Financial fraudsters and money launderers are increasingly seeking to evade AML/CFT controls by engaging in P2P transactions. The use of wallets not hosted by any financial institution or VASP is commonly referred to as

214 Chainalysis, "60% of Bitcoin is Held Long Term as Digital Gold. What About the Rest?" (Jun. 18, 2020), https://blog.chainalysis.com/reports/bitcoin-market-data-exchanges-trading.

215 DOJ, "International Law Enforcement Operation Targeting Opioid Traffickers on the Darknet Results in 150 Arrests Worldwide and the Seizure of Weapons, Drugs, and over $31 Million," (Oct. 26, 2021), https://www.justice.gov/opa/pr/international-law-enforcement-operation-targeting-opioid-traffickers-darknet-results-150.

216 A nested relationship is where a VASP holds an account at another VASP, often providing accounts to smaller VASPs for access to liquidity and trading pairs. See FATF, *Updated Guidance for a Risk Based Approach Virtual Assets and Virtual Assets Providers,* (October 2021), https://www.fatf-gafi.org/media/fatf/documents/recommendations/Updated-Guidance-VA-VASP.pdf, p.55.

217 31 CFR 1010.100(ff).

an "unhosted" or "self-hosted" wallet.[218] Users of unhosted wallets can retain custody and transfer their virtual assets without the involvement of a regulated financial institution, and these unhosted wallet transfers of virtual assets are often referred to as P2P transactions. Because unhosted wallet users can transact without involving any financial services provider, many of the most important obligations of the U.S. AML/CFT regime applicable to financial institutions may not apply. This can limit authorities' collection of and access to information and reduce the effectiveness of preventive measures by financial institutions. At the same time, P2P transfers of virtual assets may provide increased transparency of certain information when occurring on public blockchains, as investigators can use blockchain analytics software to trace these transactions.

P2P service providers, typically natural persons engaged in the business of buying and selling virtual assets, may have different regulatory requirements depending on their precise business model, and many P2P exchange providers act as money transmitters under the BSA.[219] However, some of these providers have insufficient compliance programs to mitigate the risk of criminal abuse; others are intentionally operating in a manner to facilitate the exchange of illicit proceeds. For example, money mules are increasingly using unhosted wallets and P2P service providers to convert between fiat currency and virtual assets and to rapidly disburse illicit funds.

DeFi refers to a class of virtual asset protocols and platforms, some of which allow for automated P2P transactions without the need for an account or custodial relationship and often through the use of smart contacts.[220] These protocols and platforms are open to anyone to use and provide an alternative to traditional financial intermediaries like banks or brokerages, as well as VASPs operating as exchangers. Recent law enforcement investigations involving virtual assets have uncovered chain hopping (moving assets from one blockchain network to another via an exchange, swap, or "wrapped" asset), and some of this activity has involved the use of smart contracts and other DeFi services. DeFi services often involve no AML/CFT or other processes to identify customers, allowing layering or proceeds to take place instantaneously and pseudonymously. Even though many of these transactions are recorded on public blockchains the publicly available information generally does not identify the owners of the transacting wallets and the identity of those owners can only be established with additional information. While some DeFi services purport to run autonomously without the support of a central company, group, or person, many have a controlling organization—through a decentralized autonomous organization, concentrated ownership or governance rights, or otherwise—which provides a measure of centralized administration or governance.

218 Under a Notice of Proposed Rulemaking (NPRM), banks and MSBs would be required to submit reports, keep records, and verify the identity of customers in relation to transactions above certain thresholds involving CVC/Legal Tender Digital Assets (LTDA) wallets not hosted by a financial institution ("unhosted wallets") or CVC/LTDA wallets hosted by a financial institution in certain jurisdictions identified by FinCEN. See "FinCEN Extends Reopened Comment Period for Proposed Rulemaking on Certain Convertible Virtual Currency and Digital Asset Transactions," https://www.fincen.gov/news/news-releases/fincen-extends-reopened-comment-period-proposed-rulemaking-certain-convertible.

219 FinCEN, "FinCEN Guidance," (May 9, 2019), https://www.fincen.gov/sites/default/files/2019-05/FinCEN%20Guidance%20CVC%20FINAL%20508.pdf.

220 FinCEN, *Ransomware* Trends.

**Case examples**

- In June 2021, a Texas-based man known as "Doctor Bitcoin" pled guilty to illegally operating a cash-to-virtual asset conversion business. In just one scheme spanning almost one year, he conducted 37 transactions with a customer whose money stemmed from a Nigerian lottery scam, converting between $550,000 and $1.5 million to virtual assets. Doctor Bitcoin promised not to get involved in the details of this customer's business dealings, advised on how to circumvent financial institution reporting requirements by keeping deposits under $9,500, collected fees for his services, and failed to verify the source of cash. He also registered as a marketing agency so his customers could describe the payments as marketing consulting fees to avoid suspicious activity filing requirements. The defendant admitted he was not licensed to engage in the business of transmitting money within the states where he practiced, nor was he registered as a money transmitting business with Treasury.[221]
- In August 2021, FinCEN and the CFTC announced a $100 million civil money penalty (CMP) assessed against Bitcoin Mercantile Exchange, or "BitMEX," a purportedly "offshore" VASP. The platform, located in the Seychelles, was found to permit U.S. customers onto its platform despite claims to the contrary. Ultimately, it was found that BitMEX failed to register with the CFTC and to willfully violate its U.S. AML obligations under the BSA.[222] BitMEX's owners have also been indicted on charges of willfully failing to establish, implement, and maintain an adequate AML program.[223]

## 1. Virtual Asset Service Provider Registration and Compliance Obligations

When VASPs fail to register as MSBs with FinCEN or do not implement sufficient AML controls, such as filing SARs or keeping certain records, criminals are more likely to exploit those VASPs without detection. Businesses that provide virtual asset services that are required to, but fail to, register with federal functional regulators such as the CFTC or SEC create similar vulnerabilities.

There are identified cases of VASPs that are based in or operate wholly or in substantial part in the United States which may fail to register as MSBs and implement the requisite AML programs for the services they provide. Whether through willful blindness or reckless disregard, this lack of compliance represents a significant risk to the U.S. financial system. To clarify the compliance obligations for CVCs, FinCEN issued interpretive guidance in 2013 and 2019 regarding the application of FinCEN's regulations to these types of assets and related business models. FinCEN has also taken enforcement actions against noncompliant MSBs.[224]

Law enforcement has also observed criminals, including drug dealers and credit card fraud schemers, using virtual asset kiosks, sometimes referred to as bitcoin ATMs.[225] Virtual asset kiosks are stand-alone machines that allow users to convert fiat currency to and from virtual assets and can serve as an easy-to-use physical access point for purchasing, transferring, or cashing out virtual assets. While virtual asset kiosks operators are considered MSBs

221 DOJ, "'Doctor Bitcoin' Pleads Guilty to Illegal Cash-to-Crypto Scheme," (Jun. 29, 2021), https://www.justice.gov/usao-ndtx/pr/doctor-bitcoin-pleads-guilty-illegal-cash-crypto-scheme.

222 In the matter HDR Global Trading Limited, 100x Holdings Limited, ABS Global Trading Limited, Shine Effort Inc. Limited, and HDR Global Services (Bermuda) Limited d/b/a BitMEX, Assessment of Civil Money Penalty Number 2021-02, Financial Crimes Enforcement Network, Aug. 10, 2021; and *Commodity Futures Trading Commission v. HDR Global Trading Limited et.al.,* 1:20-cv-08132, (S.D. NY, Aug. 10, 2021).

223 DOJ, "Founders And Executives Of Off-Shore Cryptocurrency Derivatives Exchange Charged With Violation Of The Bank Secrecy Act," (Oct. 1, 2020), https://www.justice.gov/usao-sdny/pr/founders-and-executives-shore-cryptocurrency-derivatives-exchange-charged-violation.

224 FinCEN, Guidance, "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%20Guidance%20CVC%20FINAL%20508.pdf.

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

in the United States and are required to comply with MSB AML/CFT obligations, some kiosk operators fail to do so, enabling criminals to purchase virtual assets anonymously or launder illicit proceeds in exchange for higher transaction fees than other virtual asset service providers.[226] Additionally, criminals have directed victims of impersonation schemes, romance schemes, and lottery schemes to make payments through virtual asset kiosks.[227]

Additionally, OFAC, in 2021, issued a brochure on sanctions compliance guidance for virtual currency[228] (a subset of virtual assets) clarifying that OFAC sanctions compliance obligations apply equally to transactions involving virtual assets and those involving traditional fiat currencies. Members of the virtual asset industry are responsible for ensuring that they do not engage, directly or indirectly, in transactions prohibited by OFAC sanctions, such as dealings with blocked persons or property, or engage in prohibited trade- or investment-related transactions. All companies in the virtual asset industry are encouraged to develop, implement, and routinely update a tailored, risk-based sanctions compliance program. OFAC has authority to impose civil penalties for failures to adhere to OFAC sanctions requirements. The brochure complements OFAC's frequently asked questions on virtual currency[229] as well as its updated advisory highlighting the sanctions risk associated with ransomware payments and "mitigating factors" in any related enforcement action.[230]

Other agencies have also acted to clarify and enforce their regulatory frameworks. For instance, the SEC has brought enforcement actions against a number of individuals and entities operating without the required registrations.[231]

### Case examples

- In May 2021, Kais Mohammad was sentenced for operating Herocoin, an illegal virtual asset MSB that exchanged up to $25 million, including on behalf of criminals, through in-person transactions and a network of bitcoin ATM-type kiosks.[232] As part of his business, he offered bitcoin-cash exchange services, charging commissions of up to 25 percent, significantly above the prevailing market rate; processed virtual assets deposited into the machines; supplied the machines with cash that customers would withdraw; and maintained the server software that operated the machines. Mohammad intentionally failed to register his company with FinCEN and consciously chose not to develop and maintain an effective AML program, file required CTRs, conduct due diligence on customers, and file required SARs.[233]

---

226 DOJ, "Westwood Man Agrees to Plead Guilty to Federal Narcotics, Money Laundering Charges for Running Unlicensed Bitcoin Exchange and ATM," (Aug. 23, 2019), https://www.justice.gov/usao-cdca/pr/westwood-man-agrees-plead-guilty-federal-narcotics-money-laundering-charges-running.

227 FBI, "The FBI Warns of Fraudulent Schemes Leveraging Cryptocurrency ATMs and QR Codes to Facilitate Payment," (Nov. 4, 2021), https://www.ic3.gov/Media/Y2021/PSA211104.

228 Treasury, *Sanctions Compliance Guidance for the Virtual Currency Industry.* (October 2021), https://home.treasury.gov/system/files/126/virtual_currency_guidance_brochure.pdf.

229 Treasury, "Frequently Asked Questions: Questions on Virtual Currency," (updated Oct. 15, 2021), https://home.treasury.gov/policy-issues/financial-sanctions/faqs/topic/1626.

230 Treasury, "Updated Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments," (Sep. 21, 2021), https://home.treasury.gov/system/files/126/ofac_ransomware_advisory.pdf.

231 SEC, "SEC Charges Poloniex for Operating Unregistered Digital Asset Exchange," (Aug. 9, 2021), https://www.sec.gov/news/press-release/2021-147. Other SEC virtual asset-related enforcement actions can be found here: https://www.sec.gov/spotlight/cybersecurity-enforcement-actions.

232 DOJ, "Yorba Linda Man Sentenced to 2 Years in Prison for Operating Illegal ATM Network that Laundered Bitcoin and Cash for Criminals," (May 28, 2021), https://www.justice.gov/usao-cdca/pr/yorba-linda-man-sentenced-2-years-prison-operating-illegal-atm-network-laundered.

233 DOJ, "O.C. Man Admits Operating Unlicensed ATM Network that Laundered Millions of Dollars of Bitcoin and Cash for Criminals' Benefit," (Jul. 22, 2020), https://www.justice.gov/usao-cdca/pr/oc-man-admits-operating-unlicensed-atm-network-laundered-millions-dollars-bitcoin-and.

- In 2021, OFAC entered into a $507,000 settlement agreement with a U.S. virtual asset payment service provider for processing virtual asset transactions between the company's customers and persons located in sanctioned jurisdictions. While the company's sanctions compliance controls included screening its direct customers and merchants in the United States and elsewhere for a potential nexus to sanctions, the company failed to screen available information about the individuals who used its payment processing platform to buy products from those merchants. Specifically, prior to effecting transactions, the company received information about some of the buyers, such as names, addresses, telephone numbers, email addresses, and, at times, IP addresses.[234]

## 2. Anonymity-Enhanced Cryptocurrencies and Service Providers

Another growing trend is criminals' use of anonymity-enhancement technologies, such as enhanced cryptography or operation on an opaque blockchain, in the virtual asset sector. These are assets, such as AECs, or services, such as mixers or tumblers, that help criminals hide the movement or origin of funds, creating additional obstacles for investigators.

Anonymity-enhancement technologies create challenges for investigators attempting to trace illicit proceeds. For example, some virtual assets and VASPs operate on public, transparent blockchains, where pseudonymous user and transaction information can be viewed and sometimes paired with other pieces of information that can enable regulators and law enforcement to identify transaction participants. However, law enforcement has observed illicit actors showing an interest in the use of virtual assets and services specifically designed to obscure transactional activity and limit transparency, such as AECs, mixers, and tumblers.

The virtual asset Monero, for example, 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. These transactions are not broadcast publicly on the Monero blockchain. Instead, they use one-time generated addresses to conceal both the sender and beneficiary to external entities. With every new transaction, ring signatures obfuscate the origin of the funds by mixing values with a minimum number of other transactors, creating challenges for investigators tracing illicit funds such as ransomware proceeds.

Criminals may also try to identify noncompliant VASPs that specialize in obfuscating a virtual asset's origin. Providers of anonymizing services, such as mixers or tumblers, are generally providers of software platforms that accept virtual assets and retransmit them in a manner that anonymizes the original source. While these services may operate as money transmitters and thus have obligations under the BSA, they may deliberately operate in a noncompliant manner to make it more difficult for regulators and law enforcement to trace illicit funds.

