WASHINGTON – Today, the U.S. Department of the Treasury published the 2024 National Risk Assessments on Money Laundering, Terrorist Financing, and Proliferation Financing. These reports highlight the most significant illicit finance threats, vulnerabilities, and risks facing the United States.

The reports detail recent, significant updates to the U.S. anti-money laundering/counter-financing of terrorism framework and explain changes to the illicit finance risk environment. These include the ongoing fentanyl crisis, foreign and domestic terrorist attacks and related financing, increased potency of ransomware attacks, the growth of professional money laundering, and continued digitization of payments and financial services. These assessments also address how significant threats to global peace and security—such as Russia’s ongoing illegal, unprovoked, and unjustified war in Ukraine and Hamas’s October 7, 2023 terrorist attacks in Israel—have shaped the illicit finance risk environment in the United States.

Today’s publications are the fourth iterations of the money laundering and terrorist financing risk assessment, and the third update of the proliferation financing risk assessment, in less than a decade. The public and private sectors can use these updated risk assessments to better understand the current illicit finance environment and inform their own risk mitigation strategies.

“Whether it’s terrorism, drug trafficking, Russian aggression, or corruption, illicit finance is the common thread across our nation’s biggest national security threats,” said Under Secretary of the Treasury for Terrorism and Financial Intelligence Brian E. Nelson. “Treasury, through our National Risk Assessments, is at the cutting edge of analyzing the global risk
environment to protect the U.S. and international financial systems from abuse by illicit actors. We urge both the public and private sectors to engage with these reports, as well as our forthcoming National Strategy for Combatting Terrorist and Other Illicit Finance.”

KEY FINDINGS:

- **Money Laundering:** Criminals use both traditional and novel money laundering techniques, depending on availability and convenience, to move and conceal illicit proceeds and promote criminal activity that harms Americans. The crimes that generate the largest amount of illicit proceeds laundered in or through the United States remain fraud, drug trafficking, cybercrime, human trafficking and human smuggling, and corruption. The United States continues to face both persistent and emerging money laundering risks related to: (1) the misuse of legal entities; (2) the lack of transparency in certain real estate transactions; (3) the lack of comprehensive AML/CFT coverage for certain sectors, particularly investment advisers; (4) complicit merchants and professionals that misuse their positions or businesses; and (5) pockets of weaknesses in compliance or supervision at some regulated U.S. financial institutions.

- **Terrorist Financing:** The United States continues to face a wide range of terrorist financing threats and actors, both foreign and domestic. Consistent with the 2022 risk assessment, the most common financial connections between individuals in the United States and foreign terrorist groups entail individuals directly soliciting funds for or attempting to send funds to foreign terrorist groups utilizing cash, registered money services businesses, or in some cases, virtual assets. The 2024 report also discusses Hamas and the ways they exploit the international financial system, including through solicitation of funds from witting and unwitting donors worldwide. Additionally, domestic violent extremist movements have proliferated in recent years, posing an elevated threat to the United States and continued challenges for law enforcement.

- **Proliferation Financing:** Russia and the Democratic People’s Republic of Korea (DPRK) presented heightened risk since the 2022 assessment. To support its unlawful war in Ukraine, Russia has expanded efforts to illegally acquire U.S.-origin goods with military applications using a variety of obfuscation techniques, such as the use of front
companies and transshipment points around the world. Networks linked to the DPRK increasingly exploit the digital economy, including through hacking of virtual asset service providers and the overseas deployment of fraudulent information technology workers.

Treasury’s Office of Terrorist Financing and Financial Crimes led the assessment process and coordinated closely with offices and bureaus across the Department, relevant law enforcement and regulatory agencies, staff of the federal functional regulators, and across the intelligence and diplomatic communities.

In the coming weeks, Treasury will release the 2024 National Strategy for Combatting Terrorist and Other Illicit Finance, a strategic plan directly informed by the analysis contained in the risk assessments. In the strategy, Treasury will share recommendations for addressing the highlighted issues. This valuable feedback has aided Treasury in assessing and addressing illicit finance risk identified in prior iterations of the strategy to support improvements to the AML/CFT regime, including the launching of the new beneficial ownership reporting requirement that went into effect on January 1, 2024, and informing forthcoming proposed rules to address illicit finance vulnerabilities in the residential real estate sector and for certain investment advisers.

**READ MORE:**

The 2024 National Money Laundering Risk Assessment

The 2024 National Terrorist Financing Risk Assessment

The 2024 National Proliferation Financing Risk Assessment

####
Department of the Treasury

National Money Laundering Risk Assessment (NMLRA)
# Table of Contents

EXECUTIVE SUMMARY ........................................................................................................ 1

INTRODUCTION .................................................................................................................. 3

SECTION I. THREATS .......................................................................................................... 5

Fraud ................................................................................................................................... 5
1. Investment Fraud .............................................................................................................. 6
2. Healthcare Fraud .............................................................................................................. 9
3. Update on COVID-19-Related Fraud ........................................................................... 11
4. Elder Financial Exploitation ......................................................................................... 12
5. Special Focus: Check Fraud ......................................................................................... 15
6. Business Email Compromise (BEC) ........................................................................... 17

Drug Trafficking ............................................................................................................ 18
1. Illicit Synthetic Opioids (including Fentanyl) and Heroin ........................................... 19
2. Priority DTO Threat Actors ......................................................................................... 21

Cybercrime ..................................................................................................................... 23
1. Ransomware ................................................................................................................ 23
2. Malware ........................................................................................................................ 25

Professional Money Laundering .................................................................................. 26
1. Money Mule Networks ................................................................................................. 27
2. Chinese Money Laundering Organizations and Networks ........................................ 29
3. Special Focus: Russian Money Laundering and Sanctions Evasion ......................... 31

Corruption ...................................................................................................................... 32
1. Foreign Corruption ....................................................................................................... 33
2. Domestic Corruption .................................................................................................... 34
3. Special Focus: Unlawful Campaign Finance ............................................................... 35

Human Trafficking & Human Smuggling ..................................................................... 36
1. Human Trafficking ....................................................................................................... 36
2. Human Smuggling ....................................................................................................... 39

Special Focus: Tax Crime ............................................................................................. 40

Update on Wildlife Trafficking and other Nature Crimes ............................................. 41
1. The Intersection of Nature Crimes with Other Threats .............................................. 41

SECTION II. VULNERABILITIES AND RISKS .............................................................. 43

Cash ................................................................................................................................... 43
1. Bulk Cash Smuggling .................................................................................................. 43
2. Cash Consolidation Cities .......................................................................................... 44
3. Cash-Intensive Businesses and Front Companies ..................................................... 46
4. Funnel Accounts ....................................................................................................... 47

Financial Products and Services .................................................................................. 48
1. Money Orders .............................................................................................................. 48
EXECUTIVE SUMMARY

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

The 2024 National Money Laundering Risk Assessment (NMLRA) examines the current money laundering environment and identifies the ways in which criminals and other actors seek to launder funds. It aims to inform the understanding of illicit finance risk by governmental and private sector actors, strengthen risk mitigation strategies of financial institutions, and enhance policy deliberations by the U.S. government. As this NMLRA discusses, criminals constantly develop and adopt new ways to launder illicit funds. Thus, there is a need to constantly track and address evolving money laundering trends and methodologies.

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

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

Another concerning money laundering vulnerability is the lack of comprehensive AML/CFT regulations for certain financial intermediaries, such as investment advisers, that may not be directly subject to comprehensive AML/CFT regulations or generally examined for AML/CFT compliance. Treasury plans to issue in the first quarter of 2024 an updated NPRM that would propose applying AML/CFT requirements pursuant to the Bank Secrecy Act, including suspicious activity reporting obligations, to certain investment advisers. Additionally, the 2024 NMLRA highlights a number of new financial services that criminals seek to exploit, such as so-called “decentralized finance” (DeFi) and online gaming. Illicit actors, including ransomware cybercriminals, thieves, scammers, and the Democratic People’s Republic of Korea (DPRK) cyber actors, are now using DeFi services to transfer and launder their illicit proceeds. In recent years, legal and technological developments have led to substantial growth in online gaming activity in the United States. The anonymity afforded by online gaming and the size and rapid growth of this sector now present unique money laundering risks.
Over the last 50 years the United States has built a robust AML/CFT framework to address illicit finance risk. The United States Department of the Treasury and its interagency partners continue to ensure that the U.S. AML/CFT regime stays ahead of criminals who use existing and emerging techniques to launder the profits of their crimes.

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

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

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

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

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

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

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

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

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

¹ The potential loss from fraudulent scams and cyberattacks reported to the FBI in 2022 equaled $10.3 billion, which is assumed to underrepresent actual loss based upon the voluntary nature of reporting to the FBI Internet Crime Center (IC3). See Federal Bureau of Investigation (FBI), “2022 Internet Crime Report,” FBI Internet Crime Complaint Center, [https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3Report.pdf](https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3Report.pdf). See Figure 12.
Some regulated financial institutions remain a money laundering vulnerability despite many having adequate AML/CFT programs. Analysis of these vulnerabilities, including occasional AML/CFT compliance deficiencies, is a key feature of this report.

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

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

This Report was prepared pursuant to Sections 261 and Section 262 of the Countering America’s Adversaries Through Sanctions Act (PL 115-44) as amended by Section 6506 of the FY22 National Defense Authorization Act (NDAA) (P.L. 117-81). The 2024 NMLRA primarily relies on open-source reporting from the Department of Justice (DOJ), the use of publicly available court documentation, and consultations with law enforcement agencies (LEAs). The NMLRA also utilizes information from Bank Secrecy Act (BSA) reporting, such as strategic analysis on suspicious activity reports (SARs) conducted by the Financial Crimes Enforcement Network (FinCEN) as well as various types of enforcement actions taken by U.S. regulatory agencies. (See Annex on Methodology for further information.)

---

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

3 Information from LEAs will be cited as “according to law enforcement sources.”
SECTION I. THREATS

In the context of the NMLRA, money laundering threats⁴ are the predicate crimes that generate illicit proceeds for laundering in, from, or through the United States. Money laundering threats also represent criminal actors such as those engaged in professional money laundering (PML), and TCOs, including DTOs.⁵ Where reliable data exists, this section also discusses the proceeds of crimes generated abroad (e.g., corruption) that are laundered through or in the United States. The findings related to money laundering threats within this risk assessment align with the 2021 AML/CFT National Priorities issued by the FinCEN.⁶

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

Fraud

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

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

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

---

⁴ See ANNEX on METHODOLOGY.
⁵ TCOs, to include DTOs, are identified as AML/CFT National Priorities.
⁷ FinCEN Alert, FIN-2023-Alert005, September 8, 2023
⁸ Fraud is identified as an AML/CFT National Priority.
but to highlight how fraudsters target U.S. citizens and companies and abuse the U.S. financial sector to launder illicit proceeds.

1. Investment Fraud

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

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

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

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

---

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

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

a) **Ponzi Schemes**

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

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

---

17 FBI’s typology refers to the breakdown and subdivision of investment fraud as reported in “Internet Crime Report 2022”. SEC’s typology refers to that provided on Investors.Gov.
21 Investment frauds differ greatly by scheme used. Based on analysis of DOJ cases, the most common narrative is what has been reflected and discussed.
As soon as an investor places virtual assets into a smart contract, the smart contract automatically diverts the investor’s funds to other investors, such that earlier investors are paid with funds from later investors.\textsuperscript{25}

\textit{b) Virtual Asset Investment Schemes}

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

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

\textit{Pig Butchering}

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

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


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

\textsuperscript{28} DOJ, “Middlesex County Man Charged with Laundering $2.1 Million Obtained from Internet-Related Frauds”, (October 11, 2022), https://www.justice.gov/usao-nj/pr/middlesex-county-man-charged-laundering-21-million-obtained-internet-related-frauds#:~:text=Okuonghae laundered at least 21 million, whichever is greater.
to fake virtual asset investment platforms, controlled by the scammer or co-conspirators posing as investment advisers or customer service representatives. Once victims make an initial “investment,” the fake platforms are manipulated to show substantial gains. Sometimes, victims are allowed to withdraw some of these initial “funds” to further engender trust in the scheme. It is not until a large investment is made that victims find that they are unable to withdraw their funds. Even when a victim is denied access to their funds, the fraud is often not yet over. Scammers request additional payments for purported taxes or fees, promising these payments will allow victims access to their accounts. Scammers often continue to steal from their victims and do not stop until they have deprived victims of any remaining savings. In some cases, the criminals prompt victims to liquidate holdings in tax-advantaged accounts or take out home equity lines of credit and second mortgages on their homes to fund purported investments.29

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

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

2. Healthcare Fraud

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

---

29 FinCEN, “FinCEN Alert on Prevalent Virtual Currency Investment Scam Commonly Known as “Pig Butchering” (FIN-2023-Alert005)”, (September 8, 2023), https://www.fincen.gov/sites/default/files/shared/FinCEN_ALERT_Pig_Butchering_FINAL_508c.pdf.
fraudulent activity and run the gamut from corporate fraud, bribery, and kickbacks, to activity resulting in the illicit distribution and diversion of narcotics. These large-scale fraud schemes increase healthcare costs, waste limited resources, and cause an increased risk of mortality. Investigators and prosecutors have employed innovative methods to target particularly egregious activity, given the complexity of these schemes.

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

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

---

38 All states, the District of Columbia, and the U.S. territories have Medicaid programs designed to provide health coverage for low-income people. Although the Federal government establishes certain parameters for all states to follow, each state administers their Medicaid program differently, resulting in variations in Medicaid coverage across the country. See Medicaid Program History, https://www.medicaid.gov/about-us/program-history/index.html.
41 Durable medical equipment (DME) is defined as equipment and supplies ordered by a health care provider for everyday or extended use. Coverage for DME may include oxygen equipment, wheelchairs, crutches or blood testing strips for diabetics.
a) **Telemedicine Fraud**

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

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

3. **Update on COVID-19-Related Fraud**

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

---


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

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

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

4. Elder Financial Exploitation

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

---

48 FinCEN, “FinCEN Alert on COVID-19 Employee Retention Credit Fraud,” FIN-2023-Alert007, (November 22, 2023), [https://fincen.gov/sites/default/files/shared/FinCEN_ERC_Fraud_Alert_FINAL508.pdf](https://fincen.gov/sites/default/files/shared/FinCEN_ERC_Fraud_Alert_FINAL508.pdf).
increasing number of these schemes are now cyber-enabled.\textsuperscript{54} According to the FBI, virtual asset-related losses reported by older adults increased by 350 percent from 2021 to 2022.\textsuperscript{55}

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

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

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

\begin{itemize}
    \item \textsuperscript{54} FinCEN, “Advisory on Elder Financial Exploitation,” (June 15, 2022), \url{https://www.fincen.gov/sites/default/files/advisory/2022-06-15/FinCEN_percent20Advisory_percent20Elder_percent20Financial_percent20Exploitation_percent20FINAL_percent20508.pdf}
    \item \textsuperscript{55} FBI, “Elder Fraud Report,” (2022), \url{https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3ElderFraudReport.pdf} In 2022, the FBI’s Internet Crime Complaint Center received almost 10,000 complaints from victims over the age of 60 involving the use of some type of virtual asset, such as Bitcoin, Ethereum, Litecoin, or Ripple. Losses incurred by these victims totaled over $1 billion.
    \item \textsuperscript{56} CFPB and FinCEN, Memorandum on EFE, \textit{supra} Note 1. See also, FTC Older Consumers Report, \textit{supra} Note 1.
    \item \textsuperscript{57} DOJ, “Associate Attorney General Vanita Gupta Delivers Remarks at the Elder Justice Coordinating Council Meeting,” (Dec. 7, 2021), \url{https://www.justice.gov/opa/speech/associate-attorney-general-vanita-gupta-delivers-remarks-elder-justice-coordinating}
    \item \textsuperscript{59} FinCEN, “Advisory on Elder Financial Exploitation,” (June 15, 2022), \url{https://www.fincen.gov/sites/default/files/advisory/2022-06-15/FinCEN_percent20Advisory_percent20Elder_percent20Financial_percent20Exploitation_percent20FINAL_percent20508.pdf}
    \item \textsuperscript{60} DOJ, “Woodbridge Money Launderer Sentenced for his Role in a Romance Fraud Scheme” (Mar. 11 2022) \url{https://www.justice.gov/usaو-edwa/pr/woodbridge-money-launderer-sentenced-his-role-romance-fraud-scheme&text=Woodbridge percent20Money percent20Launderer percent20Sentenced percent20for percent20his percent20Role percent20in percent20a percent20Romance percent20Fraud percent20Scheme,-Friday percent2C percent20Mar.\textsuperscript{61} DOJ, “Defendant in ‘Grandparent Scam’ Network Sentenced for RICO Conspiracy Targeting Elderly Americans,” (Aug. 17, 2022), \url{https://www.justice.gov/opa/pr/defendant-grandparent-scam-network-sentenced-rico-conspiracy-targeting-elderly-americans.}
virtual assets, and laundering funds through multiple bank accounts, often using fake PII, 62 and through the use of money mules. 63

Call Center Fraud

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

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

In government impersonation scams, the fraudster impersonates a law enforcement agent, Internal Revenue Service (IRS) representative, or other government official. The scammers may also spoof phone numbers or use fake credentials to appear legitimate. Scammers create various scenarios to elicit payment, including that the victim has missed jury duty and must provide payment immediately to avoid arrest or must provide personal information to renew a driver’s license, passport, or medical license. 67

These types of scams frequently emanate from call centers in South Asia, mainly India, and often target Americans. 68 In 2022, with the assistance of U.S. law enforcement, Indian law enforcement accomplished multiple call center raids, disruptions, seizures, and arrests of the individuals alleged to be involved in perpetrating these cyber-enabled financial crimes and global telemarketing frauds.

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

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

5. **Special Focus: Check Fraud**

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

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

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

---


71 Id.

72 FDIC, “Remote Deposit Capture: A Primer,” (Updated: June 6, 2023), https://www.fdic.gov/regulations/examinations/supervisory/insights/sisum09/sisum09-summer2009-article02.html#:~:text=RDC percent20allows percent20financial percent20institution,percent20customers,percent20instant percent20credit percent20to percent20their percent20account.


74 Id.


78 FinCEN, “FinCEN Alert on Nationwide Surge in Mail Theft-Related Check Fraud Schemes Targeting the U.S. Mail,” FIN-2023-Alert003, (February 27, 2023), https://www.fincen.gov/sites/default/files/shared/FinCEN%20Alert%20Mail%20Theft-Related%20Check%20Fraud%20FINAL%20508.pdf.
U.S. law enforcement has also observed an increase in check fraud activity, with fraudsters targeting checks from businesses and checks with large dollar amounts due to a perception that the accounts the checks draw from are well funded and the checks will not bounce, leading to large losses and unpaid bills for victims.

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

**Mail Theft-Related Check Fraud**

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

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

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

---


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

81 FinCEN, “FinCEN Alert on Nationwide Surge in Mail Theft-Related Check Fraud Schemes Targeting the U.S. Mail”, (February 7, 2023), [https://www.fincen.gov/sites/default/files/shared/FinCEN percent20Alert percent20Mail percent20Theft-Relatedpercent20Check percent20Fraud percent20FINAL percent200508.pdf](https://www.fincen.gov/sites/default/files/shared/FinCEN%20Alert%20Mail%20Theft-Related%20Check%20Fraud%20FINAL%200508.pdf).


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

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

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

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

6. Business Email Compromise (BEC)

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

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

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

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

In March 2023, FinCEN issued a Financial Trends Analysis on patterns and trends identified in BSA data relating to BEC in the real estate sector in 2020 and 2021.⁸⁹ FinCEN found that the sector remains a target for BEC attacks exploiting the high monetary values generally associated with real estate transactions and the various communications between entities involved in the real estate closing process (e.g., title companies, title agents, closing agents, and escrow companies, and other individuals and entities involved in the title and closing processes). Perpetrators of BEC in the real estate sector may obtain unauthorized access to networks and systems to misappropriate confidential and proprietary information to increase the likelihood that their scam is successful.