### Case examples

- In October 2020, FinCEN assessed a $60 million CMP against Larry Harmon, the owner and operator of Helix, a virtual asset mixer, or tumbler, for operating as an unregistered MSB, failure to implement an AML program, and failure to file SARs from 2014 to 2020. FinCEN's investigation revealed that from June 2014 through December 2017, Helix conducted over 1.2 million transactions for its customers while failing to collect and verify customer names, addresses, and other identifiers on these transactions and was associated with virtual asset wallet addresses that sent or received over $311 million. Coin Ninja, which operated as an unregistered MSB, was operated in the same manner as Helix and failed to register with FinCEN.[235] In 2021, Harmon pleaded guilty to a money laundering conspiracy arising from his operation of Helix, admitting that he conspired with darknet

234 Treasury, "OFAC Enters Into $507,375 Settlement with BitPay, Inc. for Apparent Violations of Multiple Sanctions Programs Related to Digital Currency Transactions," (Feb. 18, 2021), https://home.treasury.gov/system/files/126/20210218_bp.pdf.

235 FinCEN, "First Bitcoin "Mixer" Penalized by FinCEN for Violating Anti-Money Laundering Laws," (Oct. 19, 2020), https://www.fincen.gov/news/news-releases/first-bitcoin-mixer-penalized-fincen-violating-anti-money-laundering-laws.

vendors to launder bitcoin generated through drug trafficking and other illegal activities.[236]

## COMPLICIT MERCHANTS AND PROFESSIONALS

As highlighted in the 2018 NMLRA, criminals seek out complicit merchants, professionals, and financial services employees to help effectuate their money laundering schemes. Law enforcement continues its focus on complicit professionals who abuse their professional position to aid criminals (as well as themselves), through cases involving prosecutions of merchants facilitating TBML, as well as attorneys, real estate agents, and financial services employees, among others.

### 1. Merchants

- In February 2019, four men and two women were found guilty for their roles in a two-year multi-million-dollar BMPE money laundering scheme. These individuals were part of a complex money laundering scheme whereby money derived from the sale of drugs in the United States was laundered through businesses in Laredo, Texas, to return these proceeds to Mexican drug dealers. The drug money was distributed among downtown Laredo perfume stores, and the owners accepted loose bulk cash, even after being told it was "narco dinero." The store owners also failed to file Form 8300s or filed Form 8300s which omitted pertinent information such as the name of the courier who brought the bulk cash.[237]
- In early 2018, the IRS seized over $4 million from bank accounts controlled by the owner of a company that provided helicopter services. The seized funds were proceeds attributed to wire fraud stemming from fraudulent helicopter lease payments. The owner engaged in a scheme that transferred millions of dollars between bank accounts of shell companies controlled by the same group of individuals, who were officers for the helicopter company, and the income derived by these officers and subsidiaries came from the leasing of unairworthy aircraft that were not in compliance with Federal Aviation Administration regulations. Evidence indicated that the owner and his various shell corporations generated approximately $20 million a year from the fraudulent leasing of helicopters.[238]

### 2. Attorneys

Attorneys in the United States provide a wide variety of services. Attorneys are licensed by state bar associations and are bound by professional codes of ethics. Some maintain bank accounts in their own name for client use (mostly escrow accounts in which clients' funds are held for future transactions). Others act in an advisory capacity and may handle funds associated with settlement checks or trusts that they administer on behalf of their clients, while others may work on behalf of large corporations. Attorneys are not subject to comprehensive AML/CFT measures. Attorneys are obligated to file Form 8300 for cash transactions exceeding $10,000 and may choose to use a Form 8300 under certain circumstances for cash transactions less than $10,000. While attorneys have strong professional entry and continuing ethical requirements, these may not adequately address ML/TF vulnerabilities

236 DOJ, "Ohio Resident Pleads Guilty to Operating Darknet-Based Bitcoin 'Mixer' That Laundered Over $300 Million," (Aug. 18, 2021), https://www.justice.gov/opa/pr/ohio-resident-pleads-guilty-operating-darknet-based-bitcoin-mixer-laundered-over-300-million.

237 DOJ, "Six Convicted for Roles in Multi-Million Dollar Black Market Peso Exchange Money-Laundering Scheme," (Feb. 12, 2019), https://www.justice.gov/opa/pr/six-convicted-roles-multi-million-dollar-black-market-peso-exchange-money-laundering-scheme.

238 FBI, "Four Executives of Guam Based Hansen Helicopters Charged in Alleged Conspiracy to Defraud the FAA and Related Charges," (May 31, 2018), https://www.fbi.gov/contact-us/field-offices/honolulu/news/press-releases/four-executives-of-guam-based-hansen-helicopters-charged-in-alleged-conspiracy-to-defraud-the-faa-and-related-charges. See also *United States v. John D. Walker et al.*, 1:18-cr-00010.

and do not require reporting of suspicious activity to authorities.[239] In addition, there is no enforceable mechanism to compel attorneys to follow voluntary best practices guidelines nor any mechanisms which would result in the issuance of civil or criminal penalties for failing to comply with these practices.

- In August 2021, an attorney was sentenced for money laundering, wire fraud, and bank fraud charges for a scheme involving the use of a trust account. According to the indictment, the lawyer, while serving in her official capacity providing services to clients, transferred unearned money from her client's trust account to her business and personal account where she then used the money for her own use.[240]
- In December 2020, an attorney was charged with money laundering for his role in facilitating the financial operations of a narcotics trafficking organization. According to the criminal complaint, the attorney received payments from the traffickers to launder narcotics proceeds as well as to make payments to other individuals involved in the scheme. The attorney allegedly used the law firm's bank accounts to receive funds originating from narcotics proceeds via wire transfers, checks, credit card payments, and mobile payment apps. In some instances, the attorney collected cash. After receiving these funds, the attorney allegedly used these funds to pay for his legal fees. Additionally, the attorney is alleged to have instructed members of the organization to establish cash-intensive businesses to launder funds to disguise the origin of illicit proceeds. Many of the payments received by the law firm were allegedly concealed by deliberately foregoing the use of receipts or other documentation to record transactions.[241]
- In April 2020, a Texas attorney was charged for his involvement in a scheme to launder probable narcotics proceeds. According to the criminal complaint, the attorney was introduced as a known money launderer by a high-level opioids dealer to an undercover DEA agent posing as someone involved in the narcotics trade. The undercover DEA agent approached the lawyer and told him he would need to launder $500,000 a month and that the money came from narcotics proceeds. The lawyer allegedly agreed to launder the proceeds and provided advice to the undercover agent to facilitate the scheme, to include directing them to set up a shell company or a cash business such as a laundromat or a car wash. The lawyer later came to take several cash deliveries from the undercover agent presented as narcotics proceeds in exchange for a fee before later delivering the laundered proceeds to the undercover DEA accounts via the attorney's law firm's bank account.[242]

### 3. Real Estate Professionals

- In February 2021, a real estate attorney in Kentucky pleaded guilty to money laundering charges for purchasing real estate with the intention of using the purchases to disguise the proceeds of illegal sports betting. The attorney conspired with another individual engaged in illegal betting to disguise the illicit proceeds through investments in commercial real estate. As part of the scheme, the attorney used funds which he knew were derived from illegal betting to purchase companies that held real estate properties. When purchasing these properties, the attorney deliberately concealed the involvement and ownership of the individual involved in illegal gambling.[243]

---

239 FATF, *Mutual Evaluation of the United States*, (2016), https://www.fatf-gafi.org/publications/mutualevaluations/documents/mer-united-states-2016.html, p. 10.

240 DOJ, "Former South Dakota Attorney Sentenced for Wire Fraud, Money Laundering, and Bank Fraud," (Aug. 5, 2021), https://www.justice.gov/usao-sd/pr/former-south-dakota-attorney-sentenced-wire-fraud-money-laundering-and-bank-fraud.

241 DOJ, "Federal Superseding Indictment Charges Two Baltimore Defense Attorneys and Private Investigator for Conspiracy to Create False Records in a Federal Investigation and to Obstruct Official Proceedings," (Dec. 18, 2020), https://www.justice.gov/usao-md/pr/federal-superseding-indictment-charges-two-baltimore-defense-attorneys-and-private.

242 IRS, "Dallas attorney charged in narcotics money laundering scheme," (Apr. 16, 2021), https://www.irs.gov/compliance/criminal-investigation/dallas-attorney-charged-in-narcotics-money-laundering-scheme.

243 IRS, "Bowling Green attorney pleads guilty to laundering over $700,000 of illegal proceeds," (Feb. 27, 2020), https://www.irs.gov/compliance/criminal-investigation/bowling-green-attorney-pleads-guilty-to-laundering-over-700000-of-illegal-proceeds.

- In December 2018, a California real estate broker was indicted on money laundering charges for allegedly purchasing residential real estate on behalf of individuals who sought to acquire properties to cultivate marijuana. According to the indictment, these individuals allegedly received funds from China for down payments on residential properties. Once the funds were in the United States, they were aggregated to make the down payment on a property to facilitate its ultimate purchase organized by the real estate broker. To avoid detection by financial institutions and lenders, the real estate broker is said to have used hard money lenders to arrange financing for the property purchases.[244] In some instances, the broker allegedly used her real estate firm to provide loans to the home purchasers to ultimately ensure the transaction closed and her clients could purchase the homes.[245]

### 4. Financial Services Employees

- In April 2019, Standard Chartered Bank (SCB) agreed to the forfeiture of $240 million, a fine of $480 million, and the amendment and extension of its DPA with the DOJ for an additional two years for conspiring to violate the International Emergency Economic Powers Act (IEEPA). As part of the amended DPA, SCB admitted that, from 2007 through 2011, two former employees of its branch in Dubai willfully conspired to help Iran-connected customers conduct U.S. dollar transactions through the U.S. financial system for the benefit of Iranian individuals and entities.[246]
- In November 2018, Ng Chong Hwa, also known as Roger Ng, was charged with conspiring to launder billions of dollars embezzled from 1Malaysia Development Berhad (1MDB), Malaysia's investment development fund, and conspiring to violate the FCPA by paying bribes to various Malaysian and Abu Dhabi officials. Ng was also charged with conspiring to violate the FCPA by circumventing the internal accounting controls of The Goldman Sachs Group, Inc., which underwrote more than $6 billion in bonds issued by 1MDB in three separate bond offerings in 2012 and 2013, while Ng was employed as a managing director. Tim Leissner, the former Southeast Asia Chairman and participating managing director of Goldman Sachs, also pled guilty to a two-count criminal information charging him with conspiring to launder money and conspiring to violate the FCPA by both paying bribes to various Malaysian and Abu Dhabi officials and circumventing the internal accounting controls of Goldman Sachs. Leissner was ordered to forfeit $43.7 million as a result of his crimes. As alleged in court filings, between approximately 2009 and 2014, as 1MDB raised money to fund its projects, billions of dollars were misappropriated and fraudulently diverted from 1MDB, including funds 1MDB raised in 2012 and 2013 through three bond transactions that it executed with Goldman Sachs. As part of the scheme, and as alleged in court filings, Low Taek Jho, Ng, Leissner, and others conspired to bribe government officials in Malaysia, including at 1MDB, and Abu Dhabi to obtain and retain lucrative business for Goldman Sachs, including the 2012 and 2013 bond deals. They also allegedly conspired to launder the proceeds of their criminal conduct through the U.S. financial system by purchasing, among other things, luxury residential real estate in New York City and elsewhere and artwork from a New York-based auction house and by funding major Hollywood films.[247]

---

244 A hard money lender is a private lender that charges higher interest rates and fees than traditional lenders and that has no AML/CFT reporting obligations under U.S. law.

245 DOJ, "Sacramento Real Estate Broker Indicted for International Money Laundering Conspiracy Funding Residential Marijuana Grows with Wires from China," (Dec. 20, 2018), https://www.justice.gov/usao-edca/pr/sacramento-real-estate-broker-indicted-international-money-laundering-conspiracy.

246 DOJ, "Standard Chartered Bank Admits to Illegally Processing Transactions in Violation of Iranian Sanctions and Agrees to Pay More Than $1 Billion," (Apr. 9, 2019), https://www.justice.gov/opa/pr/standard-chartered-bank-admits-illegally-processing-transactions-violation-iranian-sanctions.

247 DOJ, "Malaysian Financier Low Taek Jho, Also Known As "Jho Low," and Former Banker Ng Chong Hwa, Also Known As 'Roger Ng,' Indicted for Conspiring to Launder Billions of Dollars in Illegal Proceeds and to Pay Hundreds of Millions of Dollars in Bribes," (Nov. 1, 2018), https://www.justice.gov/opa/pr/malaysian-financier-low-taek-jho-also-known-jho-low-and-former-banker-ng-chong-hwa-also-known.

## Compliance Deficiencies

While many regulated U.S. financial institutions have adequate AML programs, compliance deficiencies at these institutions continue to be a money laundering vulnerability, particularly in light of the size and global reach of the industry. There are more than 11,000 depository institutions (4,917 FDIC-insured banks[248] and 5,099 federally insured credit unions[249]), more than 29,000 MSBs registered with FinCEN,[250] more than 3,400 active broker-dealers registered with the SEC,[251] and approximately 1,000 casinos in the United States.[252]

### 1. Banks

The annual number of BSA/AML enforcement actions taken by federal regulators has fluctuated over the last half decade. For certain formal enforcement actions (e.g., cease-and-desist orders) related to BSA/AML, the federal banking agencies (FBAs) take action based on (1) failure to establish and maintain a reasonably designed BSA compliance program or (2) failure to correct a previously reported problem with the BSA/AML compliance program. This supervisory approach is reflected in the FBAs' August 2020 updated joint statement on the enforcement of BSA/AML requirements, describing circumstances in which an agency is required by law to issue a mandatory cease-and-desist order to address noncompliance.[253] Additionally, in August 2020, FinCEN issued a statement to provide clarity and transparency to its approach when contemplating compliance or enforcement actions against covered financial institutions that violate the BSA.[254] The DOJ also takes action against banks for AML program failures and other BSA violations, as noted in the case examples.

Many of the cases cited below, which have occurred since the 2018 NMLRA, illustrate a focus by supervisors on financial institutions which did not remediate or correct noncompliance within a mandated timeframe. In 2019, the Office of the Comptroller of the Currency (OCC) observed that "BSA/AML-related deficiencies identified by the OCC stem from three primary causes: inadequate CDD and enhanced due diligence (EDD), insufficient customer risk identification, and ineffective processes related to suspicious activity monitoring and reporting, including the timeliness and accuracy of SAR filings. Talent acquisition and staff retention to manage BSA/AML compliance programs and associated operations present ongoing challenges, particularly at smaller regional and community banks."[255]

#### Case examples

- In December 2021, FinCEN announced that it has assessed an $8 million CMP on CommunityBank of Texas, N.A. (CBOT) for willful violations of the BSA and its implementing regulations. Specifically, CBOT admitted that it willfully failed to implement and maintain an effective AML program that was reasonably designed to guard against money laundering. CBOT also admitted that it willfully failed to report hundreds of suspicious transactions to FinCEN involving illegal financial activity by its customers and processed by, at, or through the

248 FDIC, "Key Statistics," (data as of Oct. 15, 2021—updated weekly) https://banks.data.fdic.gov/bankfind-suite/bankfind.

249 NCUA, "Industry at a Glance," (December 2020), https://www.ncua.gov/files/publications/analysis/industry-at-a-glance-december-2020.pdf.

250 FinCEN, "MSB Registrant Search," https://www.fincen.gov/msb-registrant-search.

251 FINRA, "Key FINRA Statistics for 2020," https://www.finra.org/media-center/statistics#key.

252 American Gaming Association, *State of the States 2020: The AGA Survey of the Commercial Casino Industry*, (June 2020), https://www.americangaming.org/wp-content/uploads/2020/06/AGA-2020-State_of_the_States.pdf.

253 FBAs, "Joint Statement on Enforcement of Bank Secrecy Act/Anti-Money Laundering Requirements," (Aug. 13, 2020), https://www.fdic.gov/news/press-releases/2020/pr20091a.pdf.

254 FinCEN, "Financial Crimes Enforcement Network (FinCEN) Statement on Enforcement of the Bank Secrecy Act," (Aug. 18, 2020), https://www.fincen.gov/sites/default/files/shared/FinCEN%20Enforcement%20Statement_FINAL%20508.pdf.

255 OCC, *Semiannual Risk Perspective*, (Spring 2019), https://www.occ.gov/publications-and-resources/publications/semiannual-risk-perspective/files/pub-semiannual-risk-perspective-spring-2019.pdf, p. 22.

bank even after the bank became aware that certain customers were subjects of criminal investigations. The violations occurred from at least 2015 through 2019 and caused millions of dollars in suspicious transactions to go unreported to FinCEN in a timely and accurate manner, including transactions connected to tax evasion, illegal gambling, money laundering, and other financial crimes.[256]

- In September 2021, the OCC issued a consent order to Washington Federal Bank, National Association, Seattle, Washington, directing the bank to pay a CMP of $2.5 million for BSA/AML compliance violations associated with its previously disclosed February 2018 consent order. The BSA violations included the failure to (1) adopt and implement an adequate BSA/AML compliance program, (2) file necessary SARs, (3) file necessary CTRs, and (4) include required information on transmittal orders.[257]
- In January 2021, FinCEN assessed a $390 million CMP against Capital One, National Association for willfully failing to implement and maintain an effective AML program, willfully failing to file thousands of SARs, and negligently failing to file thousands of CTRs with respect to a high-risk check cashing business unit.[258] The violations occurred from at least 2008 through 2014 and caused millions of dollars in suspicious transactions to go unreported in a timely and accurate manner, including proceeds connected to organized crime, tax evasion, fraud, and other financial crimes laundered through the bank into the U.S. financial system. In 2008, after Capital One acquired several other regional banks, Capital One established the Check Cashing Group as a business unit comprised of between approximately 90 and 150 check cashers in the New York and New Jersey area. During the course of establishing the Check Cashing Group and banking these customers, Capital One became aware of several compliance and money laundering risks associated with banking this particular group, including warnings by regulators, criminal charges against some of the customers, and internal assessments that ranked most of the customers among the bank's highest risk customers for money laundering. Despite the warnings and internal assessments, Capital One willfully failed to detect and report suspicious activity by this customer group, even when it had actual knowledge of criminal charges against specific customers, including Domenick Pucillo, a convicted associate of the Genovese organized crime family. In October 2018, the OCC assessed a $100 million CMP against Capital One for deficiencies in its BSA/AML program finding that the bank failed to achieve timely compliance with the OCC's 2015 consent order, as required, which cited weaknesses in its compliance program and related controls; deficiencies in its risk assessment, remote deposit capture and correspondent banking processes; and failing to file SARs.[259]
- In December 2020, Apple Bank for Savings agreed to pay a $12.5 million FDIC CMP for violations of the BSA and its implementing regulations between April 2014 and September 2018 and for failing to comply with a previous FDIC consent order in a timely manner (issued in 2015, terminated in 2020).[260] The 2015 consent order required the bank to enhance its BSA/AML compliance program by hiring qualified compliance staff, conducting an AML risk assessment, developing a system of internal controls, and remediating CDD and EDD deficiencies identified, among other things.[261]

256 FinCEN, "FinCEN Announces $8 Million Civil Money Penalty against CommunityBank of Texas, National Association for Violations of the Bank Secrecy Act," (Dec. 16, 2021), https://www.fincen.gov/news/news-releases/fincen-announces-8-million-civil-money-penalty-against-communitybank-texas.

257 OCC, Consent Order, "In the Matter of Washington Federal Bank, National Association Seattle, Washington," (Sep. 30, 2021), https://www.occ.gov/static/enforcement-actions/ea2021-040.pdf.

258 FinCEN, "FinCEN Announces $390,000,000 Enforcement Action Against Capital One, National Association for Violations of the Bank Secrecy Act," (Jan. 15, 2020), https://www.fincen.gov/news/news-releases/fincen-announces-390000000-enforcement-action-against-capital-one-national.

259 OCC, "OCC Assesses $100 Million Civil Money Penalty Against Capital One," (Oct. 23, 2018), https://www.occ.gov/news-issuances/news-releases/2018/nr-occ-2018-112.html.

260 FDIC, Order to Pay, "In the Matter of Apple Bank for Savings New York, New York," https://d6jxgaftxvagq.cloudfront.net/Uploads/l/a/v/applebankfdicordertopay_404717.pdf.

261 FDIC, Consent Order, "Apple Bank for Savings Manhasset, New York," https://d6jxgaftxvagq.cloudfront.net/Uploads/l/a/v/apple2015consentorder_614261.pdf.

- In October 2020, the OCC issued a consent order specifically prohibiting a BSA Officer from working in the banking industry.[262] The BSA Officer did not ensure the City National Bank of New Jersey had a BSA program able to manage its increased risk or that the bank conducted adequate due diligence on a recruited high-risk business. The BSA Officer also failed to appropriately monitor for and report suspicious activity and did not implement a due diligence program reasonably designed to detect and report known or suspected money laundering involving correspondent accounts in the United States held by foreign financial institutions. An additional seven members of this same bank management team and the board received either CMPs, personal cease-and-desist orders, or both.[263]
- In October 2020, the OCC assessed a $5 million CMP against First Abu Dhabi Bank, USA and terminated a prior 2017 consent order. Between 2016 to 2019, the U.S. branch of First Abu Dhabi Bank, USA failed to adopt and implement a compliance program that adequately covered the required BSA/AML program elements, and the bank failed to timely file SARs related to suspicious customer activity. Some critical deficiencies included a weak BSA officer function; insufficient staffing and training; systemic deficiencies in transaction monitoring systems and alert management processes, CDD, EDD, and customer risk rating processes; and failure to adopt and implement adequate due diligence programs for foreign correspondent accounts.[264]
- In April 2020, Industrial Bank of Korea (IBK) agreed to enter into a DPA with the DOJ in connection with a one-count felony information charging IBK with violating the BSA by willfully failing to establish, implement, and maintain an adequate AML program at IBK's New York branch (IBKNY). That failure permitted the processing of more than $1 billion in transactions in violation of IEEPA. Among other things, despite requests and admonitions from regulators and IBKNY's own compliance officer, IBK and IBKNY failed to provide the resources, staffing, and training necessary to maintain an adequate AML program by declining to take steps to implement an automated transaction review program or to provide the compliance officer with any support staff or assistance. IBKNY and IBK also failed to promptly identify a series of transactions that violated the United States' economic sanctions against Iran.[265]
- In March 2020, FinCEN announced it had assessed a $450,000 CMP against the former chief operational risk officer at U.S. Bank National Association (U.S. Bank) for his failure to prevent violations of the BSA during his tenure.[266] U.S. Bank used automated transaction monitoring software to spot potentially suspicious activity, but it improperly capped the number of alerts generated, limiting the ability of law enforcement to target criminal activity. Also, in March 2020, the OCC pursued a separate $50,000 penalty against the same individual.[267]
- In January 2020, the OCC issued a cease-and-desist order against M.Y. Safra Bank, FSB, New York, NY, for, among other things, opening accounts for virtual asset customers which consisted of virtual asset-related MSBs, without sufficient consideration of BSA/AML risks and failing to implement commensurate controls to address

262 OCC, Consent Order, "In the matter of David Monegro, Former Senior Vice President, Senior Compliance and Bank Secrecy Act Officer," (Oct. 13, 2020), https://www.occ.gov/static/enforcement-actions/ea2020-062.pdf.

263 OCC, "OCC Press Release 2020-122," (Sep. 17, 2020), https://www.occ.gov/news-issuances/news-releases/2020/nr-occ-2020-122.html.

264 OCC, Consent Order, "In the Matter of First Abu Dhabi Bank USA, N.V. Washington, D.C.," (2020), https://www.occ.gov/static/enforcement-actions/ea2020-060.pdf.

265 DOJ, "Manhattan U.S. Attorney Announces Criminal Charges Against Industrial Bank Of Korea For Violations Of The Bank Secrecy Act," ( Apr. 20, 2020), https://www.justice.gov/usao-sdny/pr/manhattan-us-attorney-announces-criminal-charges-against-industrial-bank-korea; DOJ, "Industrial Bank of Korea – Deferred Prosecution Agreement," (Apr 13, 2020), https://www.justice.gov/usao-sdny/press-release/file/1270016/download.

266 FinCEN, Assessment of Civil Money Penalty, "In the Matter of Michael LaFontaine," (Feb. 26, 2020), https://www.fincen.gov/sites/default/files/enforcement_action/2020-05-21/Michael%20LaFontaine-Assessment-02.26.20_508.pdf.

267 OCC, Consent Order, "In the Matter of Michael S. LaFontaine, Former Chief Operational Risk Officer," (Mar. 5, 2020), https://www.occ.gov/static/enforcement-actions/ea2020-011.pdf.

the increased risk.[268] The virtual asset customers included virtual asset exchanges, virtual asset ATM operators, virtual asset arbitrage trading accounts, blockchain developers and incubators, and fiat currency MSBs.

- In July 2019, the OCC announced it had issued a consent order and assessed a $50,000 CMP against the former general counsel for Rabobank. The consent order was issued in connection with violations of law and unsafe or unsound practices related to the bank's 2018 guilty plea to conspiring to obstruct an OCC examination and subsequent forfeiture of approximately $370 million and CMP of $50 million. The former general counsel was prohibited from participating in the affairs of any federally insured depository institution in the future.[269]
- In April 2018, the OCC announced it had assessed a $12.5 million CMP against Bank of China's New York branch for failing to adopt and implement a compliance program that adequately covered the required BSA/AML program elements, the requirements of OFAC, and the timely filing of SARs related to suspicious customer activity.[270]
- In February 2018, U.S. Bancorp agreed to enter into a DPA with the DOJ, pay a $528 million penalty, and continue reforms of its AML compliance program in connection with two felony violations of the BSA by its subsidiary, U.S. Bank, for willfully failing to have an adequate AML program and willfully failing to file a SAR.[271] Both the OCC and the Federal Reserve issued parallel enforcement actions against the firm, for $75 million and $15 million, respectively.[272] Additionally, FinCEN announced it had assessed a $185 million CMP against U.S. Bank for willful violations of several provisions of the BSA. Internal testing by U.S. Bank showed that alert capping caused it to fail to investigate and report thousands of suspicious transactions. U.S. Bank also allowed, and failed to monitor, noncustomers conducting millions of dollars of risky currency transfers at its branches through a large money transmitter.[273]
- In January 2018, the Federal Reserve announced it had ordered a cease-and-desist order and assessed a $29 million CMP against Mega International Commercial Bank, a Taiwanese bank, for violations of the BSA and its implementing regulations at several of its U.S. branch locations.[274]

## 2. Money Services Businesses

MSBs are frequently used by customers who would otherwise have difficulty in obtaining financial services, including many who are sending critically needed remittance payments abroad for purposes such as medical care and the education of loved ones. The United States is one of the largest sources of remittances for many

268 OCC, Consent Order, "In the Matter of M.Y. Safra Bank, FSB, New York, NY," (Jan. 30, 2020), https://www.occ.gov/static/enforcement-actions/ea2020-005.pdf.

269 OCC, "OCC Issues Consent Order of Prohibition and $50,000 Civil Money Penalty Against Former General Counsel of Rabobank N.A," (Jul. 29, 2019), https://www.occ.gov/news-issuances/news-releases/2019/nr-occ-2019-82.html; see also DOJ, "Rabobank NA Pleads Guilty, Agrees to Pay Over $360 Million," (Feb. 7, 2018), https://www.justice.gov/opa/pr/rabobank-na-pleads-guilty-agrees-pay-over-360-million.

270 OCC, Consent Order, "In the Matter of Bank of China, New York Branch, New York, NY," (Apr. 24, 2018), https://www.occ.gov/static/enforcement-actions/ea2018-035.pdf.

271 DOJ, "Manhattan U.S. Attorney Announces Criminal Charges Against U.S. Bancorp For Violations Of The Bank Secrecy Act," (Feb. 15, 2018), https://www.justice.gov/usao-sdny/pr/manhattan-us-attorney-announces-criminal-charges-against-us-bancorp-violations-bank.

272 Federal Reserve System, "Federal Reserve Board fines US Bancorp $15 million and orders it to improve risk management and oversight," (Feb. 15, 2018), https://www.federalreserve.gov/newsevents/pressreleases/enforcement20180215a.htm.

273 FinCEN, "FinCEN Penalizes U.S. Bank National Association for Violations of Anti-Money Laundering Laws," (Feb. 15, 2018), https://www.fincen.gov/news/news-releases/fincen-penalizes-us-bank-national-association-violations-anti-money-laundering.

274 Federal Reserve System, "Order to Cease and Desist and Order of Assessment of a Civil Money Penalty Issued Upon Consent, Pursuant to the Federal Deposit Insurance Act, as Amended," https://www.federalreserve.gov/newsevents/pressreleases/files/enf20180117a1.pdf.

developing economies worldwide, and the continued growth of the remittances market even in the midst of the COVID-19 pandemic demonstrates the importance of protecting these channels from abuse.