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

**Drug Trafficking**

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

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

---


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

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

1. **Illicit Synthetic Opioids (including Fentanyl) and Heroin**

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

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

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

\(^91\) See Section on CMLOs.


\(^93\) To include pill presses, encapsulating machines, and die molds.


\(^95\) CDC, “Drug Overdose Deaths Remained High in 2021” (update August 22, 2023), [https://www.cdc.gov/drugoverdose/deaths/index.html#:~:text=Opioids percent20were percent20involved percent20in percent20and percent20without percent20synthetic percent20opioid percent20involvement](https://www.cdc.gov/drugoverdose/deaths/index.html#:~:text=Opioids percent20were percent20involved percent20in percent20and percent20without percent20synthetic percent20opioid percent20involvement).

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

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

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

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

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

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

2. Priority DTO Threat Actors

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

a) Sinaloa and CJNG (Mexico)

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

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


104 DTO Activity as a national AML/CFT priority.


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

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

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

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

\textbf{b) Clan del Golfo (Colombia)}

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


\textsuperscript{108} Ibid.

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

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

Cybercrime

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

1. Ransomware

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

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

Ransomware actors will often target entities that they assess are more likely to pay a ransom, focusing the attack on the victim’s most sensitive data. Attackers may also use multiple forms of extortion. Ransomware actors may pressure victims or a family member to pay a ransom, for example, by stealing confidential data and threatening to publish the data. However, law enforcement identified that ransomware groups have learned that they can extract ransoms by only stealing data and forgoing encryption, which is often the first step of traditional ransomware attacks.

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

---

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

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

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

The DOJ has also worked to prosecute individuals guilty of laundering the proceeds of ransomware attacks, including Bitzlato referenced above. Additionally, in February 2023, Denis Mihaqlovic Dubnikov,
a Russian virtual asset money launderer, pleaded guilty to one count of conspiracy to commit money laundering. Dubnikov and his co-conspirators laundered the proceeds of Ryuk ransomware attacks on individuals and organizations throughout the United States and abroad. After receiving ransom payments, Ryuk actors, including Dubnikov, engaged in international financial transactions to conceal the nature, source, location, ownership, and control of the ransom proceeds.\footnote{DOJ, “Russian Cryptocurrency Money Launderer Pleads Guilty”, (February 7, 2023), \url{https://www.justice.gov/usao-or/pr/russian-cryptocurrency-money-launderer-pleads-guilty}.}

2. Malware

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

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

Law enforcement has observed that cybercriminal groups using malware often launder funds using similar methods as ransomware actors. For example, in April 2023, the FBI announced a coordinated international operation against Genesis Market, a criminal online marketplace that advertised and sold packages of account access credentials that had been stolen from malware and infected computers around the world.\footnote{DOJ, “Criminal Marketplace Disrupted in International Cyber Operation”, (April 5, 2023), \url{https://www.justice.gov/opa/pr/criminal-marketplace-disrupted-international-cyber-operation}.} Since its inception in March 2018, Genesis Market has offered access to data stolen from over 1.5 million compromised computers worldwide containing over 80 million account access credentials. Genesis Market sold device “fingerprints,” unique combinations of device identifiers and browser cookies that may be used to circumvent anti-fraud detection systems used by many websites. The combination of stolen access credentials, fingerprints, and cookies allowed purchasers to assume the victim’s identity by tricking third-party websites into thinking the Genesis Market user was the actual owner of the account. OFAC concurrently designated Genesis Market as a specially designated national (SDN) under its cyber-related sanctions program.\footnote{Treasury, “Treasury Sanctions Illicit Marketplace Genesis Market”, (April 5, 2023), \url{https://home.treasury.gov/news/press-releases/jy1388}.}

Additionally, in March 2023, the DOJ charged the founder of BreachForums for creating and administering
a major hacking forum and marketplace for cybercriminals. The founder allegedly operated BreachForums as a marketplace for cybercriminals to buy, sell, and trade hacked or stolen data, harming millions of U.S. citizens and hundreds of U.S. and foreign companies, organizations, and government agencies. According to the complaint, the platform offered stolen data such as bank account information, social security numbers, other PII, hacking tools, breached databases, and account login information for compromised online accounts with service providers and merchants.

**Professional Money Laundering**

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

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

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


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

1. Money Mule Networks

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

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

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

131 DOJ, “Queens Man Sentenced To 121 Months In Prison For Laundering Millions Of Dollars Of Fraud And Hacking Schemes And Committing Bank Fraud“, (March 17, 2023), https://www.justice.gov/usao-sdny/pr/queens-man-sentenced-121-months-prison-laundering-millions-dollars-fraud-and-hacking#text=Damian percent20Williams percent20United percent20States, Business percent20Administration percent20fraud percent20and percent20hacking percent20schemes percent20and percent20bank percent20fraud.


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

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

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

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

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

2. Chinese Money Laundering Organizations and Networks

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

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

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

For example, CMLOs enable Mexican cartels to seamlessly exchange USD derived from the sale of narcotics for Mexican pesos.\textsuperscript{142} Once the CMLO retrieves the criminal cash in the United States, a
comparable sum of Mexican pesos is then released – almost immediately and with nearly non-existent commission rates – to the cartel in Mexico using IVTS schemes (e.g., mirror transactions). Dirty dollars remain in the United States, where at least in part, they are broken down into smaller amounts and deposited into U.S. bank accounts opened by money mules, which sometimes involve international students. This method, known as “smurfing,” allows the cartels to avoid the risk and cost associated with attempting to smuggle bulk cash across our southern border. The CMLO then sells USD to Chinese nationals for a profit, who, in some instances, use the USDs to purchase real estate or even to pay college tuition expenses.

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

**SNAPSHOT: Schemes Involving Electronic Goods**

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

143 DOJ, “Eight Indicted in Money Laundering Ring”, (July 29, 2022), [https://www.justice.gov/usaop-ma/pr/eight-indicted-money-laundering-ring#:~:text=BOSTON percent20 percentE2 percent80 percent93 percent20 Eight percent20individuals, percent20have percent20been, used percent20stolen percent20and percent20 fraudulent; Also see United States District Court (USDC), District of Massachusetts, U.S. v. ZANG, Case 1:22-cr-10185. 
3. **Special Focus: Russian Money Laundering and Sanctions Evasion**

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

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

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

---


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

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

**Corruption**

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

---


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

153 Foreign individuals who are or have been entrusted with a prominent public function, as well as their immediate family members and close associates, See “Joint Statement on Bank Secrecy Act Due Diligence Requirements for Customers Who May Be Considered Politically Exposed Persons”, (August 21, 2020), https://www.fincen.gov/sites/default/files/shared/PEP percent20Interagency percent20Statement_ FINAL percent2008.pdf.


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

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

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

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

### 1. Foreign Corruption

Money laundering tied to foreign corruption primarily involves payments to foreign officials to obtain or retain business, as well as the use of the U.S. financial system to launder the proceeds of corruption.
United States is being used to hide the proceeds of foreign offenses given the size and stability of our financial sector. U.S. law enforcement regularly investigates and prosecutes illicit activities involving extortion, bribery, and misappropriation or embezzlement of public assets by or for the benefit of a public foreign official where the U.S. financial system and markets are misused to disguise or shelter illicit proceeds.

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

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

2. Domestic Corruption

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

---


\(^{164}\) See Southern District of Florida, USA vs. Raul Gorrin Belisario Claudia Patricia Diaz Guillen, and Adrian Jose Velasquez Figueroa, Case 18-cr-80160, superseding indictment.


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

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

3. **Special Focus: Unlawful Campaign Finance**

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

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

---


170 Id.


172 Id.

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

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

**Human Trafficking & Human Smuggling**

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

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

**1. Human Trafficking**

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

---


175 Id.

176 Id.


178 Id.

179 Human trafficking and human smuggling are identified as an AML/CFT National Priority.
concerns, or involvement with the child welfare system or youth homelessness.\textsuperscript{180} Sex trafficking is often facilitated through online social media platforms.\textsuperscript{181}

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

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

Illicit proceeds from human trafficking can be paid or transferred in cash, electronic funds transfers/
remittance systems, credit card transactions, payment apps, or virtual assets.

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

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

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

\textsuperscript{188} Polaris, “The Typology of Modern Slavery”, (August 30, 2023), \url{https://polarisproject.org/the-typology-of-modern-slavery/}.


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

\textsuperscript{191} Id.


2. Human Smuggling

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

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

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


Special Focus: Tax Crime

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

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

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

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

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

**Update on Wildlife Trafficking and other Nature Crimes**

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

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

1. **The Intersection of Nature Crimes with Other Threats**

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

---


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

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

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

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

---


SECTION II. VULNERABILITIES AND RISKS

In the context of the 2024 NMLRA, a money laundering vulnerability is something that facilitates or creates the opportunity to launder money. Vulnerabilities may relate to a specific financial sector or product or a weakness in regulation, supervision, or enforcement. They may also reflect unique circumstances in which it may be difficult to distinguish legal and illegal activity. The methods that allow for the largest amount of money to be laundered quickly or with little risk of being caught present the greatest potential vulnerabilities. This section represents the residual risk of a particular sector or service. It takes into consideration any remaining risk after the effect of mitigating measures including regulation, supervision, and enforcement, among other things.

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

Cash

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

1. Bulk Cash Smuggling

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

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

---

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

216 The United States prohibits knowingly concealing more than $10,000 in currency or other monetary instruments and transporting or transferring or attempting to transport or transfer such currency or monetary instruments across a U.S. border with the intent to evade currency reporting requirements. 31 U.S.C. § 5332. In addition, 18 U.S.C. § 1956 prohibits the international transportation, transmission or transfer of funds (or attempted transportation, transmission or transfer of funds) that the person knows represent the proceeds of an unlawful activity and conducts the transportation, transmission or transfer to disguise circumstances of the unlawful activity or avoid state or federal transaction reporting requirements.
nation's borders. From an inbound perspective, for calendar year (CY) 2023, there were a total of 1,480 seizures of currency and monetary instruments totaling $18 million.\(^{217}\)

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

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

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

2. **Cash Consolidation Cities**

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

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

---

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

\(^{218}\) See 2022 NMLRA, PP.31-32.

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

\(^{220}\) HSI, BSCS statistics as of 9/8/2023.

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

**Case examples**

- In May 2022, a California woman residing in Atlanta, Georgia, was charged with smuggling over $114,000 of cash into Mexico from the United States. According to court documents, the defendant attempted to pass through a Border Patrol checkpoint as a taxi passenger. The vehicle was referred to secondary inspection, when the defendant denied the relevant custom form (i.e., made a negative declaration) for having more than $10,000. However, according to the charges, $114,294 was discovered in her purse.

- In February 2022, a Mexican man was charged with smuggling $195,731 in cash into Mexico. The cash was hidden in the bed and center console of a pickup truck. According to the charges, the defendant attempted to exit the United States through the Juarez-Lincoln Port of Entry in Laredo as a solo driver in a pickup truck. There, he allegedly gave a negative declaration for possessing currency over $10,000.  

### SNAPSHOT: Use of Private Aircraft

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

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

---

**Notes:**

222 Information provided by HSI, BCSC.

223 ICE, “California woman charged with smuggling over $114k inside taxi, following HSI, federal partner, probe,” (May 18, 2022) [https://www.ice.gov/news/releases/california-woman-charged-smuggling-over-114k-inside-taxi-following-hsi-federal#:~:text=However percent2C percent20A percent20search percent20of percent20Zuniga percent27s,a percent20possible percent20percent2024250 percent20maximum percent20fine.](https://www.ice.gov/news/releases/california-woman-charged-smuggling-over-114k-inside-taxi-following-hsi-federal#:~:text=However%2C%20A%20search%20of%20Zuniga%27s,a%20possible%2024250%20maximum%20fine.)


225 See 14 CFR 47.7(c).

226 See 14 CFR 47.3(a)(3).
3. **Cash-Intensive Businesses and Front Companies**

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

LEAs see a wide array of CIBs utilized as front companies such as convenience stores, restaurants, and liquor stores. In recent years, laundering operations have continued to exploit automotive shops including dealers and repair shops as front companies for money laundering. 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.

**Case examples**

- A March 2022 indictment charged multiple codefendants with allegedly using an Oregon beauty salon as a front to launder proceeds for a DTO that dealt fentanyl, heroin, and counterfeit oxycodone pills throughout the Pacific Northwest. Agents seized 115,000 counterfeit Oxycodone pills that contained fentanyl and 57 pounds of heroin as part of their investigation. The salon owner allegedly opened several accounts at different banks for her salon entity. She then made numerous large cash deposits and purchases of cashier’s checks under the guise of “business transactions”. The defendant allegedly used her salon to avoid scrutiny regarding the size of cash-based transactions. After the owner made the deposits and purchased the cashier checks, they used the funds to buy several real estate properties. The salon owner tried to further disguise the source of these funds by claiming the real estate transactions were purchases of “rental properties.”

- A March 2022 indictment charged the owners of a Sacramento area grocery store with operating a front business for a CJNG-supplied cocaine operation. Law enforcement was able to observe laundering by infiltrating the operation. Most laundering activity took place via money remittances and bulk cash smuggling. The laundering activity allegedly involved transporting $230,000 of bulk cash and exchanging it with a DTO associate. Court documents indicate this was one week of cocaine sales. Evidence within the criminal complaint notes the grocery store was allegedly used to store cash, disguise the source of illicit deposits, and support individual remittances to Mexico.

---


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

229 31 C.F.R. § 1010.330.


4. Funnel Accounts

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

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

Case examples

- Pharmacy owners Arkadiy Khaimov and Peter Khaim, who made millions by submitting fraudulent claims for expensive medications during the pandemic, pleaded guilty to conspiracy to commit money laundering in November 2022. The owners used 16 different registered corporate entities to funnel $47 million of illicit funds through their associated bank accounts. The codefendants conspired with an unregistered MSB to trade cash in return for their fraudulent Medicare funds. The scheme then utilized nominee account signatories to act as mules, purchasing cashier checks with the illicit money as a form of deposit. These cashier’s checks and other cash deposits were then aggregated within accounts that the codefendants ultimately owned. This allowed the codefendants to purchase legitimate assets with the proceeds of their fraud scheme.234

- An Oklahoma City restaurant owner was charged with conspiracy to commit money laundering in a May 2023 indictment for using funnel accounts as a vehicle to launder $25 million. A branch manager reported the defendant’s suspicious behavior after they allegedly attempted to open 14 separate accounts for their singular restaurant entity. The defendant moved to another bank after being denied the accounts, where they successfully open 14 accounts that resembled cash deposit funnel accounts. Court documents also detailed a separate financial institution closing the defendant’s accounts due to large deposits and rapid withdrawals.235

- A June 2023 indictment charged a Honduran national with money laundering in connection to their role as a high-level human smuggling coordinator. Court documents outlined the defendant allegedly showing associates how to open additional bank accounts to facilitate funneling activity. Investigators were also able to present a financial accounting ledger that explicitly showed smuggling fees and cash flows. Court documents also claim that the defendant’s organization had money mules deposit cash at several different banks in different regions within the United States. Following these geographically diverse deposits, the criminal actors allegedly withdrew millions of dollars in smuggling proceeds in the Phoenix, Arizona area.236


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

Financial Products and Services

1. Money Orders

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

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

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

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

---

238 31 C.F.R. § 1022.210
239 31 CFR § 1010.310-1010.314 and 31 CFR § 1010.320.
this record keeping requirement by structuring their money order transactions below this requirement, as demonstrated in the following case examples:

**Case examples**

- In February 2022, the U.S. Court of Appeals for the Eleventh Circuit affirmed a defendant’s conviction in a marijuana distribution and money laundering conspiracy. After receiving drugs from California, the defendant helped distribute and launder money for more than 900 kilograms of marijuana by processing drug money through casinos and nail salons before converting the cash into money orders under the $3,000 record keeping threshold.\(^{243}\)

- In January 2023, 24 defendants were charged with marijuana distribution, money laundering, firearms, and related offenses. They allegedly laundered proceeds from the sale of marijuana and edibles through a variety of means, including money transfers; the transportation and delivery of cash, including $179,710 in cash that authorities seized at the Albany International Airport; the purchase of cashier’s checks; real estate transactions; and cash and money order deposits into various bank accounts.\(^{244}\)

2. **Prepaid Cards**

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

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

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


\(^{248}\) 31 C.F.R. 1010.100(ff)(4) and (7).
Prepaid cards can also be used in some cases as a method of cross-border funds transfer, in which two or more prepaid cards are linked to the same account: funds loaded to a prepaid card in the United States, for instance, could be withdrawn from a second, linked card in another country.249

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

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

Case examples
• In March 2023, Chaohui Chen and Wenyi Zheng were sentenced to 21 months and 36 months imprisonment, respectively, after pleading guilty to wire fraud. Under their wire fraud scheme and gift card conspiracy they deceived victims into purchasing prepaid Walmart gift cards and providing that information to the defendants for their personal gain. According to the plea agreement, a typical execution of the scheme involved unnamed third parties who would make false and fraudulent telephone calls, sometimes claiming to the victims they were part of the Social Security Administration. Using false pretenses, the callers would convince victims to purchase prepaid gift cards and provide to them with the 16-digit gift card numbers and unique pins for the gift cards, in return for a cashier’s check in the amount of the gift card purchased. Once in control of the gift cards, the defendants would redeem the gift cards at various stores by purchasing household items and additional prepaid gift cards, which they would convert and use for their personal gain, and neglect to return any of the money to the victims.251

• In June 2022, Yanio Montes De Oca and Atnetys Ferreira Milian were sentenced to 27 months and one year of probation for their respective roles in a conspiracy to commit money laundering. Between December 2015 and July 2019, De Oca laundered thousands of gift cards that were obtained using fraudulent debit and credit cards encoded with information stolen using gas station skimming devices. After obtaining the gift cards from co-conspirators, De Oca sold them and transferred the

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

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

3. **Peer-to-Peer Payments**

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

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

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

---


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

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

Case examples

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

257 31 C.F.R. Part 1022.
259 American Bankers Association, “Peer to Peer Payment Scams,” https://www aba.com/advocacy/community-programs/consumer-resources/protect-your-money/peer-to-peer-payment-scams#~text=Scammers percent20posing percent20as percent20a percent20legitimate,paid percent20for percent20and percent20they percent20disappear.
261 American Bankers Association, “Peer to Peer Payment Scams,” https://www aba.com/advocacy/community-programs/consumer-resources/protect-your-money/peer-to-peer-payment-scams#~text=Scammers percent20posing percent20as percent20a percent20legitimate,paid percent20for percent20and percent20they percent20disappear.
Union, PayPal, Zelle, Venmo, and Cash App.\textsuperscript{262}

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

### Legal Entities and Arrangements

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

#### 1. Legal Entities

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

**Case examples**

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


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

- In September 2022, the DOJ announced federal criminal charges against 47 defendants for their alleged roles in a $250 million fraud scheme that exploited a federally funded child nutrition program in Minnesota during the COVID-19 pandemic. The defendants are alleged to have defrauded the Federal Child Nutrition Program, exploiting changes in the program intended to ensure underserved children received adequate nutrition during the COVID-19 pandemic. The defendants are alleged to have created dozens of shell companies to receive and launder the proceeds of their fraudulent scheme.²⁶⁵

- In May 2022, brothers Luis Enrique Martinelli Linares and Ricardo Enrique Martinelli Linares, both dual citizens of Panama and Italy, pleaded guilty to conspiracy to commit money laundering and admitted to agreeing with others to establish offshore bank accounts in the names of shell companies to receive and disguise over $28 million in bribe proceeds from Odebrecht S.A., a Brazil-based global construction conglomerate, for the benefit of a close relative, a high-ranking public official in Panama. Both were sentenced to 36 months in prison and ordered to forfeit more than $18.8 million, pay a $250,000 fine, and serve two years’ supervised release.²⁶⁶

2. Beneficial Ownership Information

Lack of transparency in legal entity ownership structures has continued to be a challenge for U.S. law enforcement agencies, requiring time and resource-intensive processes to obtain beneficial ownership information (BOI). This issue also remains a key vulnerability globally. A 2022 FATF study on the state of global effectiveness and compliance with the FATF standards revealed that only half of jurisdictions, on average, have the necessary laws and regulations to understand, assess the risks of, and verify the beneficial owners or controllers of legal persons and arrangements. Furthermore, only 9 percent of countries are meeting the overall effectiveness requirements concerning beneficial ownership transparency.²⁶⁷ To strengthen the standard on beneficial ownership transparency for legal persons, in March 2022, FATF adopted significant amendments to Recommendation 24.²⁶⁸ These amendments seek to enhance the quality of BOI collected by governments, facilitate efficient access to BOI by competent authorities (including through registries or an alternative mechanism), and improve international


cooperation. The amendments also include a new requirement for national authorities to collect BOI in the course of public procurement as a means to combat corruption.\(^{269}\)

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

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

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

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

---

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

\(^{270}\) Public Law No. 116-283 (Jan. 1, 2021).