The U.S. government remains concerned about the risk that many MSBs, including VASPs, may not be compliant with one or more of their BSA obligations including those which are operating without required federal registration. At the federal level, IRS Small Business/Self-Employed (SB/SE) has been delegated by FinCEN to examine the AML program of MSBs.[275] A total of 49 out of 50 states also have separate licensing requirements and supervision mechanisms for MSBs. The United States continues to see cases of MSBs which operate without required registration or licensing and therefore fall outside state and federal AML/CFT regulation and supervision. In addition, the need to address noncompliant VASPs draws finite resources away from supervision and examination of other MSBs at the federal level. This limits the extent to which federal regulators and examiners can focus on enforcing compliance requirements for MSBs that are not VASPs. This is reflected in a decrease in FinCEN civil enforcement actions since 2017, as well as a decrease in principal exams regarding such entities. The number of money transfer principal exams by IRS SB/SE declined every year from 2018 through 2020. COVID-19 may also have played a role in the reduction of exams. The reduction in the federal examiner force, driven by budget constraints, has also contributed to this decline. The current examiner force is half of what it was in 2010, despite the existence of some 25,000 registered MSBs in the United States, along with hundreds of thousands of agents and a steadily rising volume of money transfer payments. The risk of unregistered MSBs following traditional business models, however, has likely not fallen as the examiner force has been reduced, and law enforcement continues to bring criminal charges against unlicensed MSBs. Specifically, elevated levels of activity in high-risk cross-border corridors, such as United States-China, are areas of concern, as are weak AML/CFT compliance practices in small MSB providers servicing international corridors in general.

### Case examples

- In April 2021, two individuals were indicted for failing to maintain AML controls and failing to file SARs and for operating an unlicensed money transmitting business that facilitated more than $1 billion in high-risk transactions. Between 2014 and 2016, the defendants devised and executed a scheme to bring lucrative and high-risk international financial business to small, unsophisticated financial institutions.[276]
- In March 2021, a black market money remitter pled guilty to money laundering. The money remitter laundered more than $500,000 in funds that had been represented to him to be the proceeds of a scheme to bribe Brazilian political officials, using a network and bank accounts to which he had access by virtue of his operation of an unlicensed money transmitting business.[277]
- In October 2020, the CEO of Surf Financial Group LLC pled guilty to conspiring with others to defraud shareholders of publicly traded companies, transmitting millions of dollars through the operation of an unlicensed MSB in California and falsifying multiple years of federal tax returns. Between 2017 and 2018, the CEO owned and operated an unlicensed money transmitting business as a means to transmit financial proceeds from foreign locations, including Hong Kong and the Bahamas, all of which disguised the source, origin, and control of such financial proceeds. In 2017, he entered into a business partnership with at least one co-conspirator who resided in Mexico and delivered dairy products for a living. To conceal his control over the MSB, the CEO directed the Mexican resident

275 31 C.F.R. § 1010.810. State regulators may also examine MSBs for compliance with certain BSA requirements, possibly including compliance with the AML program requirement, as elements of a more comprehensive list of requirements under state law.

276 DOJ, "Two Charged in High-Risk International Financial Scheme," (Apr. 14, 2021), https://www.justice.gov/opa/pr/two-charged-high-risk-international-financial-scheme.

277 DOJ, "Black Market Money Remitter Pleads Guilty In Manhattan Federal Court," (Mar. 16, 2021), https://www.justice.gov/usao-sdny/pr/black-market-money-remitter-pleads-guilty-manhattan-federal-court#:~:text=Jose%20Morely%20Chocron%20Laundered%20More,U.S.%20District%20Judge%20Jed%20S.

to fraudulently open a deposit account in his name at a financial institution in San Diego and to transmit funds as a nominee when directed.[278]

## 3. Securities Broker-Dealers

Broker-dealers are subject to a number of core AML regulations, including having an AML program, a customer identification program (CIP), CDD, CTR, and SAR rules, as well as record keeping requirements.[279] Recent enforcement actions against broker-dealers have included deficiencies in the areas of suspicious activity detection and reporting, customer identification programs, as well as AML program failures, including independent testing and ongoing training. Enforcement actions related to deficiencies in the detection and reporting of suspicious activity have included failures related to suspicious money movements and securities trading, including suspicious deposits and sales of low-priced securities and other suspicious trading that triggered red flags of market manipulation. The SEC staff has highlighted for broker-dealers the various risks arising from illicit activities associated with transaction in low-priced securities through omnibus accounts, particularly transactions effected on behalf of omnibus accounts maintained for foreign financial institutions.[280]

### Case examples

- In September 2021, the SEC settled charges against LPL Financial LLC for AML violations and for being a cause of certain antifraud violations by Eugenio Garcia Jimenez, Jr., an unregistered investment adviser not affiliated with LPL. LPL paid more than $4.8 million to resolve the matter. According to the SEC's order, Garcia opened an account at LPL to further his scheme to defraud his advisory client, the Municipality of Mayagüez, Puerto Rico (the "City"). The order found that, although required by LPL's CIP procedures, LPL did not verify certain identification documents before opening the account. Further, the order found that because LPL did not verify the purported customer address provided by Garcia—which differed from the registered address of Mayagüez Economic Development Inc. (MEDI) (the City's municipal corporation)—LPL could not comply with its obligation to accurately document its CIP procedures. Additionally, according to the SEC's order, even though LPL was in possession of suspicious and conflicting customer account information, LPL received assets transferred from a previous firm and processed wire transfers resulting in Garcia's further misappropriation of millions of dollars from MEDI.[281]
- In June 2021, the Financial Industry Regulatory Authority (FINRA) announced a settlement with Robinhood Financial LLC (Robinhood) totaling approximately $70 million for systemic supervisory failures and customer harm. As part of this settlement, FINRA stated that Robinhood failed, amongst a number of other violations, to have a reasonably designed CIP and that as a result the firm approved over 5.5 million new customer accounts between June 2016 and November 2018 while relying on a customer identification system that was largely automated and suffered from flaws. In all, Robinhood approved more than 90,000 accounts from June 2016 to November 2018 that had been flagged for potential fraud without further manual review.[282]
- In May 2021, the SEC announced settled charges against GWFS Equities Inc. (GWFS), a Colorado-based registered

278 DOJ, "CEO of Financial Firm Pleads Guilty to Running Multi-Million Dollar Securities and Tax Fraud Scheme, and Operating an Unlicensed Money Services Business," (Oct. 7, 2020), https://www.justice.gov/opa/pr/ceo-financial-firm-pleads-guilty-running-multi-million-dollar-securities-and-tax-fraud-scheme.

279 SEC, "Anti-Money Laundering (AML) Source Tool for Broker-Dealers, https://www.sec.gov/about/offices/ocie/amlsourcetool.htm.

280 SEC, "Staff Bulletin: Risk Associated with Omnibus Accounts Transacting in Low-Priced Securities," (Nov. 12, 2020), https://www.sec.gov/tm/risks-omnibus-accounts-transacting-low-priced-securities.

281 SEC, "LPL Financial Settles Charges Involving Violation of Anti-Money Laundering Rule," (Sep. 30, 2021), https://www.sec.gov/enforce/33-10992-s.

282 FINRA, "FINRA Orders Record Financial Penalties Against Robinhood Financial LLC," (Jun. 30, 2021), https://www.finra.org/media-center/newsreleases/2021/finra-orders-record-financial-penalties-against-robinhood-financial.

broker-dealer and affiliate of Great-West Life & Annuity Insurance Company, for violating the federal securities laws governing the filing of SARs. GWFS provides services to employer-sponsored retirement plans. The order found that GWFS failed to file approximately 130 SARs, including in cases when it had detected external bad actors gaining, or attempting to gain, access to the retirement accounts of participants in the employer-sponsored retirement plans it serviced. Further, for nearly 300 SARs that GWFS did file, the order found that GWFS did not include the "five essential elements" of information it knew and was required to report about the suspicious activity and suspicious actors, including cyber-related data such as URL and IP addresses.[283]

- In August 2020, the SEC, FINRA, and CFTC announced parallel settlements with Interactive Brokers LLC, a registered broker-dealer, for a total of $38 million in penalties paid to the three regulators. The firm's AML program was deficient in many respects, including that the firm failed to reasonably surveil certain money movements, failed to develop and implement reasonably designed surveillance tools for certain money movements and securities transactions, failed to reasonably investigate potentially suspicious activity, failed to file SARs, and had inadequate AML testing performed. As a result of these failures, Interactive Brokers did not reasonably surveil, detect, and report many instances of suspicious activity that were Ponzi schemes, market manipulation schemes, and other unlawful activity. For example, according to the SEC's order, over a one-year period, Interactive Brokers failed to file more than 150 SARs to flag potential manipulation of microcap securities in its customers' accounts, with some of the trading accounting for a significant portion of the daily volume in certain of the microcap issuers.[284]
- In October 2019, FINRA announced a settlement with BNP Paribas Securities Corp. and BNP Paribas Prime Brokerage (collectively BNP) in which BNP was fined $15 million for AML program and supervisory failures involving penny stock deposits and resales, and wire transfers. FINRA found that from February 2013 to March 2017, despite its penny stock activity, BNP did not develop and implement a written AML program that could reasonably be expected to detect and cause the reporting of potentially suspicious transactions. Until 2016, BNP's AML program did not include any surveillance targeting potential suspicious transactions involving penny stocks, even though BNP accepted the deposit of nearly 31 billion shares of penny stocks, worth hundreds of millions of dollars. During the same period, BNP processed more than 70,000 wire transfers with a total value of over $230 billion, including more than $2.5 billion sent in foreign currencies. BNP's AML program did not include any review of wire transfers conducted in foreign currencies and did not review wire transfers conducted in U.S. dollars to determine whether they involved high-risk entities or jurisdictions.[285]
- In December 2018, the DOJ entered into a DPA with Central States Capital Markets, LLC, a broker-dealer registered with the SEC, pursuant to which Central States was to forfeit $400,000. Central States failed to file SARs in connection with a series of transactions occurring in accounts at Central States owned by Scott Tucker.[286]
- In December 2018, FINRA announced a settlement with Morgan Stanley Smith Barney LLC (Morgan Stanley) in which Morgan Stanley was fined $10 million for AML program and supervisory failures. These failures included that Morgan Stanley's automated AML surveillance system did not receive critical data from several systems, undermining the firm's surveillance of tens of billions of dollars of wire and foreign currency transfers, including transfers to and from countries known for having high money laundering risk. Morgan Stanley also failed to devote sufficient resources to review alerts generated by its automated AML surveillance system, and consequently analysts often closed alerts without sufficiently conducting and/or documenting their

283 SEC, "SEC Charges Broker-Dealer for Failures Related to Filing Suspicious Activity Reports," (May 12, 2021), https://www.sec.gov/news/press-release/2021-82.

284 SEC, "SEC Charges Interactive Brokers With Repeatedly Failing to File Suspicious Activity Reports," (Aug. 10, 2020), https://www.sec.gov/news/press-release/2020-178.

285 FINRA, "FINRA Fines BNP Paribas Securities Corp. and BNP Paribas Prime Brokerage, Inc $15 million for AML Program and Supervisory Failures," (Oct. 24, 2019), https://www.finra.org/media-center/newsreleases/2019/finra-fines-bnp-paribas-securities-corp-and-bnp-paribas-prime.

286 SEC, Administrative Proceeding File No. 3-18940, (Dec. 19, 2019), https://www.sec.gov/litigation/admin/2018/34-84851.pdf.

investigations of potentially suspicious wire transfers. Morgan Stanley's AML Department did not reasonably monitor customers' deposits and trades in penny stock for potentially suspicious activity.[287]

- In December 2018, several regulators announced a settlement with UBS Financial Services (UBSFS) for willful violations of the BSA. UBFS agreed to pay a $5 million civil penalty to resolve the SEC's charges[288], and separately agreed to pay $10 million to FinCEN and FINRA to resolve parallel charges. From 2004 to 2017, UBSFS failed to implement an adequate AML program and failed to implement an adequate due diligence program for foreign correspondent accounts. UBSFS also failed to implement appropriate policies and procedures to ensure the detection and reporting of suspicious activity through all accounts.[289]
- In March 2018, the SEC announced a cease-and-desist order for Aegis Capital Corporation, a registered broker-dealer. From at least late 2012 through early 2014, Aegis failed to file SARs on hundreds of transactions when it knew, suspected, or had reason to suspect that the transactions involved the use of the broker-dealer to facilitate fraudulent activity or had no business or apparent lawful purpose.[290]
- In 2018, the SEC levied substantial AML penalties against Charles Schwab & Co. Inc. and TD Ameritrade Inc. for failing to file SARs on the suspicious transactions of independent investment advisers (IAs) that it terminated from using their platforms to custody client accounts. The firms failed to file SARs where they suspected or had reason to suspect that the terminated advisers had engaged in a range of suspicious transactions, including (1) transactions involving possible undisclosed self-dealing or conflicts of interest; (2) charging client accounts excessive advisory fees; (3) potentially fraudulent transactions in client accounts; (4) posing as a client to effect or confirm transactions in the client account; and (5) executing client trades and collecting advisory fees without being properly registered as an adviser.[291]

## 4. Casinos

The modern casino is an entertainment venue that offers its patrons highly regulated gaming.[292] To facilitate gaming activity, casinos ordinarily provide some financial services to their customers and are subject to comprehensive federal AML requirements.[293] The gaming environment is becoming increasingly complex for AML compliance with sports betting and online gaming legislation passing in more states each year. FinCEN has granted limited exceptive relief to casinos from certain customer identity verification requirements in the context of online gaming.[294]

Criminal prosecutions and enforcement actions show that illicit proceeds earned from drug trafficking, illegal gambling, and fraud are placed in casinos directly as cash. According to the DEA, casinos remain a popular way for

287 FINRA, "FINRA Fines Morgan Stanley $10 million for AML Program and Supervisory Failures," (Dec. 26, 2018), https://www.finra.org/media-center/news-releases/2018/finra-fines-morgan-stanley-10-million-aml-program-and-supervisory.

288 SEC, "SEC Charges UBS Financial Services Inc. with Anti-Money Laundering Violations," (Dec. 17, 2018), https://www.sec.gov/enforce/34-84828-s.

289 FinCEN, "FinCEN Assesses $14.5 Million Penalty against UBS Financial Services for Anti-Money Laundering Failures," (Dec. 17, 2018), https://www.fincen.gov/news/news-releases/fincen-assesses-145-million-penalty-against-ubs-financial-services-anti-money.