3. Trusts

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

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

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

\(^{273}\) For example, the interest on principal invested, or rental income from property held in trust.


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

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

Case examples

- On June 30, 2022, OFAC issued a Notification of Blocked Property to Heritage Trust, a Delaware-based trust in which OFAC-designated Russian oligarch Suleiman Abusaidovich Kerimov holds a property interest. Heritage Trust was formed in July 2017 for the purpose of holding and managing Kerimov’s U.S.-based assets. Kerimov used a complex series of legal structures and front persons to obscure his interest in Heritage Trust, the funds of which first entered the U.S. financial system through two foreign Kerimov-controlled entities prior to imposing sanctions against him. The funds were subsequently invested in large public and private U.S. companies and managed by a series of U.S. investment firms and facilitators. Kerimov and his proxies used various layers of U.S. and non-U.S. shell companies to hold formal titles to assets and to conduct transactions in a manner that concealed his interest.

- On August 31, 2022, the DOJ announced the return of approximately $686,000 in forfeited criminal proceeds to the Republic of Peru linked to the corruption and bribery of former Peruvian President Alejandro Celestino Toledo Manrique (Toledo) by Odebrecht S.A. (Odebrecht), a Brazil-based construction conglomerate. In the civil forfeiture matter and a related case, the United States alleged that Toledo, while holding public office as President of Peru, solicited millions in bribe payments from Odebrecht in connection with government contracts awarded for construction of the Peru-Brazil Southern Interoceanic Highway, a Peruvian government infrastructure project. Odebrecht

---

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

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

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

Virtual Assets280

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

In the United States, VASPs have AML/CFT obligations if they fall under the BSA definition of a financial institution, which covers banks, broker-dealers, mutual funds, MSBs, futures commission merchants (FCMs), introducing brokers, and other forms of financial institutions.281 Many VASPs in the United States are considered MSBs, but depending on the activities in which the VASP engages, they may be considered FCMs or securities intermediaries such as broker-dealers.282 Foreign-located VASPs that operate wholly or in substantial part in the United States are considered MSBs, unless an applicable exemption applies, and must comply with applicable BSA requirements. Each of these types of financial institutions has AML/CFT obligations, including requirements to establish and implement an effective AML Program283 and

---


280 This report uses the terms “virtual asset” and “VASP (virtual asset service provider),” terms not contained explicitly in U.S. law or regulation, to align with the terminology defined by the FATF. Virtual assets, as used in this report, include non-sovereign-administered digital assets such as convertible virtual currencies [CVCs], like bitcoin and stablecoins. For consistency, this terminology is also used in case examples, but this is intended only to facilitate an understanding of illicit finance risk and does not alter any existing legal obligations. This, however, does not cover central bank digital currencies, which are representations of fiat currency.

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


283 See 31 C.F.R. § 1020.210 (banks); 31 C.F.R. § 1021.210 (casinos and card clubs); 31 C.F.R. § 1022.210 (MSBs); 31 C.F.R. § 1023.210 (brokers or dealers in securities); 31 C.F.R. § 1024.210 (mutual funds); 31 C.F.R. § 1026.210 (futures commission merchants and introducing brokers in commodities).
recordkeeping and reporting requirements, including SAR filing obligations. FinCEN, OFAC, SEC, and the Commodities Futures Trading Commission (CFTC) have issued statements and guidance on regulatory requirements for VASPs.

Further, VASPs that are U.S. persons, like all other U.S. persons, wherever located, are required to comply with economic sanctions programs administered and enforced by OFAC. At the same time, non-U.S. persons may also have OFAC sanctions compliance obligations in some circumstances. Sanctions compliance obligations are the same regardless of whether a transaction is denominated in virtual assets or traditional fiat currency.

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

1. **Inconsistent Compliance with Domestic Obligations**

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

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

---

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


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

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

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

291 See Footnotes 338 and 339.
293 DOJ, “Ian Freeman Sentenced to 8 Years in Prison for Operating a Bitcoin Money Laundering Scheme” (October 2, 2023), https://www.justice.gov/usao-nh/pr/ian-freeman-sentenced-8-years-prison-operating-bitcoin-money-laundering-scheme.
Case examples:

- Binance: In November 2023, Binance Holdings Limited and its affiliates, which operate the world’s largest VASP, Binance.com, entered into the largest resolutions in the Treasury’s history with FinCEN (including a penalty of $3.4 billion) and OFAC (including a penalty of nearly $1 billion), as well as resolutions of parallel investigations by the DOJ and the CFTC. As part of these resolutions, Binance pleaded guilty and paid penalties totaling over $4.3 billion, to resolve the Justice Department’s investigation into violations related the BSA, failure to register as a money transmitting business, and the International Emergency Economic Powers Act.294

- Binance’s founder and CEO also pleaded guilty to BSA violations and resigned from Binance.295 After launching in 2017, Binance quickly became the largest VASP in the world, with the greatest share of its customers coming from the United States. As a result of serving U.S. customers, Binance was required to register with FinCEN as an MSB and to establish, implement and maintain an effective AML program. Due in part to Binance’s failure to implement an effective AML program, including (among other things) failing to perform KYC on a large number of its users, illicit actors used Binance’s exchange in various ways. Furthermore, Binance failed to file SARs on their suspicious transactions, including those related to terrorist financing, ransomware, child sexual abuse materials, as well as darknet markets, scams, and other illicit activity. As part of the resolution with FinCEN, Binance has also agreed to retain an independent compliance monitor for three years and remediate and enhance its AML and sanctions compliance programs. Binance separately has also reached agreements with the CFTC, FinCEN, and OFAC, and the Justice Department will credit approximately $1.8 billion toward those resolutions. Under its settlement with FinCEN, Binance also agreed to significant compliance undertakings, including a groundbreaking five-year monitorship, an independent review of its AML program, and a SAR lookback review.

- Bittrex: In October 2022, OFAC and FinCEN announced that Bittrex, a VASP, had entered into separate settlements of over $24 million and $29 million, respectively.296 Bittrex failed to prevent persons located in sanctioned jurisdictions, namely the Crimea region of Ukraine, Cuba, Iran, Sudan, and Syria, from using its platform to transact approximately $263 million in virtual assets between March 2014 and December 2017. Additionally, from February 2014 to December 2018, Bittrex failed to maintain an effective AML program as required under the BSA by maintaining an inadequate transaction monitoring system on its platform, to address the risks associated with its products appropriately, and failing to file any SARs over a three-year period, including on transactions involving sanctioned jurisdictions. Bittrex’s inadequate AML compliance program and transaction monitoring left its platform open to abuse by bad actors, including money launderers, terrorist financiers, ransomware attackers, and sanctions evaders.

---


2. Inconsistent Implementation of International AML/CFT Obligations

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

3. Obfuscation Tools and Methods

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

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


Criminals are constantly evolving techniques to obfuscate illicit proceeds and are learning how to use these techniques effectively. The pace of change can present challenges for competent authorities.

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

**Case examples**

- In February 2022, two individuals were arrested for an alleged conspiracy to launder virtual assets stolen during a 2016 hack, presently valued at approximately $4.5 billion. Over the last five years, approximately 25,000 of those stolen bitcoin were allegedly transferred out of the defendant’s wallet via a complicated money laundering process that ended with some of the stolen funds being deposited into financial accounts controlled by both defendants.

- A criminal complaint filed by DOJ alleges that the defendants employed numerous sophisticated laundering techniques, including converting bitcoin to other forms of virtual assets, including anonymity-enhanced cryptocurrencies, via chain hopping and depositing the stolen funds into accounts at a variety of VASPs and darknet markets and then withdrawing the funds. In August 2023, one defendant, Ilya Lichtenstein, pleaded guilty to money laundering conspiracy, which carries a maximum penalty of 20 years in prison, and the other defendant, Heather Morgan, pleaded guilty to one count of money laundering conspiracy and one count of conspiracy to defraud the United States, each of which carries a maximum penalty of five years.

**4. Mixing**

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

---


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

\textit{Case examples}

- In March 2023, the DOJ announced a coordinated action against ChipMixer, a virtual asset “mixing” service responsible for laundering more than $3 billion worth of virtual assets.\textsuperscript{305} The operation involved U.S. federal law enforcement’s court-authorized seizure of two domains that directed users to the ChipMixer service and one Github account, as well as the German Federal Criminal Police’s seizure of the ChipMixer back-end servers and more than $46 million in cryptocurrency. As alleged in the complaint, ChipMixer processed hundreds of millions of dollars’ worth of bitcoin connected to or associated with ransomware strains, stolen funds, customers of Hydra Market, and Russian intelligence services. ChipMixer also served U.S. customers but failed to register with FinCEN and employed technology to conceal the operating location of servers to avoid law enforcement detection. In addition to the coordinated action, an individual was charged with money laundering, operating an unlicensed money transmitting business, and identity theft, connected to the operation of ChipMixer.

- In August 2023, the DOJ unsealed an indictment charging a Russian and U.S. national of creating, operating, and promoting Tornado Cash, a virtual asset mixer that facilitated more than $1 billion in money laundering transactions, and laundered hundreds of millions of dollars for the Lazarus Group, the sanctioned DPRK cybercrime organization.\textsuperscript{306} According to the indictment, Tornado Cash service advertised to customers that it provided untraceable and anonymous financial transactions. Storm and Semenov allegedly chose not to implement know-your-customer or anti-money laundering programs as required by law. Even after the Treasury designated Tornado Cash in August 2022, the operators allegedly helped the Lazarus Group to transfer criminal proceeds from a virtual asset wallet that OFAC had designated as blocked property. The operators are each charged with one count of conspiracy to commit money laundering, one count of conspiracy to operate an unlicensed money transmitting business, and one count of conspiracy to violate the International Economic Emergency Powers Act. OFAC also sanctioned Semenov for his role in providing material support to Tornado Cash and to the Lazarus Group.\textsuperscript{307}

\begin{footnotesize}
\begin{itemize}
\item [305] DOJ, “Justice Department Investigation Leads to Takedown of Darknet Cryptocurrency Mixer that Processed Over $3 Billion of Unlawful Transactions” (March 15, 2023), \url{https://www.justice.gov/opa/pr/justice-department-investigation-leads-takedown-darknet-cryptocurrency-mixer-processed-over-3}.\textsuperscript{306}
\item [306] DOJ, “Tornado Cash Founders Charged with Money Laundering and Sanctions Violations”, (August 23, 2023), \url{https://www.justice.gov/opa/pr/tornado-cash-founders-charged-money-laundering-and-sanctions-violations#:\text{According percent20to percent20the percent20indictment percent2C percent20unsealed,laundrying percent20transactions percent2C percent20and percent20laundered percent20hundreds}}.\textsuperscript{307}
\end{itemize}
\end{footnotesize}
5. **Disintermediation**

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

6. **Special Focus: Decentralized Finance (DeFi)**

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

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

---


309 CFTC, “Statement of CFTC Division of Enforcement Director Ian McGinley on the Ooki DAO Litigation Victory” (June 9, 2023), [https://www.cftc.gov/PressRoom/PressReleases/8715-23#:~:text=June percent2009 percent2C percent202023%text=Critically percent20charged](https://www.cftc.gov/PressRoom/PressReleases/8715-23#:~:text=June percent2009 percent2C percent202023%text=Critically percent20charged).

AML/CFT Compliance Deficiencies

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

1. Banks

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

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

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

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

---


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


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

Case examples

• In October 2023, the Federal Reserve Board (FRB) fined Metropolitan Commercial Bank (MCB), of New York, New York, approximately $14.5 million for violations of customer identification rules and deficient third-party risk management practices relating to the bank’s issuance of reloadable prepaid card accounts.318 In 2020, MCB opened prepaid card accounts for illicit actors using stolen identities who subsequently used the accounts to collect more than $300 million in illegally obtained state unemployment insurance benefits. By opening prepaid card accounts through a third-party program manager without having adequate procedures for verifying each applicant’s true identity, MCB violated customer identification rules set forth in the BSA and its implementing regulations. The Board required MCB to improve its customer identification, customer due diligence, and third-party risk management programs.

• In September 2023, FinCEN issued a consent order imposing a civil money penalty of $15,000,000 on Bancréedito International Bank and Trust Corporation, an International Banking Entity operating in Puerto Rico for willfully violating the BSA between October 2015 and May 2022, by failing to timely report suspicious transactions to FinCEN; failing to establish a due diligence program for correspondent accounts established, maintained, administered, or managed in the United States for foreign financial institutions; and failing to implement and maintain an AML program.319 Bancréedito did not comply with SAR reporting obligations, failing to file SARs for years and ignoring violations cited by its primary regulator, the Puerto Rico Office of the Commissioner of Financial Institutions. These transactions included suspicious activity by a Bancréedito executive and suspicious activity involving customers in the high-risk jurisdiction of Venezuela, including customers linked to foreign bribery and money laundering.

• In September 2023, FinCEN assessed a concurrent civil money penalty of $15 million against Shinhan Bank America (SHBA) for willfully violating the BSA from April 2016 through March 2021, including failure to implement and maintain an effective AML program that was reasonably designed to guard against money laundering and failing to timely report several hundred transactions to FinCEN involving suspicious financial activity by its customers processed by, at, or through the bank.320 As a result, tens of millions of dollars in suspicious transactions were not reported to FinCEN in a timely manner, including transactions connected to tax evasion, money laundering, and other financial crimes. The FDIC issued a concurrent civil money penalty of $5 million against SHBA for violations of the BSA and its implementing AML regulations and for failure to comply with the requirements of an FDIC-issued consent order dated June 12, 2017.321 The New York Department of Financial Services also assessed a civil penalty of $10 million for AML-related violations.

• In April 2023, FinCEN assessed a $1.5 million civil money penalty on South Dakota-chartered The Kingdom Trust Company (Kingdom Trust) for violations of the BSA and its implementing regulations. As part of the consent order, Kingdom Trust admitted that it willfully failed to accurately and timely report hundreds of transactions to FinCEN involving suspicious activity by its customers, including transactions with connections to a trade-based money laundering scheme and multiple securities fraud schemes that were the subject of both criminal and civil actions. These failures stemmed from Kingdom Trust’s severely underdeveloped and ad-hoc process for identifying and reporting suspicious activity.322

• In January 2023, the FRB issued a civil money penalty on Popular Bank $2.3 million for processing six Paycheck Protection Program (PPP) loans despite “having detected that the loan applications contained significant indications of potential fraud.”323 Specifically, in addition to the processing and funding of the loans, the Bank failed to timely report the potential fraud which demonstrated “ineffective controls and procedures that resulted in violations of the Bank’s internal BSA protocols”.324

• In December 2022, Danske Bank pleaded guilty and agreed to forfeit $2 billion to resolve the United States’ investigation into Danske Bank’s fraud on U.S. banks related to the Bank’s concealment of the state of its AML/CFT controls. According to court documents, Danske Bank defrauded U.S. banks regarding subsidiary Danske Bank Estonia’s customers and anti-money laundering controls to facilitate access to the U.S. financial system for Danske Bank Estonia’s high-risk customers, who resided outside of Estonia – including in Russia.325 Specifically, between 2008 and 2016, Danske Bank Estonia – which Danske Bank acquired through an acquisition of Finland-based Sampo Bank in 2007 326 – processed $160 billion through U.S. banks on behalf of its high-risk customer base that resided outside of Estonia. By at least February 2014, as a result of internal audits, information from regulators, and an internal whistleblower, Danske Bank knew that some high-risk customers were engaged in highly suspicious and potentially criminal transactions, including transactions through U.S. banks. Danske Bank also knew that Danske Bank Estonia’s anti-money laundering program and procedures did not meet Danske Bank’s standards and were not appropriate to meet the risks associated with the high-risk customers. Instead of providing the U.S. banks that processed Danske Bank’s transactions with truthful information, Danske Bank lied about the state of Danske Bank Estonia’s AML compliance program, their transaction monitoring capabilities, and information regarding Danske Bank Estonia’s customers and their risk profiles. Danske Bank did this allegedly to continue to gain access to the U.S. financial system.327

• In October 2022, OFAC issued a Finding of Violation to Nodus International Bank, an international financial entity in Puerto Rico, for violations of the Venezuelan Sanctions Regulations and the Reporting, Penalties, and Procedures Regulations. According to OFAC documentation, upon


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


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

• In September 2022, the OCC assessed a $6 million civil money penalty against Sterling Bank and Trust, FSB, Southfield, Michigan. According to the consent order, in addition to prudential deficiencies, the Bank failed to implement an adequate system of AML/CFT internal controls and failed to file SARs in a timely manner.329

• In July 2022, OFAC announced that it reached an agreement with American Express National Bank (Amex), a subsidiary of the American Express Company that provides charge and credit card products and travel-related services to consumers and businesses, to settle the potential civil liability for 214 apparent violations of OFAC’s Kingpin sanctions. According to OFAC documentation, Amex processed transactions for an account whose supplemental card holder was designated. A combination of human error and sanctions compliance program deficiencies enabled the account to process $155,189.42 worth of transactions.330

• In July 2022, OFAC issued a Finding of Violation to MidFirst Bank (MidFirst) for violations of the Destruction Proliferators Sanctions Regulations (WMDPSR). According to OFAC documentation, MidFirst maintained accounts for and processed 34 payments on behalf of two individuals added to OFAC’s SDN List for 14 days post-designation. The violations stemmed from the Bank’s misunderstanding of the frequency of its vendor’s screening of new names added to the SDN List against its existing customer base; the vendor only engaged in screening of MidFirst’s entire existing customer base once a month instead of daily.331

• In June 2022, the FDIC issued a consent order regarding Oxford University Bank of Oxford, Mississippi.332 The order required the bank, among other things, to: (1) assess AML/CFT department staffing; (2) appoint a BSA officer; (3) develop, adopt, and implement appropriate CDD procedures; (4) develop and establish a system of internal controls; (5) establish and maintain an independent testing program for compliance with the BSA and its implementing rules and regulations; (6) develop an effective training program and revise the Bank’s AML/CFT Risk Assessment; and (7) develop, adopt, and implement revised procedures and processes for monitoring and reporting suspicious activity.


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

2. Money Services Businesses

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

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

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

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

---

334 31 C.F.R. § 1010.100(ff). See also https://www.fincen.gov/am-i-msb.
335 See previous sections for vulnerabilities unique to check, money orders, and providers and sellers of prepaid access.
Unregistered and unlicensed MSBs can include hawalas and other forms of IVTS. There is no practical or functional distinction between a hawala and any other money transmitter. While it is theoretically possible for IVTS to operate wholly outside the banking system, it is not often the case. Instead, law enforcement investigations indicate IVTS often use an account at a bank to clear and settle transactions internationally. The following are case examples of AML/CFT compliance failures and unregistered or unlicensed MSBs.

**Case Examples**

- In September 2023, Ryan Salame, the co-CEO of FTX’s Bahamian affiliate (FTX Digital Markets Ltd.), pleaded guilty to a conspiracy to make unlawful political contributions and defraud the Federal Election Commission and a conspiracy to operate an unlicensed money transmitting business. Between 2019 and 2021, Salame along with other co-conspirators, owned and operated an unlicensed money-transmitting business to transmit customer deposits of virtual assets and traditional currencies on and off the FTX exchange. Salame opened a fraudulent bank account by using false and misleading statements on the bank’s due diligence questionnaire. Ultimately, Salame agreed to forfeit more than $1.5 billion to authorities.

- In June 2023, a Paraguayan man admitted his role in facilitating an international money laundering conspiracy; he pled guilty to one count of operating an unlicensed money-transmitting business. According to court documentation, the individual was the owner and operator of a money exchange business in the Republic of Paraguay, which was not licensed or registered to operate as a money-transmitting business under the laws of the United States or the state of New Jersey. The individual’s associates traveled to New Jersey and Florida and accepted approximately $800,000 in U.S. currency from purported drug traffickers and caused those funds to be transmitted through the individual’s money exchange business. Using the unlicensed business, the individual caused those funds to be transmitted through accounts located in multiple countries and ultimately caused the funds to be transferred back to an account maintained by the purported drug traffickers. To disguise the illicit source of funds, the individual and his associates coordinated to generate fraudulent invoices that stated legitimate business reasons for the transfers of the laundered funds. Unbeknownst to the individual and one of his associates, the currency they accepted was actually from two undercover FBI agents as part of an undercover investigation of the money laundering network.

- In June 2023, in Massachusetts, a man was charged with money laundering in connection with an alleged unlicensed money transmitting business. The business was allegedly responsible for converting more than $1 million in cash to bitcoin - largely on behalf of scammers and drug dealers. The defendant used his vending machine business and encrypted messaging apps to secretly communicate with customers.

- In May 2023, in Florida, the president, chief executive officer, and founder of Aurae Lifestyle and Club Swann was charged with illegally operating an unlicensed money-transmitting business. The defendant provided fiat and virtual asset financial services to customers through his different lines of

---


business. The conspiracy charge carries a fine up to $250,000.\textsuperscript{345}

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

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

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

3. Securities Broker-Dealers and Mutual Funds

Broker-dealers and mutual funds have AML/CFT obligations under the BSA and their implementing regulations. In its 2024 Examination Priorities, the SEC reiterated that it will continue to focus on AML/CFT programs to review whether broker-dealers and certain registered investment companies are: (1) appropriately tailoring their AML program to their business model and associated AML risks; (2) conducting independent testing; (3) establishing an adequate customer identification program, including for beneficial owners of legal entity customers; and (4) meeting their SAR filing obligations.\textsuperscript{349} The SEC also noted that it will review policies and procedures to oversee applicable financial intermediaries during examinations.


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


of certain registered investment companies. Additionally, the 2023 Examination Priorities highlighted the elevated risk for broker-dealers and certain registered investment companies due to the current geopolitical environment and the increased imposition of OFAC and international sanctions.\(^\text{350}\)

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

**Case examples**

- In September 2023, the SEC announced charges against registered investment adviser DWS Investment Management Americas Inc. (DIMA or DWS), a subsidiary of Deutsche Bank AG, for its failure to develop a mutual fund AML/CFT program. The SEC’s order found that DIMA caused mutual funds it advised to fail to develop and implement a reasonably designed AML program to comply with the BSA and applicable FinCEN regulations. The order also found that DIMA caused such mutual funds’ failure to adopt and implement policies and procedures reasonably designed to detect activities indicative of money laundering and to conduct AML/CFT training specific to the mutual funds’ business.\(^\text{352}\)

- In July 2023, the SEC announced charges against Merrill Lynch, Pierce, Fenner & Smith (Merrill Lynch), and its parent company BAC North America Holding Co. (BACNAH) for failing to file hundreds of SARs from 2009 to late 2019. According to the SEC’s order, BACNAH assumed responsibility for Merrill Lynch’s SAR policies and procedures and for filing their SARs. Over the course of a decade, BACNAH improperly used a $25,000 threshold instead of the required $5,000 threshold for reporting suspicious transactions or attempted transactions where a suspect may have been seeking to use Merrill Lynch to facilitate criminal activity. As a result, BACNAH caused Merrill Lynch to fail to file hundreds of required SARs.\(^\text{353}\)

- In March 2023, the SEC announced settled charges against Utah-based brokerage firm Cambria Capital, LLC, for failing to file SARs on numerous transactions. The SEC’s order finds that from March 2017 through May 2019, Cambria failed to file SARs on suspicious activity that raised red flags identified in the firm’s anti-money laundering policies and procedures. According to the SEC’s order, most of the suspicious activity was associated with the liquidation of microcap securities, including the deposit of physical certificates; the liquidation of large quantities of microcap securities; and the immediate wire out of liquidation proceeds from customer accounts. In addition, the order also finds that in many of these transactions, the pattern of liquidations often occurred in combination with other red flags noted in Cambria’s policies and procedures, such as unusually large deposits; suspicious wire activity; or multiple accounts simultaneously trading in the same microcap security.\(^\text{354}\)


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

4. Complicit Professionals

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

Case examples

• In January 2024, Peter McVey, who served as vice president and director of treasury services for a Missouri bank, pleaded guilty to failing to maintain an appropriate anti-money laundering program under the BSA. According to court documents, between April 2014 and July 2022, McVey assisted high-risk bank customers engaged in deceptive sweepstakes and short-term online loan activities in evading the bank’s AML/CFT controls. Specifically, McVey worked with other bank officials and customers to submit fraudulent CTR exemption forms to FinCEN and knowingly accepted forged bank forms from customers that permitted them to exceed applicable limits on daily transaction values. McVey also admitted that he did not follow KYC or SAR requirements.\(^356\)

• In October 2023, a New Jersey-based employee of an international financial institution was arrested for accepting bribes to facilitate millions of dollars of money laundering.\(^357\) According to documents filed in this case and statements made in court, in early 2022, the employee exploited his position as a bank employee to facilitate money laundering activities in exchange for bribes. The employee used his position and inside access to open bank accounts in the names of shell companies with nominee owners. Those accounts were then used to launder narcotics proceeds, including to Colombia. The employee allegedly assisted the money laundering efforts by giving those who bribed him online access to the accounts, along with dozens of debit cards for the accounts that were later used to withdraw cash from ATMs in Colombia. The employee allegedly received thousands of dollars in bribes for each account he opened. The investigation has revealed that millions of dollars were laundered to Colombia through accounts opened by the employee since early 2022.


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

**Luxury and High-Value Goods**

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

1. **Real Estate**

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

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

---


enterprises, must establish AML/CFT programs and file SARs. However, an estimated 20 to 30 percent of residential real estate purchases in the United States are non-financed and not fully subject to comprehensive AML/CFT requirements. Since 2002, “persons involved in real estate closings and settlements” have received a temporary exemption from compliance as a financial institution from FinCEN and are exempt from instituting and maintaining comprehensive AML/CFT programs.

Because of the key role real estate professionals play in closings and settlements, this is a critical vulnerability, and real estate professionals have been found to act as both witting and unwitting participants in money laundering schemes. Currently, under FinCEN’s Real Estate Geographic Targeting Order (GTO), in effect since 2016, title insurance companies involved in the non-financed purchase of residential real estate by a legal entity in select jurisdictions are required to report the legal entity’s beneficial ownership information. FinCEN has utilized this tool to gather information about vulnerabilities in the non-financed market, and the Real Estate GTOs currently cover 69 counties. However, GTOs are time-limited and location-specific and remain a temporary solution to information gaps. In December 2021, the Treasury issued an advance notice of proposed rulemaking (ANPRM) to solicit public feedback on how to address the risks associated with this sector. Building on this information and public feedback, FinCEN has an NPRM in OMB review that will continue the process of addressing money laundering vulnerabilities in the residential real estate sector.

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

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

362 31 USC § 5318 (g),(h).
or source of funds for the property, the use of all-cash payments to avoid the AML/CFT scrutiny that comes with financing, the use of loan-back mortgage schemes to reintegrate illicit proceeds into the licit economy, over or under paying for real estate, and the successive transfer of real estate at a higher value or between legal entities and arrangements or natural persons, sometimes for no consideration.\textsuperscript{369}

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

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

\textbf{Case examples}

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


• In January 2023, a Miami federal grand jury indicted a Venezuelan Supreme Court justice for conspiring to launder bribes he received in exchange for using his position to resolve civil and criminal cases in Venezuela to favor bribe payers. It is alleged that the justice received more than $10 million in bribes, typically from Venezuelan contractors who had received contracts from Venezuelan government-owned entities. The individual allegedly used the bribe proceeds to purchase or renovate real estate around the world, including a villa in Tuscany, Italy, for 2.4 million euros, a luxury villa in La Romana, Dominican Republic, for $1.5 million; a building in Las Mercedes in Caracas, Venezuela, for $1.3 million, and an apartment in Miami for $1.3 million. He also used the bribe proceeds for cars, luxury goods, expensive travel, and musical entertainment.\textsuperscript{373}

• In December 2022, a Russian intelligence agent designated by OFAC was charged with conspiracy to violate the International Emergency Economic Powers Act, bank fraud conspiracy, money laundering conspiracy, and four counts of money laundering in connection with the purchase and maintenance of two condominiums in Beverly Hills, California. As alleged in the indictment, beginning in 2013, the individual and a co-conspirator devised a scheme to purchase and maintain two luxury condominiums in Beverly Hills while concealing his interest in the transactions from U.S. financial institutions. Specifically, the individual used the services of a corporate nominee, a multi-tiered structure of California-based shell companies, and numerous U.S. bank and brokerage accounts. Using this framework, the individual wired approximately $3.92 million to the nominee from overseas accounts in Latvia and Switzerland belonging to companies registered in the British Virgin Islands. The suspect then used the money to pay $3.2 million in cash for real estate in the name of a corporate entity set up by the nominee, with the individual having no visible affiliation with the purchase. The remaining $800,000 was invested in a brokerage account maintained by the nominee and used to pay expenses for the condominiums.\textsuperscript{374}

• In November 2022, an individual in Delaware was sentenced to 45 years in prison for conspiracy to commit money laundering, conspiracy to distribute cocaine, and various other drug and money laundering offenses. According to court records and evidence presented at trial, between 2009 and 2017, the individual and his wife laundered over a million dollars in drug proceeds through the purchase of real estate in Delaware and Pennsylvania using their company, Zemi Property Management. They deposited drug money into several different bank accounts – and asked their friends and family members to do the same – and then used those funds to buy cashier’s checks that funded the property purchases.\textsuperscript{375}

2. **Precious Metals, Stones, and Jewels**

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

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


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

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

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

**Case Examples**

- In June 2023, Eduard Ghiocel and Floarea Ghiocel pleaded guilty to laundering $1.4 million in proceeds from robberies, scams, and fraudulent employment claims.382 Among other actions, the pair stole jewelry from elderly communities in San Diego and pawned the items in jewelry stores in San Francisco. The Ghiocels wired the cash via an MSB to Romania in addition to shipping gold bars, gold coins, and luxury vehicles bought with the stolen proceeds to Romania. These efforts were in support of an international crime ring that targeted elderly victims.

- In April 2023, nine individuals were federally charged with conspiring to defraud the United States, evade U.S. sanctions laws, and money laundering. The conspirators used a web of business entities to obtain valuable artwork from U.S. artists and to secure U.S.-based diamond grading services for the benefit of Nazem Ahmad, who the U.S. sanctioned for being a financier for Hizballah. Ahmad was involved in the international trade of diamonds, real estate development, and the global art market. The defendants used U.S.-based Diamond Grading Company-1 to affect the sale prices of diamonds,
increasing the profit made from the diamonds. By using a network of corporate entities and individuals to hide Ahmad’s involvement, the group attempted to evade U.S. sanctions. ³⁸³

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

3. Update on Art

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

Case Examples

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


4. **Automobiles**

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

**Case examples**

- In November 2022, Daniel Fruits was sentenced to six years in federal prison after pleading guilty to wire fraud and money laundering. According to court documents, Fruits, who was hired to manage and run a Greenwood, Indiana-based trucking company, defrauded his employer out of more than $14 million over a 4.5-year period. From January 2015 through June 2019, a Kentucky-based legal entity invested over $14 million into the trucking company. Fruits used those embezzled funds to purchase real estate; several vehicles, including two Ferraris and a Corvette; farm equipment including a horse trailer; a show horse; expensive jewelry, including multiple Rolex watches; firearms; private jet flights; and high-end escort services.\(^{389}\)

- In May 2022, Stephen Mudd, Jr. was convicted and sentenced for conspiring to commit money laundering by assisting in the unlawful purchase of automobiles with criminal proceeds and was sentenced for a financial crime involving the use of a nominee to purchase automobiles to conceal the source of the funds used. While working as a car salesman, Mudd helped falsify employment and bank account information to facilitate the purchase of automobiles with criminal proceeds—with either the proceeds providing a cash down payment or the means of monthly payments on an automobile loan from a financial institution. Mudd knew that lenders would not extend financing without proof of a legitimate source of income.\(^{390}\)

- In March 2022, James Pinson, the owner of a used car dealership, was convicted of three counts of wire fraud, six counts of mail fraud, one count of aggravated identity theft, and two counts of conspiring to commit money laundering. Evidence at trial revealed that to carry out his scheme, Pinson bought pick-up trucks at wholesale prices at auction, obtained hundreds of copies of Kentucky and West Virginia residents’ driver’s licenses, fraudulently titled the trucks in the name of those residents, and fraudulently induced the auto manufacturer to repurchase the trucks at 150 percent of their retail value. The auto manufacturer issued 350 checks in the names of individual false owners between 2013 and 2015. Pinson forged signatures on all 350 checks and deposited them into his bank account.\(^{391}\)

---

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


Casinos and Gaming

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

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

The casino and gaming industry has expanded considerably in recent years with increases in commercial revenue and an influx of new market participants, such as online gaming platforms. There are roughly 1,500 casinos and card clubs in the United States and commercial revenue from casino gaming and sports betting reached a record $60 billion in 2022. Casino and gaming activity is increasingly dispersed across the United States as a growing number of state, tribal, and territorial jurisdictions legalize and operationalize gaming activity, including online and sports betting. The jurisdictions with the largest commercial casino markets by revenue are Las Vegas (Nevada) and Atlantic City (New Jersey). Casinos and card clubs in these regions are also among the most highly regulated and file among the most SARs in the country. Those BSA requirements include AML program obligations, including written procedures, internal controls, training of personnel, a designated compliance officer, and independent testing, among other requirements. Both casinos and card clubs are also subject to obligations relating to general and gaming-specific SAR and CTR filing as well as recordkeeping, and, other requirements. In addition to federal AML/CFT reporting obligations under the BSA, some states, such as Nevada, require additional state-level reporting by casinos and gaming operators. FinCEN supervises casinos and card clubs and delegated examination authority belongs to the IRS SB/SE.

---

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


395 FinCEN, SAR Filings by Industry, (July 2023), https://www.fincen.gov/sites/default/files/shared/Section percent201 percent20percent20Casino percent20percent20and percent20Card percent20Club percent20SARs.xlsx


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

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

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

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

**Case Examples**

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

---


\(^{399}\) FinCEN, SAR Filings by Industry, (July 2023), [https://www.fincen.gov/sites/default/files/shared/Section percent201 percent20and percent20Club percent20SARs.xlsx](https://www.fincen.gov/sites/default/files/shared/Section percent201 percent20and percent20Club percent20SARs.xlsx).
a luxury apartment and vehicle, all using the proceeds of drug trafficking. The indictment alleges, among other transactions, that $51,000 in cash was seized from a checked bag belonging to one individual; that two other individuals purchased casino chips and placed sportsbook bets totaling over $540,000 and later cashed out more than $445,000; and that members of the group spent tens of thousands of dollars on Rolex and Audemars Piguet watches and a diamond and gold chain.  

- In July 2022, Demetrius Burt Catching was sentenced to 93 months in federal prison after pleading guilty to the distribution of marijuana and money laundering. According to the plea agreement, Catching admitted to distributing marijuana in the Lexington area and then taking the proceeds from the marijuana sales and placing large sports bets and wagers at various Indiana casinos. According to the plea, after Catching was banned from one of the casinos, he recruited others to go in his place to make his wagers and bets. Cash from the wagers was deposited in bank accounts in his name. Catching was also ordered to forfeit approximately $215,000 in proceeds from his drug trafficking and money laundering offenses, and ordered to serve an additional, consecutive term of 55 months for supervised release violations on previous convictions.

- In May 2022, the California Gambling Control Commission issued a stipulated settlement decision and order for Lucky Chances Casino, located in Colma, California. As part of the settlement decision, the commission required the Casino to perform the following actions, among others: (1) fully comply with the BSA and its implementing regulations, (2) report to the Bureau of Gambling Control any examination by FinCEN and IRS any examination regarding the Casino’s compliance with the implementation of the BSA (3) implement and maintain an effective AML program; (4) employ a compliance officer to ensure compliance with the BSA; (5) and hire a qualified independent consultant to review the effectiveness of the Casino’s AML program.

1. **Special Focus: Online Gaming**

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

a) **Sports Betting**

Since the U.S. Supreme Court overturned a broad prohibition on regulated sports betting in 2018, U.S.-based persons have collectively wagered more than $220 billion in legal sports bets as of 2023, nearly half of which occurred between 2022 and 2023. Legal sports betting in the United States occurs across numerous settings, including at in-person sportsbooks (which can be co-located on casino premises)
and at sporting events, such as stadiums and racetracks. However, most sports betting activity in the United States occurs via online or mobile gaming platforms. These platforms generally operate either (1) as third-party operators through licensing arrangements with BSA-covered casinos that are licensed at the state, tribal, or territorial level; or (2) by acquiring online gaming operator licenses or permits directly from relevant authorities without an affiliation with a brick-and-mortar, BSA-covered casino.

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

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

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

---

404 See 31 CFR 1010.100(t)(5)(i) and 31 CFR 1010.100(ff)(5)(i)(A).
b) **Offshore Online Gaming**

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

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

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

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

### Entities Not Fully Covered by AML/CFT Requirements

#### 1. **Investment Advisers**

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

---


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

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

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

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

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

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


\textsuperscript{416} In most of the identified cases, authorities pursued civil or criminal enforcement for violations of the federal securities laws against the investment adviser or other associated individuals.
relationship with the client (or, in the case of private funds, the ultimate investor). They may be unable to require an IA to disclose relevant information. At the same time, entities that can obtain information about ultimate clients and investors (typically the IA and certain service providers for the advised fund) are not required to do so, nor are they required to report potentially suspicious activity. Third, certain business practices often promote the secrecy of client/ or investor identity and information and the outsourcing of key compliance responsibilities.