290 SEC, "https://www.sec.gov/litigation/admin/2018/34-82956.pdf.

291 SEC, "In the Matter of TD Ameritrade, Inc," (Sep. 24, 2018), https://www.sec.gov/litigation/admin/2018/34-84269.pdf.

292 American Gaming Association, "Best Practices for Anti-Money Laundering Compliance 2019–2020," https://www.americangaming.org/wp-content/uploads/2019/12/AGA-AML-Best-Practices_12-9.pdf.

293 The BSA regulatory requirements for casinos and card clubs include requirements for (1) an AML program: 31 CFR 1021.210, (2) currency transaction reporting: 31 CFR 1021.311, (3) suspicious activity reporting: 31 CFR 1021.320, and (4) record-keeping: 31 CFR1021.410.

294 FinCEN, "Exceptive Relief for Casinos from Certain Customer Identity Verification Requirements," (Oct. 19, 2021), https://www.fincen.gov/sites/default/files/2021-10/Casino%20Exceptive%20Relief%20101921_0.pdf.

launderers to obfuscate their drug proceeds because of their high volume of currency transactions.[295] A trend that law enforcement has seen is "chip walking." For example, in multiple jurisdictions, one target frequently gambled at a casino with cash from sex trafficking. The target took large sums of casino chips and left the casino in one city and drove to a casino in another city to play with those chips. The target did not cash out but left the casino again with large sums of chips he handed off to a second target at the casino.

According to FinCEN SAR filing insights, in terms of suspicious activity reported in 2019, minimal gaming with large transactions was the highest reported activity with more than 5,000 SARs reflecting this activity.[296] Reports of chip walking have dramatically increased since this was added to the SAR form in 2018, and it is now the second most selected suspicious activity on the SAR form, with more than 4,400 reports cited. The other frequently cited suspicious activities include transaction(s) below CTR threshold; unknown source of chips; two or more individuals working together; alters or cancels transaction to avoid CTR requirement; and suspicion concerns source of funds. Additional analysis of trends reported by casinos checking the "other" box on the SAR form includes reports of suspicious activity involving sports betting, abandoned jackpot, and bill stuffing. The top five SAR filings by state were Nevada, Louisiana, California, New Jersey, and Pennsylvania.[297]

### Case examples

- In November 2021, Bicycle Hotel & Casino in Bell Gardens, California, entered into a non-prosecution agreement (NPA) with DOJ, accepting responsibility for failing to properly file reports for a foreign national who conducted cash transactions of millions of dollars at the casino in 2016.[298] As part of the NPA, Bicycle admitted that a "high roller" Chinese national gambled at the casino approximately 100 times over an eight-month period in 2016, playing high-limit baccarat in a VIP room with huge sums of cash that on some occasions he transported to and from the casino in duffle bags. Bicycle staff informed senior management in July 2016 of the failure to file CTRs or SARS for Casinos in the high roller's name, according to the statement of facts. Bicycle then took various remedial actions.
- In March 2021, the California Department of Justice announced a settlement in which Artichoke Joe's Casino agreed to pay a penalty of $5.3 million for misleading state gambling regulators and violating the BSA. The casino failed to timely or accurately report an investigation by FinCEN, causing the California DOJ to initiate a license disciplinary proceeding against the casino and its owners. The penalties assessed in this settlement were in addition to the $5 million penalty imposed by FinCEN as part of a settlement in which the casino admitted violation of the BSA's program and reporting requirements. The violations included failing to implement and maintain an effective AML program and failing to report certain suspicious activity.[299]
- In 2019 the California Attorney General secured a more than $3 million settlement against Hawaiian Gardens Casino for misleading gambling regulators and violating federal laws intended to protect against money laundering.[300]

---

295 DEA NDTA, p. 87.

296 FinCEN, "Prepared Remarks of FinCEN Director Kenneth Blanco," (Aug. 13, 2019), https://www.fincen.gov/news/speeches/prepared-remarks-fincen-director-kenneth-blanco-delivered-12th-annual-las-vegas-anti.

297 Id.

298 DOJ, "Bicycle Casino Agrees to Pay $500,000 Settlement and Submit to Increased Review of Anti-Money Laundering Compliance Program," (Nov. 5, 2021), https://www.justice.gov/usao-cdca/pr/bicycle-casino-agrees-pay-500000-settlement-and-submit-increased-review-anti-money.

299 California DOJ, "California Department of Justice Secures $5.3 Million Settlement from Artichoke Joe's Casino," (Mar. 25, 2021), https://oag.ca.gov/news/press-releases/california-department-justice-secures-53-million-settlement-artichoke-joe%E2%80%99s.

300 California DOJ, "Attorney General Becerra Secures $3.1 Million Settlement from Hawaiian Gardens Casino," (Dec. 5, 2019), https://oag.ca.gov/news/press-releases/attorney-general-becerra-secures-31-million-settlement-hawaiian-gardens-casino.

## Luxury and High-Value Goods

### 1. Real Estate

Most purchases of real estate in the United States involve funds derived from legal means, and most purchases serve a legitimate purpose. However, certain types of real estate transactions are vulnerable to abuse by illicit actors seeking to launder criminal proceeds, including the proceeds of foreign corruption. High-risk real estate transactions include those involving the purchase of high-value property, the use of legal entities to conceal the ultimate owner, all-cash purchases, and the use of intermediaries who are not covered by AML obligations. FinCEN's regulations implementing the BSA require banks, non-bank residential mortgage lenders and originators, and housing-related government sponsored enterprises to establish AML programs and file SARs,[301] but FinCEN's regulations exempt other persons involved in real estate closings and settlements from the requirement to establish AML programs, and the regulations do not impose a SAR filing requirement on such persons.[302]

Given the relative stability of the real estate sector as a store of value, the opacity of the real estate market, and gaps in industry regulation, the U.S. real estate market continues to be used as a vehicle for money laundering and can involve businesses and professions that facilitate (even if unwittingly) acquisitions of real estate in the money laundering process. The real estate sector therefore represents a significant vulnerability that can facilitate money laundering schemes related to a wide range of crimes and sanctions evasion. The use of real estate in money laundering could also affect prices in certain real estate markets; when bad actors deliberately overpay for property, prices can rise, putting legitimate buyers and sellers at an economic disadvantage.

The purchase of real estate may also provide a reliable way for criminals to store or conceal illicit proceeds in an appreciating asset while also benefiting from greater opportunities for anonymity compared with other financial assets. This anonymity is particularly easy to achieve if buyers do not need a mortgage loan and purchase the property in the name of a legal entity, as there is no collection of information on the true buyer and limited or no AML/CFT safeguards. In an all-cash transaction, buyers can make purchases without a real estate agent, title insurance, financing through a financial institution or mortgage company, or an attorney to close the deal.[303] Moreover, other than a financing bank or mortgage originator, most of these intermediaries have very limited or no AML/CFT obligations.

These risks are compounded in transactions involving commercial real estate, as there are additional types of purchasing options and financing arrangements available for parties seeking to build or acquire property worth hundreds of millions of dollars.[304] Lawyers, accountants, and individuals in the private equity fields—all positions with minimal to no AML/CFT obligations under the BSA—typically facilitate commercial real estate transactions, often working at different stages of the deal and operating with differing amounts of beneficial ownership and financial information related to buyers and sellers. In commercial real estate, the use of purpose-built legal entities and indirect ownership chains is the norm as parties create tailored corporate entities to acquire or invest in a manner that limits their legal liability and financial exposure.[305] The result is an opaque field of diverse foreign

301 31 CFR parts 1020, 1029, 1030.

302 31 CFR 1010.205(b)(1)(v).

303 National Association of Realtors, "International Activity in U.S. Residential Real Estate Market Declines, According to Realtor® Survey," (Jul. 16, 2018), https://www.nar.realtor/newsroom/international-activity-in-us-residential-real-estate-market-declines-according-to-realtor-survey.

304 Congressional Research Service, *COVID-19 and the Future of Commercial Real Estate Finance*, (Oct. 19, 2020), https://sgp.fas.org/crs/misc/R46572.pdf.

305 Douglas E. Cornelius, Esq., and John P. O'Neill, Esq., *Closing Commercial Real Estate Transactions*, http://dougcornelius.com/files/closing_commercial_real_estate_transactions.pdf.

and U.S. domiciled legal entities associated with transactions worth hundreds of millions of dollars in the United States' most lucrative industries.

While there may be legitimate reasons for some buyers (e.g., celebrities and high-net-worth individuals) to use a legal entity, intermediary, or other means to seek privacy from the public in a real estate transaction, these vulnerabilities are extremely useful to illicit actors. At the same time, less sophisticated criminals seeking anonymity may also use less complicated nominees, such as a friend or relative, to own property on their behalf to conceal illicit proceeds.

In response to law enforcement concerns and to gather more information about money laundering risk, starting in 2016, FinCEN issued renewed and expanded Geographic Targeting Orders (GTOs) requirements in high-risk U.S. locations that often see significant real estate money laundering activity.[306] The GTOs cover certain counties within the following major U.S. metropolitan areas: Boston, Chicago, Dallas-Fort Worth, Honolulu, Las Vegas, Los Angeles, Miami, New York City, San Antonio, San Diego, San Francisco, and Seattle. The latest GTO related to real estate continues to require U.S. title insurance companies to identify the natural persons behind legal entities used in all-cash purchases of residential real estate. The purchase amount threshold remains $300,000 for each covered metropolitan area. No GTO has ever targeted commercial real estate.

Of note, the GTO requirements apply to locations such as Los Angeles County, the Borough of Manhattan, and Miami-Dade County, areas that have been traditionally popular among foreign real estate buyers. The U.S. real estate market stands out for offering foreign buyers asset appreciation and value stabilization in an investor-friendly business climate. Notably, these GTOs are likely to capture a relatively large share of foreign buyers' activity, as foreign buyers tend to purchase more expensive property than U.S. citizens and are more likely to use cash, rather than a mortgage loan. A disproportionate share of foreign buyers reportedly come from Mexico, Colombia, and China.[307] On December 6, 2021, FinCEN announced an Advance Notice of Proposed Rulemaking (ANPRM) to solicit public comment on a potential rule to permanently address the vulnerability of the U.S. real estate market to money laundering and other illicit activity.[308]

### Case examples

- In September 2021, a money launderer and drug supplier for a Baltimore DTO was sentenced to 10 years in prison for money laundering. The launderer had acquired multiple properties with the proceeds from his criminal activities. Investigators revealed that the launderer used LLCs, associates, or family members to conceal the ownership of the properties, as well as to conceal the source of funds used to purchase the properties.[309]
- In March 2021, a local narcotics distributor in Kentucky affiliated with a major Mexican DTO was sentenced to prison for drug trafficking and money laundering violations. Investigators revealed that the defendant used a portion of $4.2 million in drug proceeds to purchase local real estate.[310]

306 FinCEN, "FinCEN Renews Real Estate Geographic Targeting Orders for 12 Metropolitan Areas," (Oct. 29, 2021), https://www.fincen.gov/news/news-releases/fincen-renews-real-estate-geographic-targeting-orders-12-metropolitan-areas.

307 National Association of Realtors, "International Activity in U.S. Residential Real Estate Market Declines, According to Realtor® Survey," (Jul. 6, 2018), https://www.nar.realtor/newsroom/international-activity-in-us-residential-real-estate-market-declines-according-to-realtor-survey.

308 FinCEN, ANPRM, "Anti-Money Laundering Regulations for Real Estate Transactions," (Dec. 6, 2021), https://www.fincen.gov/sites/default/files/2021-12/RE_ANPRM_FRN_120321_FINAL_508.pdf.

309 DOJ, "Money Launderer and Wholesale Supplier of Narcotics to East Baltimore Monument Street Drug Trafficking Organization Sentenced to 10 Years in Federal Prison and Ordered to Forfeit $472,000," (Sep. 14, 2021), https://www.justice.gov/usao-md/pr/money-launderer-and-wholesale-supplier-narcotics-east-baltimore-monument-street-drug.

310 DOJ, "Multi-Drug Trafficker And Money Launderer Sentenced To 34 Years In Federal Prison," (Mar. 4, 2021), https://www.justice.gov/usao-wdky/pr/multi-drug-trafficker-and-money-launderer-sentenced-34-years-federal-prison.

- In March 2021 a marijuana courier pled guilty to charges as part of an investigation into a DTO for transporting marijuana and the proceeds generated from its sales. The organization laundered marijuana proceeds through purchases of real estate, luxury vehicles (such as a Lamborghini), and a business among other means. The courier acted as a "straw" purchaser for two residential properties in Las Vegas, Nevada.[311]
- In January 2021, DOJ settled a civil forfeiture action involving a Florida-based boutique investment firm that received millions of dollars in criminal proceeds from DTOs via a BMPE scheme to launder the illicit funds through investments in high-end commercial and residential real estate in the United States. According to court documentation, these investments include those made in the Westin Hotel in Tyson's Corner, Virginia, and in a condo building and an apartment building in Atlanta, Georgia.[312] As alleged in the complaint, throughout the investment process, the investment firm did not inquire about the source of the funds it received, including the funds from the DTOs.[313]
- In December 2020, the DOJ filed three civil forfeiture complaints alleging that properties in Kentucky, Texas, and Ohio were acquired using funds misappropriated from PrivatBank in Ukraine as part of a multi-billion-dollar loan scheme. All three properties are alleged to be subject to forfeiture based on violations of federal money laundering statutes. The three complaints allege that two men, who owned PrivatBank, one of the largest banks in Ukraine—and who exercised significant influence over officials with responsibility for banking regulation in Ukraine before 2014—embezzled and defrauded the bank of billions of dollars and laundered a portion of the criminal proceeds using an array of shell companies' bank accounts, primarily at PrivatBank's Cyprus branch, before they transferred the funds to the United States. Their associates created a web of entities to further launder the misappropriated funds and invest them. They purchased hundreds of millions of dollars in real estate and businesses across the country, including the properties subject to forfeiture.[314]
- In October 2020, key executives at a Brazilian investment firm admitted to bribing a Brazilian government official to direct government financing to companies under the investment firm's control to effectuate an $800 million acquisition of a market-leading U.S. business. To facilitate this 12-year bribery scheme, the executives created shell companies and opened affiliated U.S. bank accounts in New York to hold the funds slotted for the Brazilian official before later donating them to foreign election campaigns. Additionally, the executives used a shell company to purchase a Manhattan apartment that they then transferred to the Brazilian government official.[315]
- In October 2018, a Honduran man was sentenced for his role in laundering more than a million dollars' worth of foreign bribe payments and public funds originating from Honduras. According to a civil forfeiture compliant, the individual worked with his brother—a former Honduran government official—to launder bribes paid for the benefit of his brother by using illicit proceeds to purchase real estate in the New Orleans area, including a commercial property. Some of the properties were held in the name of the official's brother to conceal his involvement in the scheme.[316] The individual also laundered other funds into the New Orleans area originating

311 DOJ, "Las Vegas woman pleads guilty to conspiracy to distribute marijuana in St. Louis," (Mar. 11, 2021), https://www.justice.gov/usao-edmo/pr/las-vegas-woman-pleads-guilty-conspiracy-distribute-marijuana-st-louis.