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

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

Case examples

• In December 2021, a founder of a New York financial advisory and investment company was charged with wire fraud, IA fraud, and money laundering in connection with a scheme to misappropriate more than $1 million from current and prospective clients. As alleged in the indictment, the former investment adviser executed a calculated scheme in which he repeatedly lied to his current and prospective clients about putting their money into legitimate investments, when, in reality, he stole their money to fund his lavish lifestyle. As noted in the indictment, the victims sent multiple wire transfers to the private bank account of the IA's investment firm. The IA then misappropriated the funds into his personal banking account, among other things.418

• In November 2019, Mark Scott, a former equity partner at the law firm Locke Lord LLP, was convicted of one count of conspiracy to commit money laundering and one count of conspiracy to commit bank fraud. Beginning in 2016, Scott established fake private equity investment funds in the British Virgin Islands, known as the “Fenero Funds” to launder approximately $400 million in proceeds from a large international pyramid fraud scheme called OneCoin. Scott claimed that the investments were from “wealthy European families,” when in fact the money represented proceeds of the OneCoin fraud scheme. Scott layered the money through Fenero Fund bank accounts in the Cayman Islands and the Republic of Ireland. As part of the scheme, Scott and his co-conspirators lied to banks, including U.S. banks and other financial institutions, to cause those institutions to make transfers of OneCoin proceeds and evade AML procedures.419

---


2. Third-Party Payment Processors

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

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

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

---


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

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

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

Case Examples

- In May 2023, Stephen Short was sentenced in federal court to 78 months in prison for conspiracy to commit wire and bank fraud in connection to a scheme to obtain credit card processing services for his telemarketing operation through a third-party credit card processing network. Between 2012 and 2015, Short targeted customers with outstanding credit card debt to offer services, including debt consolidation and interest-rate reduction, to generate over $19 million in fraud proceeds. The scheme involved collaboration between Short’s company and CardReady, with the latter keeping one-third of credit card sale transactions in exchange for access to the credit card processing network and concealment of the underlying merchant.424

- In July 2022, the executives of Electronic Transactions Systems Corporation were indicted for defrauding approximately 7,000 merchant clients out of millions of dollars. Between 2012 and 2019, the defendants intentionally disguised a portion of processing fees for clients, embedding hidden markups and failing to disclose the true fee structure in billing and account statements. Specifically, the company altered the Interchange fees to include hidden markups by accessing software on computer systems belonging to a third-party company.425 This action facilitated the over-valuing of the company during its acquisition in 2018.426
3. Attorneys

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

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

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

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

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

\(^{428}\) See supra note [375] (Section II, covering BSA/AML compliance deficiencies and complicit professionals, explaining the definition and origin of the term “gatekeeper”).

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

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

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

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

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


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

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

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

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

Case Examples

• In March 2023, Jack Stephen Pursley, a Texas attorney pleaded guilty to conspiring with a former client to repatriate more than $18 million in untaxed income from offshore accounts held in the Isle of Man that the client had earned through his company. Pursley was aware that his client had never paid taxes on these funds. He designed and implemented a scheme whereby fund transfers from an Isle of Man bank account to the United States were disguised as stock purchases in U.S. corporations Pursley and his client owned and controlled. The attorney received more than $4.8 million and a 25 percent ownership interest in his client’s business for his role in the fraudulent scheme.

• In 2022, an Illinois attorney named Hassan Abbas was sentenced for his role in a scheme to defraud victims in multiple states, many of whom thought they were closing real estate transactions or sending money to romantic partners. Once the attorney received the funds, he sent large sums to fellow fraudsters overseas and took a cut, which he used to spend on luxury items and an international lifestyle. When approached by financial institutions about his account activity, the attorney disguised the purposes of wire transfers to bank investigators, claiming that certain transfers were for non-existent “clients” and, in one instance, insisting that information about the wires was protected by the attorney-client privilege.

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


4. Accountants

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

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

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

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

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

- In August 2023, Craig Clayton, the owner of a “virtual CFO” business, agreed to plead guilty to laundering tens of millions of dollars in proceeds from internet fraud schemes by creating shell companies and opening fraudulent business bank accounts. According to the charging documents, from 2019 to 2021, Clayton and others used his accounting and “virtual CFO” business, Rochart Consulting, as a front to launder the proceeds of internet fraud schemes. As part of the conspiracy, Clayton founded shell companies to open business bank accounts in Rhode Island and Massachusetts, through which he laundered the proceeds of internet fraud schemes on behalf of his clients. In total, Clayton laundered more than $35 million.

- In October 2018, San Diego-based CPA Luke Fairfield, was sentenced to 21 months in prison for his role in the criminal enterprise led by former USC football player Owen Hanson – an international drug trafficking, gambling, and MLO known as “ODOG.” Hanson operated ODOG in the United States, Central and South America, and Australia from 2012 to 2016, trafficking in thousands of kilograms of cocaine, heroin, methamphetamine, MDMA (also known as “ecstasy”), and other illegal drugs in wholesale and retail quantities. The ODOG enterprise also operated a vast illegal gambling network focused on high-stakes wagers placed on sporting events. To carry out its gambling operation, the ODOG enterprise employed numerous bookies and money runners, and in the event a customer did not pay his gambling debt, the ODOG enterprise employed enforcers to threaten, intimidate, and injure its customers to force compliance. As Fairfield admitted when pleading guilty in March of 2017, his role in the ODOG enterprise included laundering money, aiding in the creation of shell companies to hide ODOG’s criminal proceeds, and training ODOG money runners on methods and tactics to hide the enterprise’s activities from law enforcement and banks. Because of this conviction, Fairfield is no longer licensed as a CPA.

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


CONCLUSION

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

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

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

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

The findings of the 2024 NMLRA, taken in tandem with the findings of the proliferation finance risk assessment and the terrorist financing risk assessment, will inform the forthcoming 2024 National Illicit Finance Strategy, which will lay out the roadmap to address the threats and vulnerabilities to the U.S. financial system, and ultimately strengthen the integrity of the U.S. financial system.
PARTICIPANTS

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

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

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

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

The NMLRA uses all available information to identify the current money laundering environment within the United States. This initiative includes feedback and input from various private sector participants through formal and informal mechanisms and targeted meetings on illicit finance trends. This action is generally done through outreach following the publication of the previously released NMLRA. Relevant components of agencies, bureaus, and offices of the Treasury, the U.S. Department of Justice (DOJ), the U.S. Department of Homeland Security (DHS), and others listed above, participated in the development of the risk assessment. This year, we engaged with several State agencies, particularly with respect to the Casino and Gaming Section (See list of Participants). Data collected is current as of January 31, 2024.

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

Numerous federal agencies collect data on the outcomes of their illicit finance investigations at the agency, interagency, and government-wide levels. However, a single source of comprehensive, government-wide data on the full range of such outcomes does not exist. Therefore, identifying cases based solely on charges filed is challenging. For instance, although there are specific money laundering statutes, additional statutes might include relevant cases - such as tax evasion - but be overly broad for the purpose of conducting such searches. Furthermore, agencies may charge defendants under the predicate crime instead of under a money laundering-related statute or a prosecutor may drop a money laundering charge as part of a plea bargain. We have identified those cases (mainly citing DOJ or LEA Press Releases) that demonstrate some type of ML activity or how criminal actors used the U.S. financial system to move, disguise, or hide proceeds of crime. Case examples may involve criminal charges in an indictment, which are merely allegations. All defendants are presumed innocent unless, and until, proven guilty beyond a reasonable doubt in a court of law. The case examples only cite the names of those found guilty. We have also utilized qualitative data, often provided by LEAs, when no public sources are available (e.g., press releases or court documentation). When citing qualitative data, the NMLRA makes clear that certain information is “according to law enforcement sources.”

We have incorporated advisories, alerts and bulletins published by our LEAs, FinCEN, and consumer protection agencies (e.g., the Consumer Trade Commission). Examples include public service announcements on various types of frauds/scams. From a drug perspective, we relied on national drug threat assessments and data provided by our health protection agencies (e.g., Centers for Disease Control and Prevention). We also rely on top-down assessments or strategies produced at the national level, which the President of the United States issues. These have included national efforts to combat human...
trafficking, ransomware, and corruption among other criminal threats with a financial nexus. We also use open-source documents from our Intelligence Community such as the “Annual Threat Assessment of the U.S. Intelligence Community.”

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

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

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

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

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

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

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

ACH   Automated Clearinghouse
ABA   American Bar Association
AEC   Anonymity-Enhanced Cryptocurrencies
AML/CFT Anti-Money Laundering / Countering the Financing of Terrorism
ANPRM Advance Notice of Proposed Rulemaking
ATM   Automated Teller Machine
AUM   Assets Under Management
BCS   Bulk Cash Smuggling
BEC   Business Email Compromise
BOI   Beneficial Ownership Information
BSA   Bank Secrecy Act
CBP   U.S. Customs and Border Protection (Department of Homeland Security)
CDD   Customer Due Diligence
CDG   Clan del Golfo
CEO   Chief Executive Officer
CFTC  Commodity Futures Trading Commission
CIB   Cash-Intensive Business
CIP   Customer Identification Program
CJNG  Cártel Jalisco Nueva Generación
CMLO  Chinese Money Laundering Organization
CTA   Corporate Transparency Act
CTR   Currency Transaction Report
CVC   Convertible Virtual Currency
DEA   Drug Enforcement Administration (U.S. Department of Justice)
DeFi  Decentralized Finance
DHS   Department of Homeland Security
DOJ   Department of Justice
DPRK  Democratic Republic of North Korea
DTO   Drug Trafficking Organization
EDD   Enhanced Due Diligence
EFE   Elder Financial Exploitation
EIDL  Economic Injury Disaster Loan
ERC   Employee Retention Credit
FAA   Federal Aviation Administration
FATF  Financial Action Task Force
FBI   Federal Bureau of Investigation
<table>
<thead>
<tr>
<th>Acronym</th>
<th>Full Form</th>
</tr>
</thead>
<tbody>
<tr>
<td>FCM</td>
<td>Futures Commission Merchant</td>
</tr>
<tr>
<td>FCPA</td>
<td>Foreign Corrupt Practices Act</td>
</tr>
<tr>
<td>FDIC</td>
<td>Federal Deposit Insurance Corporation</td>
</tr>
<tr>
<td>FFIEC</td>
<td>Federal Financial Institutions Examination Council</td>
</tr>
<tr>
<td>FFIRAs</td>
<td>Federal Financial Institution Regulatory Agencies</td>
</tr>
<tr>
<td>FinCEN</td>
<td>Financial Crimes Enforcement Network (U.S. Department of the Treasury)</td>
</tr>
<tr>
<td>FINRA</td>
<td>Financial Industry Regulatory Authority</td>
</tr>
<tr>
<td>FRB</td>
<td>Board of Governors of the Federal Reserve System (or “Federal Reserve Board”)</td>
</tr>
<tr>
<td>FTC</td>
<td>Federal Trade Commission</td>
</tr>
<tr>
<td>FY</td>
<td>Fiscal Year</td>
</tr>
<tr>
<td>GTO</td>
<td>Geographic Targeting Order</td>
</tr>
<tr>
<td>IC3</td>
<td>Internet Crime Complaint Center (Federal Bureau of Investigation)</td>
</tr>
<tr>
<td>IOLTA</td>
<td>Interest on Lawyers’ Trust Accounts</td>
</tr>
<tr>
<td>IPO</td>
<td>Initial Public Offering</td>
</tr>
<tr>
<td>IRS-CI</td>
<td>Internal Revenue Service-Criminal Investigation</td>
</tr>
<tr>
<td>IVTS</td>
<td>Informal Value Transfer Service</td>
</tr>
<tr>
<td>ML/TF</td>
<td>Money Laundering/Terrorist Financing</td>
</tr>
<tr>
<td>MLO</td>
<td>Money Laundering Organization</td>
</tr>
<tr>
<td>MSB</td>
<td>Money Services Business</td>
</tr>
<tr>
<td>NCUA</td>
<td>National Credit Union Administration</td>
</tr>
<tr>
<td>NDAA</td>
<td>National Defense Authorization Act</td>
</tr>
<tr>
<td>NDTA</td>
<td>National Drug Threat Assessment</td>
</tr>
<tr>
<td>NPRM</td>
<td>Notice of Proposed Rulemaking</td>
</tr>
<tr>
<td>OCC</td>
<td>Office of the Comptroller of the Currency</td>
</tr>
<tr>
<td>OCDETF</td>
<td>Organized Crime Drug Enforcement Task Forces (U.S. Department of Justice)</td>
</tr>
<tr>
<td>OFAC</td>
<td>Office of Foreign Assets Control (U.S. Department of the Treasury)</td>
</tr>
<tr>
<td>PII</td>
<td>Personally Identifiable Information</td>
</tr>
<tr>
<td>PML</td>
<td>Professional Money Laundering</td>
</tr>
<tr>
<td>PMSJs</td>
<td>Precious Metals, Stones, And Jewels</td>
</tr>
<tr>
<td>PEP</td>
<td>Politically Exposed Person</td>
</tr>
<tr>
<td>PMO</td>
<td>Postal Money Order</td>
</tr>
<tr>
<td>PPP</td>
<td>Paycheck Protection Program</td>
</tr>
<tr>
<td>PRC</td>
<td>People’s Republic of China</td>
</tr>
<tr>
<td>P2P</td>
<td>Peer-To-Peer</td>
</tr>
<tr>
<td>RIA</td>
<td>Registered Investment Adviser</td>
</tr>
<tr>
<td>RMB</td>
<td>Chinese Renminbi</td>
</tr>
<tr>
<td>Acronym</td>
<td>Full Form</td>
</tr>
<tr>
<td>---------</td>
<td>-----------</td>
</tr>
<tr>
<td>SAR</td>
<td>Suspicious Activity Report</td>
</tr>
<tr>
<td>SBA</td>
<td>Small Business Administration</td>
</tr>
<tr>
<td>SB/SE</td>
<td>Small Business/Self-Employed</td>
</tr>
<tr>
<td>SEC</td>
<td>Securities and Exchange Commission</td>
</tr>
<tr>
<td>SDN</td>
<td>Special Designated National</td>
</tr>
<tr>
<td>TBML</td>
<td>Trade-Based Money Laundering</td>
</tr>
<tr>
<td>TCO</td>
<td>Transnational Criminal Organization</td>
</tr>
<tr>
<td>TCSP</td>
<td>Trust and Company Service Provided</td>
</tr>
<tr>
<td>TPPP</td>
<td>Third-Party Payment Processor</td>
</tr>
<tr>
<td>USD</td>
<td>U.S. Dollar</td>
</tr>
<tr>
<td>USPIS</td>
<td>U.S. Postal Inspection Service</td>
</tr>
<tr>
<td>VAIS</td>
<td>Virtual Asset Investment Scheme</td>
</tr>
<tr>
<td>VASP</td>
<td>Virtual Asset Service Provider</td>
</tr>
</tbody>
</table>
2024 National Terrorist Financing Risk Assessment

February 2024
## Table of Contents

**EXECUTIVE SUMMARY** ................................................................. 1

Introduction ...................................................................................... 3

**THREATS** ...................................................................................... 4

Domestic Violent Extremism and Transnational Racially or Ethnically Motivated Violent Extremism .......................................................... 4
  - Domestic Violent Extremism ................................................................. 4
  - Transnational Racially or Ethnically Motivated Violent Extremism .............. 6

Islamic State of Iraq and Syria (ISIS) .................................................... 7

Al-Qa’ida (AQ) ...................................................................................... 9

Hizballah .......................................................................................... 12

Hamas .................................................................................................. 14

**VULNERABILITIES** ........................................................................... 15

Registered Money Services Businesses (MSBs) ........................................... 15
  - Person-to-Person (P2P) Payments .......................................................... 16

Unregistered Money Transmission .............................................................. 17

Cash .................................................................................................... 17

Banks ................................................................................................... 18

Virtual Assets ..................................................................................... 19

Non-Profit Organizations (NPOs) ............................................................. 23

**EMERGING TRENDS** ....................................................................... 25

Crowdfunding & Online Fundraising ......................................................... 25

Conclusion .......................................................................................... 27

Participants .......................................................................................... 28

Methodology and Terminology ................................................................. 29

List of Acronyms .................................................................................. 30
EXECUTIVE SUMMARY

Over the past 20 years, the terrorist threat to the United States has evolved significantly. In that time, our counterterrorism and counter-terrorist financing (CTF) posture has evolved alongside the threat, taking the lessons learned from the immediate aftermath of 9/11 and applying them to new threat actors and terrorist financing (TF) methods.

This 2024 National Terrorist Financing Risk Assessment (NTFRA) comes almost 10 years after the Department of the Treasury (Treasury) published the inaugural NTFRA in 2015. At that time, terrorism was the primary national security threat to the United States, and Al-Qa’ida (AQ) and its affiliates were the primary terrorism threat to the United States. The Islamic State of Iraq and Syria (ISIS) was quickly growing in both size and its use of extreme violence in Iraq and Syria. The United States faced regional terrorism threats from other Sunni jihadist groups in Afghanistan and Pakistan, Southeast Asia, and East Africa. Within the United States, there was a smaller but growing risk of individuals, often referred to as lone wolf terrorists, who were inspired by, but unaffiliated with, foreign terrorist groups and carrying out low-cost attacks using firearms, vehicles, or homemade explosives. Hizballah and other Iranian-backed groups also continued to threaten U.S. foreign interests around the world. While some of these groups relied on Iran, the world’s foremost state sponsor of terrorism, for financial support, others sought funds through kidnapping for ransom or other criminal activity or by exploiting charitable organizations or causes to raise funds. These funds moved primarily through money transmitters (registered and unregistered), banks (where functioning banking systems existed), and cash.

Almost 10 years later, the United States faces a much more complex international security environment in which terrorism is still the greatest threat to the homeland but several other major security threats also exist. Russia and the People’s Republic of China seek to undermine or create alternatives to the U.S.-led rules-based global order. Other shared international challenges, including humanitarian crises, international health concerns, and rapidly emerging or evolving technologies with the potential to disrupt traditional business and society, are increasingly intertwined with broader national security risks. These trends all impact the current terrorism landscape.

Today, the primary terrorism threat to the homeland comes from individuals in the United States who are inspired by AQ, ISIS, or domestic violent extremist (DVE) ideologies and who seek to carry out deadly attacks without direction from a terrorist group. These individuals may be radicalized to violence online through social media and can carry out these attacks with limited warning.

In particular, DVE movements, motivated by racial bias, grievances against authority, or a mix of these and other ideologies, have metastasized over the last decade to become one of the most serious terrorism threats facing the United States, particularly racially and ethnically motivated.

---

1 Office of the Director of National Intelligence, Annual Threat Assessment of the U.S. Intelligence Community, p. 22-24, (Feb. 6, 2023) (ODNI 2023 Annual Threat Assessment).
3 Individuals who commit violent criminal acts in furtherance of ideological goals stemming from domestic influences—some of which include racial or ethnic bias, or strong anti-government or anti-authority sentiments—are described as domestic violent extremists (DVEs), whereas homegrown violent extremists (HVEs) are individuals inspired primarily by foreign violent jihadist beliefs. HVEs are individuals inspired primarily by foreign terrorist groups, but who are not receiving individualized direction from those groups.
violent extremists (RMVE). The last several years have witnessed the emergence of these networks of individuals in the United States who seek to carry out violent attacks against minorities, government authorities, or critical infrastructure.

At the same time, foreign terrorist threats to the United States and U.S. interests persist. The primary threat to the United States overseas comes from ISIS-inspired affiliates that seek to attack the United States, its citizens, and its interests. AQ remains committed to attacking U.S. interests, although the threat is greatest in the regions where its affiliates operate rather than in the U.S. homeland. More recently, the October 2023 terrorist attacks by Hamas against Israel serve as a stark reminder that though much headway has been made in the fight against terrorism, this threat is close at hand. Numerous terrorist groups have called for or threatened attacks on U.S. soil and against U.S. interests abroad since those events. The Hamas attack and subsequent attacks by Hizballah, Palestinian Islamic Jihad (PIJ), and other Iran-affiliated militias showed both the reach of Iran's terrorist proxies to threaten U.S. personnel and allies and how quickly a terrorism threat to the United States and its interests overseas can reemerge.

As the nature of the terrorist threat and the actors involved have grown more varied, terrorist financing in the United States has similarly evolved over the past decade. While some individuals still seek to send money to foreign terrorist groups, many now forgo “financial jihad” and instead focus their efforts (and resources) on attacks on unprotected civilian targets in the United States. ISIS and AQ-related financial activity in the United States is most commonly associated with U.S. persons aspiring to travel abroad to conflict zones or attempting to send money to these groups or affiliates. Funds used to support travel-related activity have primarily been generated from legitimate activities, and cash is often used for these purposes. In some instances, U.S.-based individuals have sought to fundraise extensively or solicited funds specifically for ISIS.

Hizballah continues to utilize the formal and informal U.S. financial system, permissive jurisdictions, as well as sophisticated financial schemes to launder, raise, and move funds. Additionally, as more information regarding the financing of Hamas comes to light after the October 2023 terrorist attacks, it is clear that the group looks to the United States as a venue for generating revenue, casting a large net with diverse methods and sources of fundraising.

While terrorists continue to experiment and adapt to changes in technology, they still utilize tried-and-true methods. Banks and money transmitters are still exploited for their reach and capacity to send large volumes, but some terrorist groups have also increased their capability and understanding of using virtual assets to transfer funds; some groups have also begun experimenting with alternative types of virtual assets. Typologies of TF involving the charitable sector have also shifted from abuse of legitimate charities to sham charities and fraudulent charitable appeals. Lastly, the internet has facilitated a range of nefarious financial activity, and numerous terrorist groups have been observed utilizing crowdfunding and various methods of online fundraising to raise funds from witting and unwitting donors.

---

4 See Testimony of FBI Director Christopher Wray, Worldwide Threats to the Homeland, (Nov. 15, 2023) (FBI 2023 Threats Testimony).
5 Importantly, this risk assessment does not evaluate the actions of individuals engaged solely in activities protected by the First Amendment or other rights secured by the U.S. Constitution.
Introduction

The 2024 NTFRA identifies the TF threats, vulnerabilities, and risks the United States faces, updating the 2022 NTFRA. This report, as well as the 2024 National Money Laundering Risk Assessment (NMLRA) and 2024 National Proliferation Financing Risk Assessment (NPFRA), provide an overview of the current illicit finance risks to the United States. These risk assessments also inform and complement the Anti-Money Laundering and Countering the Financing of Terrorism National Priorities (Priorities) issued by the Financial Crimes Enforcement Network (FinCEN). These Priorities include both international and domestic terrorist financing risks. This assessment was prepared according to Sections 261 and 262 of Countering America’s Adversaries through Sanctions Act (P.L. 115-44) as amended by Section 6506 of the Fiscal Year 2022 National Defense Authorization Act (P.L. 117-81).

Relevant component agencies, bureaus, and offices of Treasury, the Department of Justice (DOJ), federal financial regulators, and other government agencies participated in developing the risk assessment. The 2024 NTFRA is based on an analysis of criminal prosecutions, discussions with relevant authorities and private sector entities, a review of government actions and analysis, including Treasury designations and private sector research issued since the 2022 NTFRA.

---

7 The 2022 NTFRA is available at 2022 National Terrorist Financing Risk Assessment (treasury.gov).
9 With respect to information collected from pending cases, the charges contained in an indictment are merely allegations. A defendant is presumed innocent unless, and until, proven guilty beyond a reasonable doubt in a court of law.
10 The review period is from January 1, 2022, to December 31, 2023.
THREATS

Domestic Violent Extremism and Transnational Racially or Ethnically Motivated Violent Extremism

Domestic Violent Extremism

Law enforcement agencies have stated that the threat posed by DVEs\(^\text{11}\) is one of the most pressing terrorism threats to the United States.\(^\text{12}\) A DVE is an individual based and operating primarily in the United States, without direction or inspiration from a foreign terrorist group or other foreign power, who seeks to further political or social goals wholly or in part through unlawful acts of force or violence.\(^\text{13}\) The U.S. government uses the following five categories, based on ideological motivations, to group DVE actors: (1) racially or ethnically motivated violent extremists (RMVE); (2) anti-government or anti-authority violent extremists (AGAAVE) (including militia violent extremists (MVE)); (3) animal rights or environmental violent extremists; (4) abortion-related violent extremists; and (5) other DVE threats that do not fall into the prior four categories.\(^\text{14}\)

Domestic terrorism investigations have more than doubled since 2020, according to the Federal Bureau of Investigation (FBI).\(^\text{15}\) The U.S. Intelligence Community (IC) has assessed that the DVE threat is fueled by a range of ideological and sociopolitical grievances, exacerbated by galvanizing issues such as perceived election fraud, the COVID-19 pandemic, and immigration policy, among other issues, and this threat will continue to persist for the foreseeable future.\(^\text{16}\)

The most concerning threat categories of DVE are RMVE actors, particularly those driven by a belief in the superiority of the white race, as discussed in more detail in the next section. RMVEs pose the most consistent threat of lethal and non-lethal violence against religious, cultural, and government targets.\(^\text{17,18}\) Threats have also increased in the past two years from AGAAVEs, including those motivated by a desire to commit violence against individuals or entities they perceive to be associated with a specific political party or faction thereof.\(^\text{19}\)

In recent years, U.S. government personnel, including military and law enforcement, have increasingly become a target of DVEs, especially by MVE actors.\(^\text{20}\) In addition, DVEs have increasingly called for

---

\(^{11}\) Some entities use the terms DVE and Domestic Terrorism (DT) interchangeably, but consistent with law enforcement, this assessment will use DVE as the label for an individual or group until a violent or terrorist act is committed, and then use DT after that point.

\(^{12}\) FBI/DHS Intel Assessment on DT, p. 2.

\(^{13}\) Office of the Director of National Intelligence, Domestic Violent Extremism Poses Heightened Threat in 2021, p. 3 (Mar. 1, 2021) (ODNI DVE Assessment).


\(^{15}\) FBI 2023 Threat Testimony.

\(^{16}\) ODNI DVE Assessment, p. 2, FBI/DHS Intel Assessment on DT, p.37.

\(^{17}\) FBI/DHS Intel Assessment on DT, p. 6.

\(^{18}\) In May 2023, DHS named these as the targets: “US critical infrastructure, faith-based institutions, individuals or events associated with the LGBTQIA+ community, schools, racial and ethnic minorities, and government facilities and personnel, including law enforcement.” See https://www.dhs.gov/ntas/advisory/national-terrorism-advisory-system-bulletin-may-24-2023.

\(^{19}\) Id.

\(^{20}\) FBI/DHS Intel Assessment on DT, pp. 37, 40.
physical attacks on critical infrastructure. DVEs, particularly RMVEs promoting accelerationism—an ideology that seeks to destabilize society and trigger a race war—have encouraged mobilization against lifeline and other critical functions, including attacks against the energy, communications, and public health sectors.21

- In February 2023, two individuals were charged federally with conspiracy to destroy an energy facility. From at least June 2022 to the present, one of the defendants conspired to carry out attacks against critical infrastructure, specifically electrical substations, in furtherance of his racially or ethnically motivated violent extremist beliefs. The second defendant collaborated on a plan to carry out the attacks.

- In April 2023, two individuals were sentenced for conspiring to provide material support to terrorists, with a third co-conspirator previously pleading guilty in February 2022.22 As part of the conspiracy, each defendant was assigned a substation in a different region of the United States. The plan was to attack the substations, or power grids, with powerful rifles. The defendants believed their plan would cost the government millions of dollars and cause unrest for Americans in the region. They had conversations about how the possibility of the power being out for many months could cause war, even a race war, and induce the next Great Depression.

For most DVE attacks, the predominant means of funding is self-financing.23 These funds generally come through legal means, such as personal savings or earned income. In some cases, radicalized individuals engage in legitimate commercial activity, like selling t-shirts or other merchandise, to raise funds for certain groups. Other DVEs have sought to profit from illicit activity such as drug trafficking.24 DVEs have also used online forums and crowdfunding websites to solicit donations from other people, often for activities like legal fees or travel to training camps or protests, much of which is constitutionally protected. Some DVEs have solicited or transferred funds in virtual assets or expressed interest in using virtual assets to move funds pseudonymously.25

Many DVEs and those supporting them have a sophisticated understanding of what conduct (financial or otherwise) is permissible versus illegal, making it challenging to link financial activity with violent conduct. Further, the fact that most DVE attacks are self-funded through legitimate sources means that associated transactions may not appear suspicious, making it difficult for financial institutions to identify associated transactions prior to an attack. This limits financial institutions’ ability to identify and notify law enforcement pre-emptively about a given individual who may be linked to acts of violence.26

24 Id.
Transnational Racially or Ethnically Motivated Violent Extremism

According to an assessment by the Office of the Director of National Intelligence (ODNI), “transnational RMVEs continue to pose the most lethal threat to U.S. persons and interests, and a significant threat to U.S. allies and partners through attacks and propaganda that espouses violence.” RMVEs’ ideologies, especially those involving white supremacy or neo-Nazism, often transcend domestic boundaries as the ideology itself is shared by other individuals and groups around the world. Transnational RMVEs have had some contact with individuals and like-minded movements within the United States. The FBI assesses that in the United States, those advocating for white supremacy are the most likely subcategory of RMVEs to have transnational connections with foreign extremists that espouse similar beliefs, including in Australia, South Africa, Canada and throughout Europe. This contact often occurs online; decentralized, transnational networks of RMVEs have proliferated online in recent years. Some U.S.-based RMVEs have traveled abroad to meet with like-minded individuals or groups. Additionally, evidence suggests that some RMVE attacks abroad have inspired individuals in the United States to commit similar attacks.

Russia’s war against Ukraine has elevated the popular appeal and strengthened the international nexus of certain RMVE groups. The IC has noted that the Ukraine war could present RMVE groups with an opportunity to gain battlefield experience and military equipment. In June 2022, Treasury’s Office of Foreign Assets Control (OFAC) designated two key supporters of the Russian Imperial Movement (RIM), a white supremacist, ultranationalist, paramilitary organization based in Russia with transnational connections that has carried out acts of terrorism around the world. In 2020, RIM became the first white supremacist RMVE group to be designated as a terrorist group by the U.S. State Department. RIM has sought to exploit the Russian war in Ukraine for its own benefit, provided paramilitary-style training to ideologically aligned individuals in Europe, and has had contact with organizations in the United States on an informal basis.

Financial connections between international RMVE groups and U.S.-based RMVEs with similar ideologies are tenuous so far. Crowdfunding websites have served as one nexus between U.S.-based RMVE actors and individuals located overseas, but there is no evidence to suggest any significant or

27 ODNI 2023 Annual Threat Assessment, p. 33.
29 Id.
31 ODNI 2023 Annual Assessment, p. 33: “Terrorgram, a loosely connected network of channels on the messaging application Telegram, has circumvented multiple efforts to moderate content. Terrorgram serves as a transnational forum for RMVEs to share propaganda, exchange operational guidance, and valorize the perpetrators of previous terrorist attacks.”
32 Id.
33 Testimony of Dr. Joshua Geltzer, p.2.
34 ODNI 2023 Annual Threat Assessment, p. 33.
36 RIM was also designated as a terrorist group by Canada in 2021.
large-scale financial connections between U.S. RMVEs and groups overseas.\(^{38}\)

**Islamic State of Iraq and Syria (ISIS)**

According to the ODNI Threat Assessment for 2023, ISIS remains a threat both regionally and globally despite suffering significant setbacks from losses to key leadership figures in the past two years due to numerous operations against ISIS core\(^ {39}\) in Syria and Iraq.\(^ {40}\) In response to sustained international pressure on the group and the loss of leadership figures, ISIS has adopted a less hierarchical, looser structure of networked affiliate groups.\(^ {41}\) Though ISIS core strength has been somewhat diluted, certain branches operate with near autonomy and are highly operationally capable.\(^ {42}\) The IC deems the largest ISIS threat to the United States emanates from these ISIS branches, such as ISIS-Khorasan (ISIS-K), that have the ambition and capabilities to conduct attacks beyond the Central Asia region.\(^ {43}\)

Though ISIS maintained a strong presence in the Middle East and Afghanistan throughout 2022 and 2023, ISIS-affiliated groups in various countries within Africa play an increasingly prominent role in the group as a whole, both financially and operationally. ISIS branches continue to operate extensively throughout the African continent while exploiting regional instability, weak governance, and local conflicts and grievances. The State Department assessed that ISIS waged a “large-scale terrorism campaign,” particularly in Cameroon, Chad, Niger, and Nigeria, where the porous borders near the Lake Chad region provide easy transit routes for local ISIS affiliates, as well as in Afghanistan.\(^ {44}\) The strongest and most capable ISIS affiliates in Africa are ISIS-West Africa, ISIS-Democratic Republic of Congo (ISIS-DRC), and ISIS-Somalia. Additionally, ISIS-K in Afghanistan remains an important and powerful affiliate due to its role as a regional hub, transferring hundreds of thousands of dollars to financial facilitators as well as providing personnel and weapons to support external operations.\(^ {45}\)

Sustained international pressure has resulted in diminished revenue and a loss of several key financial facilitators, such as Bilal al-Sudani, and has created financial challenges for the group, putting more pressure to raise funds.\(^ {46}\) ISIS core still has access to dwindling cash reserves in Iraq and Syria, estimated to be around $25 million in late 2022, down from $500 million at the height of the ISIS caliphate.\(^ {47}\) Reports indicate that ISIS core’s revenue may be declining, resulting in occasional skipped

---


\(^{39}\) “ISIS core” refers to ISIS’s original domain and sphere of influence in Syria and Iraq.

\(^{40}\) ODNI 2023 Annual Threat Assessment, p. 32.


\(^{42}\) Id.


\(^{44}\) Department of State, Country Reports on Terrorism 2021, p. 4, [Country_Reports_2021_Complete_MASTER_no_maps-011323-Accessible.pdf](http://state.gov).

\(^{45}\) Department of Treasury, “Fact Sheet: Countering ISIS Financing”, (Jun. 16, 2023), (CIFG Fact Sheet 2023), [2023.06.16-Fact-Sheet-on-Countering-ISIS-Financing.pdf](http://treasury.gov).


\(^{47}\) Department of Treasury, “Fact Sheet: Countering ISIS Financing”, (Nov. 18, 2022), (CIFG Fact Sheet 2022) 2023.06.16-Fact-Sheet-on-Countering-ISIS-Financing.pdf (treasury.gov).
payments for ISIS fighters and their families due to financing constraints.\footnote{CIFG Fact Sheet 2023.}

Aside from cash reserves, ISIS generates significant income through various illicit and criminal activities. Kidnapping for ransom and extortion provides significant amounts of money to the group, especially for key ISIS branches, such as ISIS-K and ISIS-Somalia. ISIS-Somalia has also become one of the most important branches for ISIS financially, as it generates significant revenue for the group through extortion of local businesses and financial institutions, some of which is then transferred and distributed to other ISIS branches and networks.\footnote{Department of Treasury, OFAC, “Treasury Designates Senior ISIS-Somalia Financier”, (Jul. 27, 2023), \url{https://home.treasury.gov/news/press-releases/jy1652}.} ISIS-Somalia, overseen by Al-Karrar office, has served as a financial and communication hub for the global ISIS enterprise, facilitating funds transfers to other branches and networks through mobile money platforms, cash transfers, hawala, and money laundering through businesses.\footnote{Id., UN Analytical Support and Sanctions Monitoring Team, Sixteenth Report of the Secretary-General on the Threat Posed by ISIL (Da’esh) to International Peace and Security and the Range of United Nations Efforts in Support of Member States in Countering the Threat, (Feb. 1, 2023) (16th Report of UN SG on ISIL), \url{https://undocs.org/S/2023/76}.}

Lastly, contributions from individual supporters also supplement the group’s cash flows. ISIS has sought to aggressively fundraise online using social media, encrypted mobile applications, online gaming platforms, and virtual asset service providers (VASPs) for fund transfers.\footnote{UN Analytical Support and Sanctions Monitoring Team, 31st Report of the Analytical Support and Sanctions Monitoring Team, p.18, (Feb. 13, 2023) (31st UN MT Report), \url{N2303891.pdf} (securitycouncilreport.org).} ISIS facilitators have adapted to new technologies like virtual assets. For example, certain branches, such as ISIS-K, have increased their understanding of virtual assets. ISIS also seeks to raise money to free pro-ISIS sympathizers and potential ISIS recruits, including children, from camps and prisons throughout Syria.\footnote{Department of Treasury, OFAC, “Treasury Designates Facilitation Network Supporting ISIS Members in Syria”, (May 9, 2022), \url{https://home.treasury.gov/news/press-releases/jy0772}.} Some fundraising networks generated funds for this specific purpose in Indonesia, Türkiye, the United States, and elsewhere, which were then transferred via hawala networks to al-Hawl, an ISIS displacement camp in Syria.\footnote{Id.}

ISIS continues to extensively utilize traditional methods to move and transfer funds, such as hawala and cash, but the group has also adopted widespread use of mobile money service providers, particularly in Eastern and Central Africa.\footnote{UN MT 31st Report, p. 18.} ISIS also utilizes regional financial hubs, such as Türkiye, as conduits for moving and raising money on behalf of the group. Notably, in 2023, ISIS-K used Türkiye as a transit hub for disbursing funds and transferring operatives and weapons from Afghanistan to Europe for possible attacks.\footnote{CIFG Fact Sheet 2023.} In 2023, the United States and Türkiye jointly designated several members of an ISIS financial facilitation network, indicating ISIS’s reliance on hawala businesses in Türkiye and Iraq for financial transactions. This network managed several hawala offices and oversaw the transfer of funds from Persian Gulf-based donors to ISIS.\footnote{Department of Treasury, OFAC, “The United States and Türkiye Take Joint Action to Disrupt ISIS Financing”, (Jan. 5, 2023), \url{https://home.treasury.gov/news/press-releases/jy1181}.} In late 2021, the United States designated Ismatullah Khalozai, who was operating “a Türkiye-based hawala business to transfer funds to finance ISIS-K
operations.” Before that, Khalozai was involved in another financing scheme out of the United Arab Emirates (UAE) and was engaged in human smuggling operations in Afghanistan, both of which benefitted ISIS-K.

ISIS-related activity in the United States is largely relegated to lone, self-radicalized individuals seeking to conduct ISIS-inspired attacks, travel abroad to join ISIS, or offer financial support to the group. Financial activity linked to ISIS in the United States typically involves supporters collecting or sending small amounts of money abroad or financing their own or others’ travel to ISIS conflict zones. This money generally comes from legal means, often personal savings, and sometimes may be collected on behalf of others. Individuals may coordinate the donations through encrypted mobile applications like Telegram, send the funds in the form of virtual assets, wire them abroad through a fiat money service business (MSB), or, if collected in cash, pass them to couriers. Some U.S. persons have also engaged in more extensive financial and fundraising activity on behalf of ISIS.

- In May 2023, U.S. authorities arrested an American citizen and charged him with attempting to provide material support to a designated foreign terrorist organization, in the form of collecting, transmitting, receiving, and distributing money to ISIS members.
- In November 2022, a Connecticut man pleaded guilty to attempting to provide material support to ISIS. According to court records, beginning in approximately September 2018, Ahmad Khalil Elshazly, a U.S. citizen, expressed a desire to travel to Syria and the surrounding area to fight on behalf of ISIS. In December 2019, Elshazly paid $500 to a person he believed was an ISIS facilitator who would be able to smuggle him out of the U.S. to Turkey.
- In October 2023, an American citizen was indicted for knowingly concealing the source of material support or resources that he intended to go to ISIS. According to the charging documents, the defendant provided multiple gift cards to an individual he believed was an ISIS supporter with the intention that the gift cards be sold on the dark web for a little less than face value and resulting profits be used to support ISIS. The defendant allegedly stated that he wanted the proceeds to go to ISIS “for war on kuffar,” (disbelievers). In total, it is alleged that between January and May 2023, he donated $705 intended to support ISIS.