312 U.S. District Court, Southern District of New York, "Civil Compliant for Forfeiture Case 1:21-cv-00169-ALC," (Jan. 8, 2021), https://www.justice.gov/usao-sdny/press-release/file/1352806/download.

313 DOJ, "Acting Manhattan U.S. Attorney Announces Settlement Of Civil Forfeiture Claims Against Over $50 Million Laundered Through Black Market Peso Exchange," (Jan. 12, 2021), https://www.justice.gov/usao-sdny/pr/acting-manhattan-us-attorney-announces-settlement-civil-forfeiture-claims-against-over.

314 DOJ, "Justice Department Seeks Forfeiture of Third Commercial Property Purchased with Funds Misappropriated from PrivatBank in Ukraine," (Dec. 30, 2020), https://www.justice.gov/opa/pr/justice-department-seeks-forfeiture-third-commercial-property-purchased-funds-misappropriated.

315 DOJ, "J&F Investimentos S.A. Pleads Guilty and Agrees to Pay Over $256 Million to Resolve Criminal Foreign Bribery Case," (Oct. 14, 2020), https://www.justice.gov/opa/pr/jf-investimentos-sa-pleads-guilty-and-agrees-pay-over-256-million-resolve-criminal-foreign.

316 DOJ, "Department of Justice Seeks Recovery of Approximately $1,528,000 in Bribes Paid to a Honduran Official," (Jan. 13, 2015), https://www.justice.gov/opa/pr/department-justice-seeks-recovery-approximately-1528000-bribes-paid-honduran-official.

from the issuance of lucrative Honduran government projects associated with his brother.[317]

## 2. Precious Metals, Stones, and Jewels

Persons involved in the trade in precious metals, stones, and jewels (PMSJs) are a diverse group, consisting of large-scale mining interests, artisanal and small-scale mining, traders, refiners, manufacturers, designers, retailers, and secondary markets such as pawnshops and auction houses.[318] In the United States, "dealers" engaged in the purchase and sale of jewels, precious metals, or precious stones are generally required to comply with AML reporting obligations if they meet a $50,000 annual threshold of both purchases and sales, with some additional exceptions.[319] While these reporting obligations are significant, the current regulatory framework for precious gems dealers still presents a vulnerability for bad actors seeking to launder their illicit proceeds.

Like other high-value assets, PMSJs may provide money launderers the opportunity to transfer the value of their illicit proceeds into an easily transportable and concealable asset. Additionally, criminals may view PMSJs as an attractive 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 international borders by couriers on their person or hidden in other items, making it difficult for law enforcement and customs personnel to detect these items. Additionally, even upon detection of PMSJs, it is difficult for government officials to identify the origin of the PMSJ, impeding law enforcement investigations. This is particularly concerning when considering that some diamonds and other gems that can easily be purchased are valued over $100,000, which makes the concealment and smuggling of those purchased via illicit proceeds a money laundering vulnerability.

### Case examples

- In December 2021, three gold dealers were sentenced in federal court for committing multiple financial crimes, including laundering money through their unlicensed money transmitting business. The multiyear investigation unraveled millions of dollars in suspicious transactions taking place at the San Diego-based office and bank accounts of Global Gold Exchange (GGEX). The defendants acted as an informal money transfer system which engaged in facilitating the transfer of money domestically and internationally outside of the conventional financial banking system. The defendants laundered cash and funds from a variety of sources; both lawful and unlawful, and employed various money laundering techniques to conduct unlawful transactions through GGEX and GGEX's bank accounts. This included transacting with a local cartel out of Mexico to falsify invoices for sales of gold, when in reality it was the receipt of large cash deposits that were returned by check after GGEX took a 10 percent fee.
- In March 2021, eight defendants were charged for allegedly using fake, stolen, or synthetic identities to submit fraudulent applications which allowed them to obtain approximately $18 million in EIDL and PPP loans under the CARES Act. As alleged in the indictment, upon receiving the funds, the defendants conspired as part of a disaster-relief loan fraud ring to use the fraudulently obtained funds as down payments on luxury homes and to buy gold coins, diamonds, jewelry, luxury watches, fine imported furnishings, designer handbags and clothing, virtual assets, and securities.[320]

---

317 DOJ, "Honduran Man Sentenced to More Than Three Years in Prison for Conspiring to Launder Over $1 Million in Bribes and Funds Misappropriated from the Honduran Social Security Agency," (Oct. 3, 2018), https://www.justice.gov/opa/pr/honduran-man-sentenced-more-three-years-prison-conspiring-launder-over-1-million-bribes-and.

318 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 (identifying types of businesses that may be covered by the Interim Final Rule).

319 See Code of Federal Regulations 31 CFR Part 1027, https://www.law.cornell.edu/cfr/text/31/part-1027.

320 DOJ, "Four Additional Members of Los Angeles-Based Fraud Ring Indicted for Exploiting COVID-Relief Programs," (Mar. 12, 2021), https://www.justice.gov/opa/pr/four-additional-members-los-angeles-based-fraud-ring-indicted-exploiting-covid-relief.

- As detailed in the September 2020 press release for Operation Apex, federal law enforcement took down a drug trafficking and illegal wildlife trafficking organization. As alleged in the indictment, conspirators in multiple locations in the United States and in Hong Kong, Mexico, Canada, and elsewhere were involved in the Wu TCO that engaged in wildlife trafficking, shark finning, drug trafficking, and money laundering. The indictment alleges that the conspiracy began as early as 2010 as members of the conspiracy submitted false documents and used sham businesses and dozens of bank accounts to hide proceeds from the illegal activities. The indictment states that members of the conspiracy would deposit bulk cash from illegal activities, including wildlife trafficking and drug trafficking, into third-party business accounts that dealt in gold, precious metals, and jewels, to hide the illegal activities. During the arrests of the defendants and searches of their homes and workplaces, agents seized $1 million in diamonds, among other things.[321]
- In February 2019, a jeweler plead guilty to money laundering violations for using his jeweler business to launder what he thought were hundreds of thousands of dollars in drug proceeds. In exchange for a fee, the jeweler took in the money he believed to be drug trafficking proceeds from an undercover federal agent, before depositing them into his business's accounts and later structuring payments belonging to the undercover federal agent.[322]
- In 2019, law enforcement uncovered a fraud scheme designed to pass off jewelry made in the Philippines as genuine Native American jewelry to the U.S. public. According to the indictment, after selling the jewelry, the fraudsters then laundered the proceeds generated in the U.S. to ultimately make them available to facilitate the overseas jewelry production.[323]

## 3. Special Focus: Art Industry

Treasury has issued a separate study on the *Facilitation of Money Laundering and Terror Finance Through the Trade in Works of Art*, which identifies art market participants and sectors of the high-value art market that may present ML/TF risks to the U.S. financial system.[324] This study was mandated by Section 6110(c) of the Anti-Money Laundering Act (the AML Act) as part of the NDAA of 2021.[325] Purchasing high-value art as a way to spend or launder illicit proceeds is not new, but the study examines market indicators and other information to determine whether the art market is attracting greater illicit finance and what can be done to further mitigate the laundering of illicit proceeds through art.

Individuals of high net worth often seek high-value goods or commodities for personal consumption or as an investment. Several qualities inherent to art, the high-value art market, and market participants may make the market attractive for money laundering by illicit actors. These include the high-dollar values of single transactions, the ease of transportability of works of art, and the long-standing culture of privacy in the market, offering anonymity to buyers and sellers through private sales and transactions, as well as the use of third-party intermediaries, such as art dealers, advisers, or interior designers, shell companies, and trusts to purchase, hold, and sell art on the clients' behalf.

---

321 DOJ, "International money laundering, drug trafficking and illegal wildlife trade operation dismantled," (Sep. 3, 2020), https://www.justice.gov/usao-sdga/pr/international-money-laundering-drug-trafficking-and-illegal-wildlife-trade-operation.

322 DOJ, "Jewelry District Business Owner Pleads Guilty to Money Laundering," (Feb. 11, 2019), https://www.justice.gov/usao-cdca/pr/jewelry-district-business-owner-pleads-guilty-money-laundering.

323 DOJ, "Seven People, Including Three Filipinos, Charged with Fraudulently Selling Jewelry Imported from the Philippines as Native American-Made," (Mar. 7, 2019), https://www.justice.gov/opa/pr/seven-people-including-three-filipinos-charged-fraudulently-selling-jewelry-imported.

324 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.

325 The AML Act was enacted as Division F, Section 6001-6511, of the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, Public Law 116-283 Stat 3388 (2021).

While banks and broker-dealers in securities are required to file SARs,[326] many other participants in the art market are not subject to SAR filing obligations. For instance, while a bank whose clients include galleries, auction houses, or other art dealers has a SAR filing obligation, the art market participants themselves do not. In March 2021, FinCEN issued a notice to inform financial institutions about (1) the AML Act efforts related to trade in antiquities and art, (2) select sources of information about existing illicit activity related to antiquities and art, and (3) specific instructions for filing SARs related to trade in antiquities and art.[327]

## ENTITIES NOT SUBJECT TO COMPREHENSIVE AML/CFT REQUIREMENTS

The U.S. government continues to assess the illicit finance risks related to other types of financial institutions that are not subject to comprehensive AML/CFT requirements to determine whether additional AML/CFT measures would be appropriate.[328]

### 1. Investment Advisers and Private Investment Vehicles

Money managers, investment consultants, and financial planners are regulated in the United States as IAs under the U.S. Investment Advisers Act of 1940 or similar state statutes.[329] As of July 2021, there were approximately 13,880 IAs registered with the SEC (RIAs), managing $110 trillion in assets for 60.8 million customers.[330] These RIAs range from those affiliated with multinational financial holding companies, advising or managing billions of dollars on behalf of wealthy individuals, institutional investors, and private funds to RIAs and state-registered IAs[331] who run small offices with 5 to 10 employees and manage tens of millions of dollars. IAs are subject to either federal or state registration and reporting requirements, many of which focus on preventing fraudulent activity.

While RIAs are not explicitly subject to AML/CFT requirements under the U.S. regulatory regime, many RIAs fulfill some AML/CFT obligations in certain circumstances. For example, an RIA that is part of a bank holding company may be subject to certain AML/CFT obligations under the rules and regulations applicable to banks, and RIAs dually registered as broker-dealers may be required to fulfill AML/CFT requirements applicable to broker-dealers. Similarly, some RIAs fulfill AML/CFT obligations for joint customers on behalf of another entity with which the RIA conducts business.[332] Often this other entity is directly subject to AML/CFT obligations (e.g., a broker-dealer or bank). Additionally, some RIAs voluntarily implement AML/CFT measures. A 2015 FinCEN Notice of proposed

326 See 31 CFR 1020.320.

327 FinCEN, "FinCEN Informs Financial Institutions of Efforts Related to Trade in Antiquities and Art," (Mar. 9, 2021), https://www.fincen.gov/sites/default/files/2021-03/FinCEN%20Notice%20on%20Antiquities%20and%20Art_508C.pdf.

328 While technically also part of this category, real estate professionals and art dealers are covered in the previous section on high-value assets.

329 SEC, *Regulation of Investment Advisers by the U.S. Securities and Exchange Commission*, (April 2012), https://www.sec.gov/about/offices/oia/oia_investman/rplaze-042012.pdf.

330 Investment Adviser Association, "Investment Adviser Industry Snapshot 2021," (July 2021), https://investmentadviser.org/wp-content/uploads/2021/08/Investment_Adviser_Industry_Snapshot_2021.pdf.

331 For example, the SEC does not mandate registration for IAs who have assets under management of at least $100 million but less than $110 million and does not require an IA to withdraw their registration unless they have less than $90 million of assets under management. See 17 CFR 275.203A-1(a)(1). IAs with assets under management of less than $100 million that are not required to register with the SEC may be subject to state registration requirements.

332 For example, this could include an RIA and bank or broker-dealer that share a customer, and the RIA is contractually obligated to performing CIP, CDD, and the portion of the customer due diligence rule regarding beneficial ownership requirements for legal entity customers. The SEC has issued and extended a "no-action position" that it will not recommend enforcement action if a broker-dealer relies on an RIA to perform some or all of the requirements of the CIP Rule and the Beneficial Ownership Rule, subject to certain conditions. See SEC, "Request for No-Action Relief Under Broker-Dealer Customer Identification Program Rule (31 C.F.R. § 1023.220) and Beneficial Ownership Requirements for Legal Entity Customers (31 C.F.R. § 1010.230)," (Dec. 9, 2020), https://www.sec.gov/divisions/marketreg/mr-noaction/2020/sifma-120920-17a8.pdf.

rule making proposed to subject RIAs, which could include RIAs to private funds (such as hedge funds and private equity funds), to AML requirements (2015 FinCEN RIA NPRM).[333]

Along with the lack of comprehensive AML/CFT regulatory requirements, other attributes of the investment advisory business create vulnerabilities that illicit actors may be able to exploit. First, the use of third-party custodians by RIAs separates the advisory functions of an RIA's business from the actual movement or transfer of client funds. While rules regulating the custody of client assets[334] are intended to protect advisory clients from unscrupulous RIAs, the use of third-party custodians, when combined with the practice of pooling customer funds into omnibus accounts for trading and investment, can impede transparency, which is core to AML/CFT effectiveness. The 2015 FinCEN RIA NPRM stated, for example, that "[w]hen an adviser orders a broker-dealer to execute a trade on behalf of an adviser's client, the broker-dealer may not know the identity of the client. When a custodial bank holds assets for a private fund managed by an adviser, the custodial bank may not know the identities of the investors in the fund."[335]

This inherent segmentation of activities has become doubly challenging as some RIAs provide services to more complex investment arrangements that insert additional U.S. and foreign legal entities, such as LLCs and trusts, between the actual advisory clients and the final investment of their funds. Such structures may be used for legitimate tax reasons but may also be used to circumvent AML regulations and obfuscate the ultimate beneficial owner of the legal entity. These structures in many circumstances may leave other service providers (who may be subject to different AML/CFT obligations) with little insight into the source of the underlying funds.[336]

Second, it is common for RIAs who manage private funds to rely on third-party administrators who, depending upon the fund administrator's regulatory regime, perform compliance with core AML/CFT requirements on behalf of the RIA or another regulated entity for these funds. In many instances, such administrators are located in offshore financial centers where private funds are routinely registered, usually for tax or other commercial or non-AML/CFT regulatory advantages. It is also common for these private funds to solicit non-U.S. investors who are seeking to diversify globally and maximize returns. Domiciling private funds in offshore jurisdictions and using foreign third-party administrators may lead to situations where data privacy or other laws or regulations in effect in those offshore jurisdictions or contractual obligations prohibit customer and beneficial ownership information from reaching U.S. RIAs, broker-dealers, and other financial institutions (and by extension, U.S. law enforcement conducting investigations, where there are AML/CFT obligations).

Third, many of the existing federal and state investment advisory regulatory requirements are not designed to explicitly address ML/TF risks. For example, the Custody Rule, which generally requires that client assets and funds advised by an RIA be held at a "qualified custodian" (usually a financial institution that is subject to U.S. AML/CFT obligations but also includes foreign financial institutions), is intended to protect advisory clients from RIAs who otherwise might steal clients' funds and assets, not to address ML/TF risks.[337] Some qualified custodians are subject to similar asset protection requirements but vastly different AML/CFT obligations and levels of supervision.

---

333 FinCEN, "Anti-Money Laundering Program and Suspicious Activity Report Filing Requirements for Registered Investment Advisers, Notice of Proposed Rulemaking," (80 Fed. Reg. 52,680), (Sep. 1, 2015), https://www.federalregister.gov/documents/2015/09/01/2015-21318/anti-money-laundering-program-and-suspicious-activity-report-filing-requirements-for-registered.

334 See 17 CFR Parts 275 and 279 (the Custody Rule).

335 80 Fed. Reg. 52,680, 52,681 (Sep. 1, 2015).

336 The SEC staff has identified potential illicit finance concerns with omnibus accounts held in the name of foreign financial institutions. See SEC, "Staff Bulletin: Risks Associated with Omnibus Accounts Transacting in Low-Priced Securities," (Nov. 4, 2021), https://www.sec.gov/tm/risks-omnibus-accounts-transacting-low-priced-securities#_ftn6.

337 The Custody Rule contains exceptions from this general provision for limited categories of assets.

For instance, an OCC-chartered national bank, state-chartered member bank, state-chartered trust company, and European multinational financial institution may all be "qualified custodians" per SEC regulations, but in practice each institution is subject to substantially different levels of AML/CFT supervision.

Moreover, due to the range of account structures used by RIAs to provide advisory services and the varying business models in the asset management industry, the specific level of ML/TF risk varies throughout the industry. For instance, comments to FinCEN's RIA NPRM 2015 noted that some RIAs operate private funds that may not permit asset withdrawals for a number of years, or act purely in an advisory capacity without placing trades through a broker-dealer or bank.[338]

Given these attributes of the investment advisory business and the lack of comprehensive AML/CFT requirements, some money launderers may see some RIAs or state-registered IAs as a low-risk way to enter the U.S. financial system.[339] For example, this could occur when a money launderer tries to fund a brokerage account with the assistance of an IA with cash or cash equivalents derived from illegal activity (e.g., securities fraud, etc.).[340] U.S. law enforcement agencies are also concerned that criminally complicit investment fund managers may expand their money laundering operations as private placement opportunities increase, resulting in continued infiltration of the licit global financial system. For example, the FBI assesses that threat actors likely place funds in private investment companies, including hedge funds and private equity funds, to launder money and thereby circumvent traditional AML/CFT programs. Additionally, industry data shows a growing shift in the securities industry with a decrease in broker-dealer registrations and an increase in RIAs[341]. This change may be driven by what is perceived to be a lower AML/CFT compliance burden for RIAs, as well as RIA fee structures that may seem more lucrative than broker-dealer commission-based compensation.

Moreover, some money launderers may see posing as IAs (not following applicable state or federal registration requirements) as an opportunity to attract assets, defraud investors and launder money. While there are numerous cases of individuals holding themselves out as advisers but then stealing client funds[342], this scheme could also allow a financial facilitator, potentially working with other complicit professionals, to place illicit proceeds into a range of financial and nonfinancial assets.

The cases below involve criminal or fraudulent conduct by individuals claiming to be acting in an investment advisory capacity or operating an investment fund. This type of criminal or fraudulent conduct is not only damaging to clients but to the overall economy. These cases also indicate how even unwitting RIAs can be involved in complex schemes to launder illicit proceeds from outside the United States.

### Case examples

- In December 2021, a former RIA and 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 RIA executed a

338 See, for example, Letter from the Investment Advisory Association to FinCEN re: Anti-Money Laundering Program and Suspicious Activity Report Filing Requirements for Registered Investment Advisers, Docket Number FINCEN-2014-0003, RIN 1506-AB10, (Nov. 2, 2015); Letter from Managed Funds Association to FinCEN re: AML Program and SAR Filing Requirements for Registered Investment Advisers (RIN: 1506-AB10) Docket Number FinCEN-2014-003, (Nov. 2, 2015).

339 For instance, the FATF 2016 Mutual Evaluation Report of the United States noted the lack of comprehensive AML/CFT obligations for IAs is a "significant gap" in the U.S. AML/CFT framework. FATF, *United States Mutual Evaluation*, (2016), https://www.fatf-gafi.org/media/fatf/documents/reports/mer4/MER-United-States-2016.pdf, p. 3.

340 See 80 Fed. Reg. 52680, 52682, footnote 15.

341 FINRA, "2021 Industry Snapshot," https://www.finra.org/rules-guidance/guidance/reports-studies/2021-industry-snapshot.

342 See, for example, FBI, "Investment Fraud," https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/investment-fraud.

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 company, and the IA then misappropriated the funds into his own personal banking account, among other things.[343]

- In May 2021, a New Jersey resident was charged with COVID-19 relief fraud and money laundering in connection with his fraudulent filing of PPP loans. This individual allegedly submitted loan applications totaling $3.8 million to multiple lenders, misrepresenting his tax and payroll documentation as well as the number of people employed by his five businesses, including his hedge fund management firm Brattle Street Capital LLC. Once in receipt of the loan, the defendant allegedly transferred the money to his brokerage account. Through bad stock trades, the defendant ended up losing $3 million.[344]
- In July 2018, U.S. law enforcement arrested two alleged participants in a billion-dollar international scheme to launder funds embezzled from Venezuelan state-owned oil company Petroleos De Venezuela S.A. (PDVSA) using Miami, Florida, real estate and sophisticated false-investment schemes. According to the criminal complaint, the conspiracy in this case allegedly began in December 2014 with a currency exchange scheme that was designed to embezzle around $600 million from PDVSA, obtained through bribery and fraud, and the defendants' efforts to launder a portion of the proceeds of that scheme. By May 2015, the conspiracy had allegedly doubled in amount to $1.2 billion embezzled from PDVSA. PDVSA is Venezuela's primary source of income and foreign currency (namely, U.S. dollar and Euros). Sophisticated false-investment money laundering schemes were used throughout this conspiracy, ranging from individual false securities (promissory notes and bonds) to entire false-investment funds, which could be subscribed to as needed to justify transactions. Surrounding and supporting these false-investment laundering schemes were complicit money managers, brokerage firms, banks, and real estate investment firms in the United States and elsewhere, operating as a network of professional money launderers.[345]

## 2. Third-Party Payment Processors

Third-party payment processors, or merchant processors, have emerged as a popular way for online merchants and brick-and-mortar stores to meet consumer demand without having to maintain a business relationship with a wide array of financial institutions. When a merchant seeks to process a transaction with a financial institution, a third party can process the transaction on behalf of the financial institution and the merchant. Instead of the funds directly transferring from the merchant account to the financial institution, the third party will use its account at a financial institution to process the transaction or, in some cases, open an account at a financial institution in the name of the merchant. These third parties most often process credit card transactions but can also process ACH debits.[346]

While the increased presence of payment processors facilitates banking for merchants, it also creates an opportunity for bad actors to launder illicit proceeds. With more and more businesses using third-party payment processors, a payment processor can, knowingly or unknowingly, process illicit proceeds from any company that signs up to use its services. This can include ACH debits from high-risk foreign jurisdictions that have deficient AML/CFT regimes.

---

343 DOJ, "Founder of Investment Advisory Firm Charged with Wire Fraud, Investment Adviser Fraud and Money Laundering," (Dec. 6, 2021), https://www.justice.gov/usao-edny/pr/founder-investment-advisory-firm-charged-wire-fraud-investment-adviser-fraud-and-money.

344 DOJ, "New York City Man Charged with Nearly $4 Million COVID-19 Relief Fraud Scheme and Money Laundering," (May 6, 2021), https://www.justice.gov/opa/pr/new-york-city-man-charged-nearly-4-million-covid-19-relief-fraud-scheme-and-money-laundering.

345 USDC, Southern District of Florida, Case 1:18-mj-03119-EGT, criminal complaint. (Jul. 23, 2018), https://storage.courtlistener.com/recap/gov.uscourts.flsd.531919/gov.uscourts.flsd.531919.3.0.pdf.

346 FinCEN, Guidance, "Risk Associated with Third-Party Payment Processors," (2012), https://www.fincen.gov/resources/advisories/fincen-advisory-fin-2012-a010.

Processors generally are not subject to BSA/AML regulatory requirements and the scope of BSA coverage is dependent on the unique circumstances of the company. Only those payment processors that meet very specific conditions set forth in FinCEN guidance (FIN-2014-R009) are exempt from BSA obligations. 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 FFIEC has provided guidance to bank examiners in the FFIEC BSA/AML Examination Handbook that addresses banks that provide account services to third-party payment processors and notes that these banks should, among other things (1) monitor their processor relationships for any significant changes in the processor's business strategies that may affect their risk profile; (2) periodically reverify and update the processors' profiles to ensure the risk assessment is appropriate; (3) ensure that their contractual agreements with payment processors provide them with access to necessary information in a timely manner; and (4) periodically audit their third-party payment processing relationships, including reviewing merchant client lists and confirming that the processor is fulfilling contractual obligations to verify the legitimacy of its merchant clients and their business practices.[347]

Recent cases indicate that the use of payment processors is on the rise for complex money laundering activity related to various crimes. Significant fraud, drug trafficking, and even sanctions evasion, among other types of illicit activity, have been facilitated through money laundering enabled by third-party payment processors.

### Case examples

- In March 2021, two individuals were convicted of bank fraud for devising a complex transaction laundering scheme involving fake companies, false websites, and fake customer service centers, designed to deceive U.S. issuing banks and credit unions into effectuating more than $150 million of credit and debit card purchases of marijuana by disguising those purchases as being for other kinds of goods, such as face creams and dog products. The scheme involved the deception of virtually all the participants in the payment processing network, including issuing banks in the United States and Visa and MasterCard. The primary method used to deceive the issuing banks involved the purchase and use of shell companies that were used to disguise the marijuana transactions using phony merchants. The shell companies were used to open offshore bank accounts with merchant acquiring banks and to initiate credit card charges for marijuana purchases made through the company.[348]
- In 2019, four executives of a Canadian payment processor were charged with fraud and money laundering in a massive fraud scheme in which their company processed payments from victims of numerous international mass-mail fraud campaigns. The indictment alleged that PacNet, under the defendants' direction, was the payment processor of choice for companies that mailed large volumes of fraudulent notifications designed to mislead victims into falsely believing they would receive a large amount of money, a valuable prize, or specialized psychic services upon payment of a fee. Many alleged victims were elderly or otherwise vulnerable. PacNet, according to the indictment, served as the middleman between banks and the fraudulent mailers, aggregating the checks, cash, and credit card payments collected by its clients; depositing the payments into PacNet-controlled bank accounts; and then distributing the funds as directed by the clients.[349]

347 FFIEC Manual, "Risk Associated with Money Laundering and Terrorist Financing, Trust and Asset Management Overview," https://bsaaml.ffiec.gov/manual/RisksAssociatedWithMoneyLaunderingAndTerroristFinancing/21.

348 DOJ, "Jury Convicts Creators Of Scheme To Fraudulently Process Over $150 Million Through U.S. Financial Institutions," (Mar. 24, 2021), https://www.justice.gov/usao-sdny/pr/jury-convicts-creators-scheme-fraudulently-process-over-150-million-through-us.

349 DOJ, "Four Executives of Canadian Payment Processor Charged with Fraud and Money Laundering," (Jun. 20, 2019), https://

- In 2019 the CEO of a credit card processing sales company was charged of fraudulently operating a credit card laundering scheme that enabled access to the credit card system for certain deceptive businesses, including an underlying telemarketing scheme. Beginning in 2012 the defendant allegedly negotiated a deal with a telemarketer to help it obtain credit card processing services by retaining approximately one-third of their credit card sale transactions in exchange for providing the telemarketer access to the credit card processing network. In securing payment card processing for the telemarketer, the defendant concealed that telemarketer was the true underlying merchant. Instead, the defendant and his co-conspirators created approximately 26 sham merchant companies and prepared fraudulent merchant applications for each of them that made the sham companies appear legitimate to ultimately make them more likely to be approved by a separate sales company which approved merchants for payment processing services at the bank. Through this arrangement, the telemarketer and other high-risk merchants concealed their identities from the payment processor and the bank, which prevented the payment processor from identifying prohibited services. Additionally, the arrangement allowed the telemarketer to layer the payments across multiple merchant accounts, enabling them to avoid detection, including through monitoring designed to identify refunds and chargebacks, by the sales agent, the payment processor, and the bank.[350]

## 3. Special Focus: Non-Federally Chartered Puerto Rican Financial Entities

Puerto Rico, an island of 3.26 million people, is one of five inhabited U.S. territories. The day-to-day governance of the island and the provision of basic services falls under the responsibility of the territorial government, led by a governor and supported by a legislative body, the Puerto Rico Legislative Assembly. Puerto Rico has a history of designing tax incentives aimed at attracting financial services businesses to the island. These incentives were primarily provided through Act No. 52 of 1989, the International Banking Center Regulatory Act,[351] allowing banks to register and operate in Puerto Rico as International Banking Entities (IBEs). In 2012, this legislation was effectively replaced by Act No. 273, the International Financial Entity Regulatory Act (IFE Act).[352] The IFE Act provides tax breaks and incentives to encourage the establishment of an International Financial Entity (IFE), a loose term that encompasses banks, broker-dealers, investment firms, and other entities.[353] As of November 2021, there were approximately 50 IFEs[354] and 27 IBEs licensed in Puerto Rico.[355] These entities by law cannot provide services to most Puerto Rican residents; they may take deposits and offer loans only to nonresident customers and foreign business entities.[356] By the end of the third quarter of 2021, there were approximately $52 billion in assets

www.justice.gov/opa/pr/four-executives-canadian-payment-processor-charged-fraud-and-money-laundering.