**Al-Qaeda (AQ)**

Like ISIS, AQ has continued to suffer losses in senior leadership over the past two years, which has further advanced the decentralization of the group. However, AQ’s presence across the African continent through local affiliates like al-Shabaab and al-Qa’ida in the Islamic Maghreb (AQIM) still represents a potent threat to regional and global security. These affiliates continue to exploit security gaps and weak state institutions, especially in Somalia, to consolidate power and retain control. IC assessments note that AQ maintains its ideological commitment to attacking Western interests and targets, and this threat is heightened in regions where AQ maintains territorial control, such as in Somalia, the Sahel, and parts

59 Id.
AQ and affiliate groups continue to utilize many of their long-standing methods of illicit revenue generation. According to the UN, al-Shabaab is still in a very strong financial position, having several reliable sources of income, with an estimated annual revenue of around $100 million.\(^\text{63}\) The group engages in systemic extortion of businesses and individuals in Somalia, leveraging its territorial control to maintain a consistent stream of revenue.\(^\text{64}\) Tactics include setting up checkpoints to extort vehicles and transportation of goods along supply routes as well as illegally taxing residential properties and developers of new properties in Mogadishu.\(^\text{65}\) Al-Shabaab predominantly collects this money in cash but also uses mobile money services, money remitters, and banks to transfer funds.\(^\text{66}\) Recent public actions against al-Shabaab financiers have highlighted al-Shabaab’s reliance on weak government institutions and regional and international networks of financial facilitators to support the group’s activities.

In October 2022, Treasury designated a network of al-Shabaab financial facilitators in Somalia who materially assisted the group and provided an array of services, from weapons procurement to recruitment.\(^\text{67}\) This network played a key role in a smuggling and weapons trafficking network in Yemen that was utilized by al-Shabaab as well as other criminal enterprises.\(^\text{68}\) One designated individual, Ahmed Hasan Ali Sulaiman Mataan, was a Somali businessman who operated a fleet of ships used to traffic weapons and improvised explosive device components from Yemen on behalf of al-Shabaab. Other members of the network acted as intermediaries for Al-Shabaab, operating between the group and businesses and NPOs in Somalia through facilitating funds transfers, collecting money, and fundraising for Al-Shabaab.\(^\text{69}\) Another individual, Hassan Afgooye, is a key leader within al-Shabaab and has helped with numerous illicit financial activities on behalf of the group, including operating sham charities, fundraising, racketeering, and kidnapping.

A subsequent Treasury action in May 2023 highlighted another financial network of al-Shabaab facilitators, including an extensive charcoal smuggling network that provided income to the group.\(^\text{70}\) Members of the illegal charcoal smuggling operation acted in contravention of a 2012 UN Security Council Resolution banning the import of Somali charcoal due to its role in funding various criminal
and terrorist groups and contributing to conflict and instability within Somalia. The charcoal smuggling network helped coordinate the sale and shipment of charcoal from Somalia to Persian Gulf countries, such as Oman and the UAE. The main interlocutor, Ali Ahmed Naaji, operated a legitimate Somalia-based international business that also funded al-Shabaab. Other members of the network assisted with fraudulent paperwork, disguising the charcoal cargo for shipment, and utilizing their own registered businesses to broker the deals.

Financial activity linked to AQ in the United States generally consists of U.S. citizens providing or attempting to provide financial support to AQ or AQ-linked groups using personal funds transferred abroad, sometimes utilizing registered MSBs.

• In July 2022, a U.S. citizen, Georgianna A.M. Giampietro, was sentenced to 66 months in prison for concealing material support and resources intended to be provided to the U.S.- and UN-designated Hayat Tahrir al-Sham (HTS), an AQ-linked terrorist group in Syria.\footnote{Department of Justice, “Sparta Woman Sentenced to 5 ½ Years in Prison for Concealing Material Support Intended for a Foreign Terrorist Organization”, (Jul. 20, 2022), \url{https://www.justice.gov/usao-mdtn/pr/sparta-woman-sentenced-5-12-years-prison-concealing-material-support-intended-foreign}.} According to court documents, in September 2018, Giampietro had conversations with an undercover agent who expressed interest in traveling to Syria to join HTS. The undercover agent told Giampietro that her husband swore an oath of allegiance to HTS and that he intended to fight on behalf of HTS. Giampietro initially provided instruction and advice to the undercover agent on how to travel to Syria in order to avoid detection by law enforcement. In subsequent conversations with the undercover agent, Giampietro offered to communicate with her contacts on their behalf to assist them in safely traveling to Syria to join HTS and later provided the undercover agent with her contact’s information to assist her and her husband in their travel to Syria. In addition, Giampietro intended that the undercover agent and her husband would provide funds to that person, who would in turn provide funds to HTS, thereby providing material support to HTS disguised as a charitable contribution. Giampietro sent money to a charitable organization that purported to help widows and orphans in Syria but actually supported militant jihad in Syria and aided HTS.\footnote{USA v. Giampietro, Case 2:19-cr-00013 (Sentencing Memorandum Opinion and Order), (D. MD Tenn. Jul. 11, 2022) p. 11-12.} 

• In January 2023, a U.S. citizen, Maria Bell, was sentenced to 34 months in prison for concealing attempts to provide material support to al-Nusrah Front (ANF) and HTS.\footnote{Department of Justice, “Sussex County Woman Sentenced to 34 Months in Prison for Concealing Terrorist Financing to Syrian Foreign Terrorist Organizations”, (Jan. 24, 2023), \url{https://www.justice.gov/usao-nj/pr/sussex-county-woman-sentenced-34-months-prison-concealing-terrorist-financing-syrian}.} According to documents filed in court, beginning at least as early as March of 2017, Bell used mobile applications to communicate with and provide advice to fighters based in Syria who were members of various factions fighting the Assad regime. The charges against Bell centered on her communication with, and provision of money to, one specific fighter based in Syria, who was a self-identified member of HTS. Notably, Bell sent cryptocurrency to this fighter via an MSB using an intermediary to conceal the source of the funds, and also provided him with advice on weapons and ammunition.
Hizballah

Hizballah has maintained its ideological commitment to diminishing the U.S. presence in the Middle East. Through its sophisticated global financing network and advanced conventional military capabilities, it maintains the capability to threaten U.S. interests at home and abroad. Hizballah leverages a worldwide network of illicit businesses, criminal enterprises, and financial facilitators to maintain a robust global presence and raise and launder large amounts of money.

Hizballah is funded in large part by the Iranian government, which provides several hundred million dollars a year in direct funding. Hizballah also engages in a range of illicit and commercial activities to supplement its income. These illicit activities range from oil smuggling and shipping and charcoal smuggling to drug and weapons trafficking. For instance, Hizballah has been implicated in several complex illicit oil smuggling schemes which were orchestrated by, and jointly benefitted, both Hizballah and Iran’s Islamic Revolutionary Guard Corps (IRGC) Qods Force. In one scheme, numerous companies and ships smuggled Iranian oil by blending it with Indian petroleum-products and creating counterfeit certificates of origin. The oil was then loaded onto ships owned by a front company and flagged in Liberia and Djibouti, seen as more permissive jurisdictions, to avoid scrutiny. This example demonstrates Hizballah’s ability to use a complex web of front companies to obfuscate both the ownership of the vessels and the true source of the oil.

Hizballah also regularly exploits the international financial system and excels in utilizing networks of seemingly legitimate front companies to raise, launder, and move money on behalf of the group. These front companies are used to obscure the true beneficial ownership. They are used extensively in various commercial activities benefiting Hizballah, such as real estate, import/export, construction, and luxury goods. These commercial activities generate significant income for the group and draw less scrutiny than outright illicit enterprises.

Hizballah relies on jurisdictions with weak government institutions, porous borders, or corrupt state officials to facilitate their illicit activities. Historically, such areas have included parts of South America, particularly the tri-border area of Brazil, Paraguay, and Argentina, as well as some parts of West Africa and the Middle East, where key financial facilitators assist in transferring and moving funds on behalf of the group. In one example, two Hizballah supporters and prominent businesspeople in Guinea assisted in moving funds from Guinea to Hizballah, and utilized political connections, bribes, and access to corrupt officials to send cash in U.S. dollars in suitcases out of Conakry airport. Hizballah also draws on individual financial contributions from sympathetic members of the Lebanese diaspora located around the world in many of the jurisdictions mentioned above.

---

74 ODNI 2023 Annual Threat Assessment pp. 31-33.
80 Id.
As noted in prior NTFRAs, Hizballah still maintains a footprint within the United States. Hizballah members and sympathizers have long been involved in an array of large-scale criminal schemes, including sophisticated money laundering, smuggling, and trafficking networks that have involved the U.S. financial system. In the past, Hizballah and its supporters have regularly transferred funds through the U.S. financial system. However, some case examples have highlighted Hizballah activity within the United States that is focused more on information-gathering or, in very isolated cases, potential preparation for attacks rather than generating revenue. As noted below, there are also instances of Hizballah operatives attempting to purchase military or export-controlled equipment, including through the use of front companies.

- In April 2023, Treasury and Justice disrupted a large international money laundering and sanctions evasion network involving over 52 people and entities located across the globe. These individuals and entities were involved in an array of activities including the transfer, shipment, and delivery of cash, precious gems, art, and luxury goods on behalf of Hizballah. This network stretched across Africa, Western Europe, the Middle East, and Asia and utilized hubs in the UAE, South Africa, Lebanon, and Hong Kong. According to court documents, Nazem Said Ahmad, who was sanctioned by the United States in 2019 for being a financier for Hizballah, and his co-conspirators, including family members and business associates, relied on a complex web of business entities to obtain valuable artwork from U.S. artists and art galleries and to secure U.S.-based diamond-grading services all while hiding Ahmad’s involvement in and benefit from these activities. Over one hundred million dollars in transactions involving artwork and diamond-grading services flowed through the U.S. financial system.

- In May 2023, Alexei Saab was sentenced to 12 years in prison for receiving military-type training from a designated foreign terrorist organization (Hizballah), marriage fraud, conspiracy, and making false statements. According to court documents, Saab joined Hizballah in 1996 and transitioned to Hizballah’s external operations unit, the Islamic Jihad Organization (IJO), where he received extensive training in IJO tradecraft, weapons, and military tactics. In 2000, Saab entered the United States and remained an IJO operative, continuing to receive military training in Lebanon and conducting numerous operations for the IJO. This included intelligence collection against potential attack targets, as well as opening a front company that he could use to obtain fertilizer in the United States for use as an explosives precursor. Finally, in or about 2012, Saab entered into a fraudulent marriage in exchange for $20,000. The purpose of the marriage was for Saab’s purported wife to apply for her citizenship.

- A review of financial institution reporting from 2021-2022 highlighted that individuals linked to known and previously designated Hizballah financiers routinely used the U.S. financial system to transfer funds through a range of financial institutions located in the United States and abroad.

---

81 See 2022 NTFRA pp. 11-12.
85 Treasury analysis of financial institution reporting.
Hamas

Harakat al-Muqawama al-Islamiya (Islamic Resistance Movement), better known by the acronym Hamas, is a U.S.-designated terrorist group primarily based in the Gaza Strip and the West Bank since its formation as an offshoot of the Muslim Brotherhood in the late 1980s. Hamas is committed to waging violent jihad against Israel and liberating Palestine through violent resistance. Hamas has been designated as a terrorist group by the United States since 1997. Since 2005, Hamas has been the governing authority in the Gaza Strip and has maintained a presence in the West Bank, intermittently provoking regional instability in the 1990s and throughout the 2000s by committing terrorist attacks and violence directed at Israel. The October 7, 2023, terrorist attacks, which Hamas perpetrated on Israel and the citizens of at least 36 other nations, underscored Hamas’s commitment to its extremist goals and brought renewed global attention to the financing and operations of the group.

Hamas has advanced military capabilities at its disposal, partly as a result of decades of accumulating weapons through Iranian government support, as well as forming extensive and complex global financing networks. Hamas is unique among other terrorist groups because its cause is viewed sympathetically by some governments and the general public in some countries with Muslim-majority populations. Notably, Hamas is not designated as a terrorist organization in most of the Middle East, and this permissive regional environment has allowed Hamas facilitators or operatives to freely raise and transfer funds.

Hamas is a well-resourced group that garners substantial financial resources from numerous and diverse sources. Due to its territorial control of the Gaza Strip, Hamas historically has been able to exploit its position as a governing entity to generate considerable revenue, in part by extorting the local population. The group’s primary external funding comes from Iran, which has provided it roughly $100 million per year. Hamas also generates of revenue from an expansive and sophisticated international investment portfolio, previously estimated to be worth at least $500 million. This investment portfolio has invested in companies and assets located across the world, including in Algeria, Saudi Arabia, Sudan, Türkiye, and the UAE, and is managed by Hamas’ Investment Office. In addition, Hamas relies on a global fundraising network to raise funds for its nefarious activities. Hamas is prolific in soliciting donations from witting and unwitting donors worldwide in both fiat and virtual assets.

Hamas facilitators have used numerous methods to collect and transfer funds into the Gaza Strip. These include crowdfunding websites and sham charities, where in some cases, the destination of the funds was concealed under the guise of humanitarian efforts. In other cases, they solicited funds directly for their cause from sympathetic donors. Hamas has also used complicit VASPs and money transmitters throughout the globe to move funds. In the aftermath of the October 7, 2023, terrorist

---

86 The European Union, members of the G7, as well as some other countries have fully designated the entirety of Hamas as a terrorist organization.

87 Following Hamas’ terrorist attack, Treasury issued an alert to U.S. financial institutions highlighting Hama’s main sources of funding and identifying red flag indicators relating to Hamas’ terrorist financing activity. These indicators include transactions that originate with or involve entities that have a nexus to Iran-supported terrorist groups such as Hizballah or Palestinian Islamic Jihad (PIJ); charitable organizations soliciting donations without appearing to provide any charitable services, and transactions involving MSBs or financial institutions in higher-risk jurisdictions that are tied to Hamas activity and that are reasonably believed to have lax Customer Due Diligence (CDD) or AML/CFT practices, see FinCEN Alert, FIN-2023-Alert006, October 20, 2023.


89 Id.
attacks, Treasury designated a Gaza-based VASP called Buy Cash Money and Money Transfer Company for serving as a key node in Hamas’s virtual asset fundraising schemes. The same entity has also been identified as being involved with funds transfers on behalf of other terrorist groups.

Hamas’s global financial footprint and use of the regulated international financial system means that its facilitators likely have access to the U.S. financial system, particularly as Hamas has sought to raise funds from international supporters. U.S. persons have been convicted of providing or conspiring to provide material support to Hamas from the United States in recent years. After the October 2023 terrorist attacks, Hamas supporters around the world mobilized global fundraising efforts on behalf of the group. These online fundraisers took various forms, often seeking to collect money on crowdfunding sites under the guise of charitable donations for Gaza.

**VULNERABILITIES**

**Registered Money Services Businesses (MSBs)**

As noted in past NTFRAs, registered MSBs, including money transmitters, play an integral role in the non-bank financial institution ecosystem, providing necessary financial services to unbanked and underbanked populations and facilitating billions of dollars in funds transfers for legitimate purposes around the world. However, MSBs have been, and continue to be, vulnerable to terrorist financing for several reasons. Their global reach, their role as the sole financial services provider in some jurisdictions, along with weaknesses in the implementation and supervision for AML/CFT requirements in some foreign jurisdictions, and their less stringent requirements than other financial institutions such as banks make them an attractive option for terrorist financing.

Numerous terrorist groups have been identified as using money transmitters to move funds. Hizballah has routinely used money remitters to move funds around the world. For example, in January 2023, Treasury identified a Lebanese MSB called CTEX that was owned by Lebanon-based economist Hassan Moukalled, who provided financial advisory services to Hizballah. CTEX was established as a front company in 2021 and by 2022 was transmitting millions of dollars in U.S. currency, including “providing U.S. dollars to Hizballah institutions.” Additionally, a review of financial institution reporting identified individuals connected to Hizballah who used MSBs to transfer funds globally.

In the United States, MSBs are subject to AML/CFT regulations imposing AML program, reporting, and recordkeeping obligations. A range of activities qualify a business as being an MSB, such as currency
exchange; check cashing; money transmission, including through VASPs; providing or selling prepaid access; and any business issuing or cashing travelers checks or money orders.\(^{96}\) MSBs have a lower SAR filing threshold ($2,000) than other regulated financial institutions ($5,000).\(^{97}\) MSBs are required to file suspicious activity reports (SARs), and an analysis of SAR reporting shows that between 2020 and 2022, MSBs filed nearly 72% of all SARs related to TF.\(^{98}\)

Large MSBs have a significant global footprint that can go beyond the reach of most traditional banking institutions. Such entities generally have advanced internal controls and compliance programs in accordance with the risk of the jurisdictions in which they do business, which tend to be higher risk than where banks operate. However, smaller MSBs, such as those that may only undertake small-scale transactions or perform only one of the services that may qualify them as an MSB (e.g., a grocery store that also provides services as a dealer in foreign exchange), may face higher TF risks. These small MSBs may have weaker AML/CFT programs and less oversight than established global MSB businesses, or they may devote fewer resources to monitoring suspicious activities than their larger counterparts. There are also several instances where money remitters outside of the United States have been owned by or employed terrorist supporters who have knowingly facilitated financial activity on behalf of these groups.

**Person-to-Person (P2P) Payments**

Depending on the platform, a person-to-person (P2P) payment can be initiated from a consumer's online bank account or prepaid card account through a mobile or desktop application (apps). P2P apps are free to download, and payments are typically free when made using a linked checking account, debit card, or stored balance; some platforms also allow funding via credit card for a fee. P2P services operate as relatively closed environments where users can only send funds to another individual on the same platform. Because of this feature, bank account details can be kept private from other users: all that is typically required from users to send a payment is the recipient’s email address or phone number. When users receive a payment, they usually have the option of maintaining a balance in the app or transferring the funds to their bank accounts. While most P2P services in the United States only operate domestically, some offer cross-border payment options. As money transmitters, P2P payment services are considered MSBs and thus subject to the reporting, recordkeeping, and AML/CFT program requirements under the Bank Secrecy Act (BSA) and must register with FinCEN.

P2P payment platforms have brought accessibility, ease, and inclusion to the regulated financial system for many individuals worldwide. These services have become particularly important for unbanked and underbanked individuals who may reside in extremely rural areas and do not otherwise have access to regulated banking services. These payment methods are not necessarily inherently more risky than traditional banking systems, but the speed and ease with which individuals can perform these transactions can make them an attractive option for criminals or terrorists. Additionally, incorporating P2P payment systems in conjunction with more traditional forms of moving and storing money, such as cash and hawala, can make a money trail significantly more complex.

---

96 See [Money Services Business Definition | FinCEN.gov](https://www.fincen.gov).
98 See [SAR Stats | FinCEN.gov](https://www.fincen.gov).
Unregistered Money Transmission

People may choose to use unregistered money transmitters in areas without access to the regulated financial system. However, unlike registered MSBs, these money transmitters operate without complying with the core AML/CFT program or the recordkeeping and reporting requirements that apply to registered MSBs, increasing the risk of exposure to illicit activity. A variety of bad actors may seek out or operate as unregistered money transmitters to facilitate illicit conduct, as people may perceive these businesses as less transparent – and their transactions thus more difficult to trace. For example, unregistered money remitters remain a vulnerability through which groups such as AQ and ISIS move money internationally, especially because the lack of registration in the United States prevents law enforcement from being apprised of suspicious money transmission activity.

While unregistered money transmitters have offered more traditional financial services (where funds are transferred through an account the unregistered remitter maintains at a financial institution), a growing number of online payment providers or social media companies are, in some cases, acting as unregistered money transmitters. In addition, individuals and entities operating as VASPs in the United States but not registered with FinCEN are acting as unregistered money transmitters. As a recent enforcement case demonstrates (discussed in more detail below), unregistered money transmitters may have significant ties to terrorist financing.99

Cash

Cash, and in particular, U.S. dollars, continues to be a fixture for terrorists raising, moving, and using funds, particularly when transferring funds across borders. While using cash is slower, bulkier, and less efficient than other mechanisms of moving funds, the anonymity, liquidity, and lack of electronic footprint mean that a cash-based money trail is more difficult to track and avoids the scrutiny that comes with transactions executed through a regulated financial institution.

As detailed in the 2022 NTFRA, U.S.-based supporters of ISIS still use cash to fund foreign travel or otherwise support the group. DVE groups or others inspired to conduct attacks in the United States also use cash to purchase weapons or materials to make explosives.