350 DOJ, "CEO Of Credit Card Processing Company Charged In $19 Million Credit Card Laundering Scheme," (Oct. 11, 2019), https://www.justice.gov/usao-sdny/pr/ceo-credit-card-processing-company-charged-19-million-credit-card-laundering-scheme.

351 Act No. 52 of Aug. 11, 1989, as amended, "International Banking Center Regulatory Act," https://bvirtualogp.pr.gov/ogp/Bvirtual/leyesreferencia/PDF/Y%20-%20Ingl%C3%A9s/52-1989.pdf.

352 Act No. 273 of Sep. 25, 2012, as amended, (contains amendments incorporated by: Act No. 154 of Sep. 10, 2014) "International Financial Entity Regulatory Act," https://www.the2022actsociety.org/wp-content/uploads/2018/08/act-273-of-2012-law.pdf.

353 Act No. 273.

354 Oficina del Comisionado de Instituciones Financieras (OCIF), *Entidades Financieras Internacionales*, (Nov. 1, 2021), https://ocif.pr.gov/Consumidores/Lista%20Concesionarios/Entidades%20Financieras%20Internacionales.pdf.

355 OCIF, *Entidades Bancarias Internacionales*, (Apr. 13, 2021), https://ocif.pr.gov/Consumidores/Lista%20Concesionarios/Entidades%20Bancarias%20Internacionales.pdf.

356 Act No. 273 of Sep. 25, 2012, as amended, (contains amendments incorporated by: Act No. 154 of Sep. 10, 2014) "International Financial Entity Regulatory Act," https://www.the2022actsociety.org/wp-content/uploads/2018/08/act-273-of-2012-law.pdf.

held by IBEs[357] and $1.64 billion held by IFEs.[358] IBEs and IFEs are overseen at the territorial level by Puerto Rico's primary financial regulator, the Office of the Commissioner of Financial Institutions. Since March 2021, they have also been subject to FinCEN and IRS supervision.[359]

The other type of financial entity, the cooperativa, is a type of credit union that operates under a charter from the Public Corporation for the Supervision and Insurance of Cooperatives of Puerto Rico.[360] Originally chartered to serve rural communities, cooperativas now offer expanded services in many locations. As of September 2021, there were approximately 110 cooperativas in operation. Unlike IBEs and IFEs, cooperativas primarily serve Puerto Rican residents, approximately 1 million individuals. As of September 2021, approximately $8 billion of deposits were held in cooperativas.[361]

IBEs, IFEs, and cooperativas (collectively Puerto Rican financial entities, or PRFEs), which are chartered and licensed by territorial authorities, present money laundering vulnerabilities to the U.S. financial system, with IBEs and IFEs being of particular concern because of their offshore banking business model. IBEs and IFEs by law cannot provide financial services to most Puerto Rican residents, taking deposits and offering loans to nonresident customers and foreign business entities. Due to low staffing requirements for IBEs and IFEs, they have a minimal physical presence in Puerto Rico as they are only required to employ four residents of Puerto Rico. While cooperativas face similar vulnerabilities from a lack of territorial and federal supervisory resources, they service Puerto Rican residents as well as offshore customers.

Until 2020, PRFEs were operating without needing to comply with the requirement to establish and maintain an AML program, although they were subject to certain other BSA requirements.[362] In a 2020 final rule, FinCEN also imposed additional AML obligations on banks lacking a federal functional regulator (the "Gap Rule"), ensuring that such entities would be subject to requirements to have an AML program and meet CIP and CDD requirements, including the verification of beneficial owners of legal entity accounts, in addition to their existing SAR obligations (which would include reporting on transactions involving suspicious real estate transactions).[363] The Gap Rule became effective on March 15, 2021, and PRFEs and others are now required to implement AML compliance programs and are subject to criminal and civil penalties if they fail to do so. However, given severe resource constraints facing federal and local regulators, there are relatively few examiners and supervisory staff assigned to supervise a considerably large amount of PRFEs. This arrangement may make these entities attractive money laundering vehicles, potentially allowing nefarious actors to misuse them to facilitate illicit financial activity.

At the territorial level, Puerto Rico has faced an ongoing financial crisis and disruption in the aftermath of

357 OCIF, Datos Estadísticos, *Entidades Bancarias Internacionales*, https://ocif.pr.gov/DatosEstadisticos/Datos%20Estadisticos/Ent%C3%ADdades%20Financieras%20Internacionales.pdf.

358 OCIF, Datos Estadísticos, *Entidades Financieras*, https://ocif.pr.gov/DatosEstadisticos/Datos%20Estadisticos/Ent%C3%ADdades%20Financieras%20Internacionales.pdf.

359 Federal Register, 85 Fed. Reg. 57129 (codified at 31 CFR 1020.210), (Sep. 15, 2020), https://www.govinfo.gov/content/pkg/FR-2020-09-15/pdf/2020-20325.pdf.

360 Corporación Pública para la Supervisión y Seguro de Cooperativas de Puerto Rico (COSSEC), "Historia de Cossec: 30 Años de Historia," https://www.cossec.com/cossec_new/historia/.

361 COSSEC, "Estadísticas Industria Cooperativas de Ahorro y Crédito," (Jun. 30, 2021), https://www.cossec.com/cossec_new/est/Junio2021/Estadisticas_Industria_Cooperativas_AC_jun_2021.pdf.

362 Pursuant to CFR 1010.310-314, 31, CFR 1020.320, and 31 CFR 1010.410, entities lacking a federal functional regulator were still required to file CTRs and SARs, as well as to make and maintain certain records. Also, pursuant to 31 CFR 1010.630, 31 CFR 1010.670, and 31 CFR 1010.605(e)(2), they were prohibited from maintaining correspondent accounts for foreign shell banks and were required to obtain and retain information on the ownership of foreign banks.

363 Federal Register, 85 FR 57129 (codified at 31 CFR 1020.210), (Sep. 15, 2020), https://www.govinfo.gov/content/pkg/FR-2020-09-15/pdf/2020-20325.pdf.

Hurricane Maria, complicating efforts for local supervisors to effectively oversee these entities to ensure compliance with the BSA according to local laws. This impacts the IRS SB/SE, the federal entity with delegated authority from FinCEN for examining the PRFEs. No other federal functional regulator is responsible for their regulation as these entities are not federally chartered and do not require FDIC insurance. The NCUA only insures a few credit unions operating on the island, although not all of these entities are cooperativas.

### Case examples

- In October 2019, according to a civil forfeiture complaint, DOJ sought to seize assets related to a scheme in which an individual and his wife fraudulently established an IFE in Puerto Rico and an international financial services entity in the USVI for the purpose of executing wire transfers using the U.S. financial system on behalf of the entities' customers. As alleged in the complaint, this individual executed a fraudulent scheme to gain access to the U.S. financial system through licensed financial entities accounts at financial institutions located in Puerto Rico, New Jersey, and North Carolina. In furtherance of the scheme, false, misleading, and inaccurate statements were transmitted through email and messaging applications to these financial institutions, who relied on those statements in deciding whether to open and maintain the accounts. For example, using a fraudulently obtained account at an IFE, the individual executed millions of dollars in wire transfers on behalf of customers located in high-risk money laundering jurisdictions in Central and South America, including an MSB owned by or affiliated with members of the individual's family.[364] In order to gain access to the U.S. financial system, the IFE used a cooperativa, which had a master account at the Federal Reserve[365] as a correspondent bank. This arrangement concealed the nature, source, ownership, and control of the funds flowing through the IFE's account and limited potential scrutiny by the cooperativa in connection with its BSA/AML duties under the laws of the Commonwealth of Puerto Rico. As part of the settlement of this case, the DOJ seized approximately $1.4 million.[366]

364 U.S. District Court for the District of Puerto Rico, civil forfeiture compliant, Case 3:19-cv-01236-FAB, Filed Oct. 09, 2019.

365 Federal Reserve Banks provide master accounts and related financial services (such as Automated Clearing House, cash, check, and wire transfer) to certain U.S. financial institutions for example, banks and credit unions. See "Federal Reserve Banks Operation Circular 1 Account Relationships," effective Aug. 16, 2021, for definitions of terms and additional information, available at https://www.frbservices.org/binaries/content/assets/crsocms/resources/rules-regulations/081621-operating-circular-1.pdf.

366 U.S. District Court for the District of Puerto Rico, stipulation for compromise settlement, Case 19-CV-1236 (FAB), Filed Jun. 28, 2021

# CONCLUSION

The 2022 NMLRA demonstrates that criminals continue to use a wide range of money laundering techniques, including traditional ones, to move and conceal illicit proceeds depending on what is available or convenient to them. The findings show that new programs, products, and technology have been exploited for fraud and laundering purposes as money launderers also adapt to changes and developments in the payments landscape. Key factors, such as actual or perceived anonymity, lack of transparency, complicit actors, and weaknesses in law or regulation, continue to be fundamental vulnerabilities that facilitate money laundering activity in the United States.

The COVID-19 pandemic clearly had an effect, at least temporarily, on how criminals exploited new sources of revenue and their ability to physically move illicit cash. Future assessments will look at these factors as the pandemic, and responses to it, continue to evolve. Other contextual factors, such as how the U.S. government responds to the public health crisis surrounding fentanyl, have and will affect how drug-related money laundering activity takes place not only in the United States but potentially more globally as synthetic opioid abuse grows.

The spotlight on the Special Focus topics, that were not fully addressed in previous assessments, should provide greater awareness raising and more insight to the public and private sectors to aid with understanding and managing risk. There is a need to do more work on the scope and nature of some of the sectoral risks (e.g., trusts, IAs, third-party payment processors) and geographic risks (e.g., the Caribbean and U.S. territories) identified in the 2022 NMLRA. As such, the findings of this report will be used to help develop policy responses to mitigate the money laundering risks identified, mainly through the issuance of the 2022 Strategy.

# LIST OF ACRONYMS

| | |
|---|---|
| ACH | Automated Clearinghouse |
| AEC | Anonymity-Enhanced Cryptocurrencies |
| AML/CFT | Anti-Money Laundering / Countering the Financing of Terrorism |
| ANPRM | Advance Notice of Proposed Rulemaking |
| BCS | Bulk Cash Smuggling |
| BEC | Business Email Compromise |
| BMPE | Black Market Peso Exchange |
| BSA | Bank Secrecy Act |
| BSA/AML | Bank Secrecy Act / Anti-Money Laundering |
| CARES Act | Coronavirus Aid, Relief, and Economic Security Act |
| CBDC | Central Bank-Issued Digital Currencies |
| CBP | U.S. Customs and Border Protection (Department of Homeland Security) |
| CDD | Customer Due Diligence |
| CFTC | Commodity Futures Trading Commission |
| CIP | Customer Identification Program |
| CJNG | Cártel Jalisco Nueva Generación |
| CMLO | Chinese Money Laundering Organizations |
| CMP | Civil Money Penalty |
| CPF | Countering Proliferation Financing |
| CTR | Currency Transaction Report |
| CVCs | Convertible Virtual Currencies |
| DEA | Drug Enforcement Administration (U.S. Department of Justice) |
| DeFi | Decentralized Finance |
| DHS | Department of Homeland Security |
| DOJ | Department of Justice |
| DPA | Deferred Prosecution Agreement |
| DTO | Drug Trafficking Organization |
| EDD | Enhanced Due Diligence |
| EU | European Union |
| FATF | Financial Action Task Force |
| FBAs | Federal Banking Agencies |
| FBI | Federal Bureau of Investigation |
| FCPA | Foreign Corrupt Practices Act |

| | |
|---|---|
| FDIC | Federal Deposit Insurance Corporation |
| FFIEC | Federal Financial Institutions Examination Council |
| 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 |
| GTO | Geographic Targeting Order |
| IA | Investment Advisers |
| IBEs | International Banking Entities |
| IC | Intelligence Community |
| 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) |
| IFE | International Financial Entity |
| IRS-CI | Internal Revenue Service-Criminal Investigation |
| IT | Information Technology |
| ML/TF | Money Laundering/Terrorist Financing |
| MSB | Money Services Business |
| NCUA | National Credit Union Administration |
| NDTA | National Drug Threat Assessment |
| NPA | Non-Prosecution Agreement |
| 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) |
| OIA | Office of Intelligence and Analysis (U.S. Department of the Treasury) |
| PF | Proliferation Financing |
| PII | Personal Identifiable Information |
| PMLO | Professional Money Laundering Organization |
| PMSJs | Precious Metals, Stones, And Jewels |
| PEP | Politically Exposed Person |
| PPP | Paycheck Protection Program |
| PRFEs | Puerto Rican Financial Entities |
| P2P | Peer-To-Peer |
| RIA | Registered Investment Advisor |

| | |
|---|---|
| SAR | Suspicious Activity Report |
| SB/SE | Small Business/Self-Employed |
| SEC | Securities and Exchange Commission |
| SIF | Synthetic Identity Fraud |
| SSA | Social Security Administration |
| SWIFT | Society for Worldwide Interbank Financial Telecommunication |
| TBML | Trade-Based Money Laundering |
| TCO | Transnational Criminal Organization |
| TFI | Terrorism and Financial Intelligence (U.S. Department of the Treasury) |
| TFFC | Terrorist Financing and Financial Crimes (U.S. Department of the Treasury) |
| UAE | United Arab Emirates |
| UI | Unemployment Insurance |
| USPS | U.S. Postal Service |
| USSS | United States Secret Service (U.S. Department of Homeland Security) |
| VASP | Virtual Asset Service Provider |


THE DEPARTMENT OF THE TREASURY
1789