• In June 2022, a U.S. resident, Dilkayot Kasimov, was sentenced to 15 years in prison for conspiring and attempting to provide material support to ISIS in the form of cash.100 According to court documents, in 2015, Kasimov’s co-conspirators planned to travel to Syria to fight on behalf of ISIS. Kasimov provided money – his own and cash collected by others – to help fund a co-conspirator’s travel and expenses. In February 2015, Kasimov traveled to John F. Kennedy International Airport and handed $1,600 in cash on behalf of himself, a co-conspirator, and others to a would-be foreign fighter.

• Two U.S. citizens were sentenced in February 2023 for attempting to provide material support to ISIS.101 According to court documents, the couple were ISIS supporters who sought to travel to the Middle East to join and fight for ISIS. One of the defendants provided $1,000 in cash as travel costs to an undercover law enforcement officer.102

102 Id.
Banks

Banks are key participants in the global financial system. U.S. banks specifically facilitate the majority of transactions that are processed on a day-to-day basis through the global financial system. Among the services that banks provide are correspondent banking services that enable foreign respondent banks to conduct business and provide services to customers in foreign markets through correspondent banks that hold accounts at U.S. financial institutions. The ability to make and receive international payments through correspondent banking relationships is vital for facilitating trade and commerce, thus promoting sustained economic growth worldwide. Most large U.S. and European banks have appropriate AML/CFT programs that comply with the BSA and other AML/CFT regulatory requirements, and also maintain sophisticated risk mitigation and monitoring practices. The sheer volume of transactions flowing through the global banking system makes it particularly challenging for banks to identify terrorist-related transactions, meaning the inherent risk of U.S. and global banks’ exposure to illicit activity is high.

Because of the structure of the activity and the limited information regarding the nature or the purpose of underlying transactions, correspondent banks face increased exposure to TF risks. Moreover, respondent banks may be located in higher-risk jurisdictions where the AML/CFT regime is weaker, and the correspondent bank cannot confidently rely on the due diligence and compliance measures of the respondent bank. For example, geographic shifts of terrorism financing centers over the past several years away from the Middle East and towards Africa have put more pressure on the financial institutions that operate in and with jurisdictions with weak governance and AML/CFT regimes, making correspondent banking vulnerabilities more acute.

In some countries, terrorists have seized control of existing regime structures, restricting access by state institutions to the international financial system. These restrictions have prevented illicit actors from transacting funds through the global banking system. Terrorist control of state regime structures may have long-term implications for achieving important public interest objectives such as addressing poverty and promoting overall financial inclusion, facilitating the delivery of humanitarian aid, and promoting sustained economic growth and development.

NPOs, charities, MSBs, and other non-bank entities play key roles in implementing these policy objectives—the success of which relies on sustained access to financial services. Bank decisions to establish and maintain such relationships are generally based on evaluations of ML/TF and other illicit finance risks associated with these customers, and the jurisdictions where they operate, along with profitability. Where the ML/TF risks are outside its risk tolerance, or the institution does not have the risk mitigation resources to effectively address the TF or other illicit finance risks, including experience with the customers’ business activities and monitoring transactions to detect suspicious activity, financial institutions may disengage with certain banking relationships (i.e., de-risking). If NPOs or MSBs lose access to the formal financial system, these entities may resort to using alternative mechanisms outside the regulated financial system, and this loss of transparency affects governments’ ability to monitor transactions and can increase their exposure to TF activity.

Additionally, groups like Hamas or Hizballah that are not consistently designated as terrorist

104 Treasury De-risking Strategy, p. 36.
organizations globally are able to exploit gaps in sanctions designations to raise and move funds using the international financial system. Though the United States has domestically designated these groups, they have not been designated by the United Nations Security Council and therefore UN member states are not obligated to domestically impose these sanctions. These global sanctions designation gaps allow individuals associated with these terrorist groups to open bank accounts and transact freely in some regions, thereby increasing the potential terrorist financing exposure of U.S. correspondent banks.

**Virtual Assets**

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. Virtual assets, as used in this report, include non-sovereign-administered digital assets (such as convertible virtual currencies (CVCs), like bitcoin and stablecoins) but do not cover central bank digital currencies (CBDCs), which are representations of fiat currency and treated the same as fiat currency by the FATF or representations of other financial assets, such as digitized representations of existing securities or deposits. For the purpose of consistency, this terminology is also used in case examples, but this is intended only to facilitate an understanding of illicit finance risk and does not alter any existing legal obligations.

In the United States, VASPs have AML/CFT obligations if they fall under the BSA’s definition of a financial institution, which covers banks, broker-dealers, mutual funds, MSBs, futures commission merchants (FCMs), and introducing brokers, among others. Many VASPs in the United States are considered MSBs, and some may be mobile payment platforms. VASPs that operate wholly or in substantial part in the United States are considered MSBs, unless an applicable exemption applies, and must comply with applicable BSA requirements. Depending on the VASP’s activities, they may also be considered FCMs or broker dealers. Each of these financial institutions has AML/CFT

---


106 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.

107 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 into consideration data privacy and other concerns.

108 31 U.S.C. § 5312(a)(2); 31 C.F.R. § 1010.100(t).
obligations, including requirements to establish and implement an AML program and recordkeeping and reporting requirements, including SAR requirements. Additionally, all VASPs subject to U.S. jurisdictions have sanctions compliance obligations.

The U.S. government assesses that both international terrorist and DVE groups have continued using virtual assets to generate and transfer funds. Since the 2022 NTFRA, certain terrorist groups, such as ISIS-K and Hamas, have increased their understanding of and are experimenting with different types of virtual assets. However, the U.S. government assesses that terrorists still prefer traditional financial products and services. This preference is likely in part due to the price volatility of many virtual assets, the limited ability to purchase goods and services with virtual assets, and a lack of infrastructure necessary to exchange virtual assets for fiat currency in some jurisdictions where terrorist groups operate.

In contrast to the 2022 NTFRA, which identified that terrorist groups most frequently solicited virtual asset donations of bitcoin, terrorist groups soliciting donations of virtual assets are increasingly turning to stablecoins, which are virtual assets that are designed to maintain a stable value relative to a national currency or other reference assets. Stablecoins purport to be less volatile than other virtual assets and may enable terrorist groups to utilize virtual assets while mitigating the financial risks associated with price fluctuations. Additionally, stablecoins may be preferred by VASPs used by terrorists to exchange virtual assets for fiat currency. Reporting and private sector analysis indicate that ISIS and other terrorist groups have moved towards using stablecoins, including Tether, to move or store funds.

Consistent with the 2022 NTFRA, most cases of terrorists using virtual assets involve groups fundraising online and specifically soliciting virtual assets from donors. Such fundraising campaigns are often disseminated through social media or encrypted apps like Telegram and often solicit funds in virtual assets and fiat currency, enabling the donor to decide which method to use. Individual donors can send virtual assets from a VASP or an unhosted virtual asset wallet to a virtual asset address owned by the terrorist group. Groups may use the funds for a range of purposes, including the procurement of weapons, propaganda creation or dissemination, logistics, or planning a specific act of violence, although purchasing goods and services often requires exchanging virtual assets for fiat currency.

---

109 See 31 C.F.R. § 1020.210 (banks); 31 C.F.R. § 1021.210 (casinos and card clubs); 31 C.F.R. § 1022.210 (MSBs); 31 C.F.R. § 1023.210 (brokers or dealers in securities); 31 C.F.R. § 1024.210 (mutual funds); 31 C.F.R. § 1026.210 (futures commission merchants and introducing brokers in commodities). An AML Program must include, at a minimum, (a) policies, procedures, and internal controls reasonably designed to achieve compliance with the provisions of the BSA and its implementing regulations; (b) independent testing for compliance; (c) designation of an individual or individuals responsible for implementing and monitoring the operations and internal controls; and (d) ongoing training for appropriate persons. Rules for some financial institutions refer to additional elements of an AML Program, such as appropriate risk-based procedures for conducting ongoing customer due diligence.

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

111 See e.g., https://www.chainalysis.com/blog/israel-nbctf-hezbollah-iran-quds-crypto-seizure, How Hamas has utilized crypto, and what may be coming (elliptic.co), Israel Seizes Crypto Wallets Worth $94 Million Linked to Palestinian Islamic Jihad (elliptic.co).

112 Unhosted wallets enable users to retain custody of their virtual assets and transfer them without the involvement of a financial institution.

113 FATF Crowdfunding for TF Report, pp. 29-30.
Terrorist groups may also use virtual assets to transfer funds to other members or related groups using VASPs or peer-to-peer virtual asset transfers, referring to payments between two unhosted wallets that do not involve a regulated financial institution.\textsuperscript{115} In some instances, transfers may take several steps and involve peer-to-peer virtual asset transfers as well as VASPs, including over-the-counter brokers, peer-to-peer virtual asset platforms,\textsuperscript{116} or purportedly decentralized exchanges,\textsuperscript{117} possibly for the purpose of obfuscation. While some of the VASPs used by terrorist groups may be local to their operations, in particular for exchanging virtual assets for fiat currency, they can also leverage VASPs based all over the world to send and receive virtual assets.\textsuperscript{118} Regardless of whether terrorist groups received funds from donations or transfers from other groups, they will likely require VASPs to exchange virtual assets for fiat currency, which is often necessary to purchase goods and services.

- In December 2022, DOJ unsealed a criminal complaint charging four defendants with conspiring to provide material support to ISIS. The defendants raised and contributed more than $35,000 through cryptocurrency and other electronic means to bitcoin wallets and accounts they believed to be funding ISIS.

When VASPs operating in the United States or abroad lack or fail to implement AML/CFT requirements, they are vulnerable to misuse for TF. Despite the FATF extending global standards for AML/CFT to VASPs in 2019, many countries have been slow to regulate VASPs. Many VASPs operating abroad have substantially deficient AML/CFT programs, particularly in jurisdictions where international standards for VASPs are not effectively implemented. Based on FATF assessments, jurisdictions are making limited progress (73 out of 98 jurisdictions rated as only partially or not compliant), and a FATF-administered survey found that many jurisdictions had not taken basic steps to assess risk or determine an approach to virtual assets.\textsuperscript{119} Uneven and often inadequate regulation and supervision around the world allow VASPs to engage in regulatory arbitrage and expose the U.S. financial system to risk from jurisdictions where regulatory standards and enforcement are less robust.

The FATF has developed a roadmap to encourage countries to implement the FATF standards for virtual assets and VASPs, which includes the planned publication of a table noting progress on implementation for FATF members and jurisdictions assessed to have materially important VASP activities.\textsuperscript{120} Although VASPs in the United States have AML/CFT and sanctions obligations, as explained above, there are cases in which VASPs fail to comply with these obligations, raising the risks of exposure to TF and other illicit activity. In some cases, VASPs may not implement AML/CFT controls or other processes to identify customers, enabling misuse by illicit actors, including terrorists. Additionally, VASPs may perceive that they are not subject to U.S. regulatory requirements for AML/CFT

\textsuperscript{115} For example, ISIS, see CIFG Fact Sheet 2023.

\textsuperscript{116} P2P service providers, typically natural persons engaged in the business of buying and selling virtual assets rather than safekeeping virtual assets or engaging in P2P transfers on their own behalf, may have regulatory requirements depending on their precise business model.

\textsuperscript{117} The use of the term “exchange” in this assessment does not indicate registration as such or any legal status of any such platform. This definition is for the purpose of the risk assessment and should not be interpreted as a regulatory definition under the BSA or other relevant regulatory regimes.


based on their geographic location or the services that they provide.

In November 2023, Binance settled with FinCEN and OFAC for violations of AML and sanctions laws, each assessing the largest civil monetary penalty in their history. Binance did business as a money transmitter in substantial part within the United States, including by cultivating and serving over 1 million U.S. customers through its main platform, but at no time did Binance register with FinCEN. Additionally, Binance failed to file SARs with FinCEN on significant sums being transmitted to and from entities officially designated as terrorist organizations by the United States and United Nations, as well as high-risk exchanges associated with terrorist financing activity. Binance user addresses were found to interact with bitcoin wallets associated with ISIS, Hamas’ Al-Qassam Brigades, Al Qaeda, and the Palestinian Islamic Jihad (PIJ). Although no SARs were filed with FinCEN, Binance has proactively cooperated with global law enforcement and blockchain vendors to combat terrorism financing. While Binance demonstrated its own broad awareness of U.S. sanctions prohibitions, including related to terrorist groups, Binance senior management expressed interest in feigning compliance rather than addressing the company’s actual risk. Separately, DOJ charged and secured a guilty plea from both Binance and its founder and chief Executive Officer, Changpeng Zhao, who is currently awaiting sentencing. These settlements were part of a global agreement simultaneous with Binance’s resolution of related matters with CTFC and an announcement of DOJ’s charges. Terrorist groups could use anonymity-enhancing technologies such as anonymity-enhanced virtual assets and techniques, like virtual asset mixing, to obfuscate the source, destination, or movement of virtual assets. This technological capability can complicate investigators’ ability to trace illicit funds. Based on Treasury’s assessments, the use of anonymity-enhancing technologies and techniques for financial transactions by terrorist groups has been limited so far, and Treasury will continue to monitor the use of these services. For example, to increase transparency in the virtual asset ecosystem, FinCEN issued a notice of proposed rulemaking (NPRM) pursuant to section 311 of the USA PATRIOT Act in October 2023 that identifies international convertible virtual currency mixing (CVC mixing) as a class of transactions of primary money laundering concern. FinCEN’s proposal would require covered financial institutions to implement certain recordkeeping and reporting requirements on transactions that covered financial institutions know, suspect, or have reason to suspect involve CVC mixing within, or involving jurisdictions outside, the United States.

In contrast, certain elements of virtual assets may support tracing funds associated with terrorist financing. Virtual asset transactions often occur on public blockchains, which means that anyone with internet access can view the pseudonymous transaction data in a public ledger for the blockchain. Public ledgers can support investigations in tracing the movement of illicit funds. However, there are some limitations due to the pseudonymous nature of the data, challenges associated with the use

---


of anonymity-enhancing technologies and techniques, and activity occurring off-chain. Still, recent seizures by Israeli authorities of virtual assets associated with terrorist groups illustrate how public blockchain data can support investigations of terrorist financing in virtual assets and emphasize the critical role that VASPs play in acting on law enforcement information to disrupt terrorist financing.

For example, in June 2023, Israeli authorities, with the help of a private sector blockchain analytics firm, seized approximately $1.7 million worth of virtual assets from a VASP allegedly used by Hizballah and Iran’s Qods Force to finance their operations, marking the first time such a seizure has been made against Hizballah. Moreover, these disruptions can impact terrorist groups’ interest in using virtual assets. In fact, disruptions by U.S. government and Israeli authorities likely contributed to Hamas’ announcement in April 2023 that they would no longer receive bitcoin donations after specifically soliciting VA since 2019.\(^\text{125}\)

The U.S. government will continue to monitor and assess whether there is more widespread adoption of virtual assets by terrorist groups. For example, as virtual assets become more commonly used across the globe (especially in areas with poor financial and telecommunications infrastructures) and are more widely accepted to pay for goods and services, they may become more popular among terrorist groups.

**Non-Profit Organizations (NPOs)**

Charitable NPOs play a vital role in delivering humanitarian assistance to vulnerable populations throughout the world. Millions of people residing in crisis or conflict zones rely on the work of charitable NPOs. In the past, certain types of U.S.-based NPOs have been vulnerable to abuse by terrorist groups;\(^\text{126}\) however, in the last decade, the charitable sector has made strides in addressing and mitigating the threat posed by TF, including by increasing due diligence measures and risk mitigation efforts, often in collaboration with Treasury and the broader U.S. government.

Today, the vast majority of U.S. charitable NPOs have little exposure to TF.\(^\text{127,128}\) Within the United States, only a small subset of charitable NPOs with an international presence are vulnerable to TF. Failure to adopt appropriate risk mitigation measures to guard against unwitting diversion when operating in conflict zones where terrorist groups are active can increase TF vulnerability. Non-U.S. NPOs based in jurisdictions with less effective AML/CFT controls are more at risk of TF abuse, according to their types, activities, or characteristics.

As noted in the 2022 NTFRA, the U.S. government acknowledges the continued practice of many charitable NPOs to apply internal risk-mitigation measures, including due diligence, governance,

---


\(^{126}\) See *2015 National Terrorist Financing Risk Assessment*.

\(^{127}\) See 2022 NTFRA, p. 24.

\(^{128}\) This assessment is consistent with the global view that it is a small subset of charitable NPOs that have exposure to terrorist financing. See Best Practices on Combating the Abuse of Non-Profit Organisations (fatf-gafi.org).
transparency, accountability, and other compliance measures, including when responding to crises.\textsuperscript{129} Furthermore, implementing partners of the United States Agency for International Development (USAID) active in high-risk environments are also subject to additional vetting measures by USAID. These organizations must implement due diligence and risk-mitigation requirements to ensure full compliance with U.S. sanctions, including threats posed by terrorist organizations.\textsuperscript{130}

Despite these measures and Treasury’s work to standardize humanitarian-related authorizations across U.S. sanctions programs, some charitable NPOs continue to report challenges accessing financial services or experiencing financial-sector de-risking that interferes with essential, lifesaving services. Certain NPOs may also be targeted with repressive measures that can impact financial access, including misinformation campaigns that may characterize authorized humanitarian activities as diversion. When financial access is lost, some charitable NPOs have reported resorting to payment channels outside the regulated financial sector, which can increase TF risks.\textsuperscript{131} Thus, protecting and maintaining access to the banking system is imperative to reduce the TF risk of charitable NPOs.

TF risk presented by NPOs primarily arises in the context of sham charities, as distinct from legitimate charitable organizations. In the past several years, terrorist organizations have leveraged sham charities as a cover to raise funds. These sham charities are generally set up as foreign NPOs and may be established under the cover of providing humanitarian assistance but instead primarily or exclusively funnel money to a terrorist organization.

The Treasury Department is focused on identifying and designating sham charitable organizations, which reduces the overall TF risk of the NPO sector. For example, the Treasury Department has recently designated a number of sham charities.

- In 2023, Treasury imposed sanctions targeting Hamas-affiliated individuals and entities, including key Hamas officials and the mechanisms by which Iran provides support to Hamas and PIJ, such as through sham or fraudulent charitable organizations. Specifically, the Treasury designated the Gaza-based Al-Ansar Charity Association (Al-Ansar) and its director, Nasser Al Sheikh Ali, for serving as a conduit for illicit Iranian funds to Hamas and PIJ.\textsuperscript{132}

- In 2023, Treasury also sanctioned the Muhjat Alquds Foundation in Gaza, a PIJ-run, Iran-funded organization whose primary mission is to provide financial support to the families of PIJ fighters and prisoners. Treasury also designated the leader of the Muhjat Alquds Foundation, PIJ political official Jamil Yusuf Ahmad ‘Aliyan, who has distributed Iranian-provided funds to PIJ personnel in Gaza, has served on PIJ’s executive committee, and has overseen PIJ finances as it relates to important group logistics.\textsuperscript{133}

\begin{itemize}
  \item The Department of the Treasury’s De-Risking Strategy.
\end{itemize}
In 2023, Treasury designated an environmentalist organization called Green Without Borders for providing support to, and collaborating with Hizballah in Lebanon.\textsuperscript{134} Hizballah utilized outposts associated with Green Without Borders to hide weapons training and munitions tunnels, and thus provided cover to Hizballah’s activities.\textsuperscript{135}

In 2022, the United States sanctioned a foreign NPO called World Human Care, established by the designated terrorist group Majelis Mujahidin Indonesia (MMI).\textsuperscript{136} World Human Care did engage in some humanitarian activities, but the organization was established by MMI primarily to raise funds for its sympathizers in Syria.\textsuperscript{137}

Fraudulent charitable appeals, without the involvement of a registered NPO, are the most common form of charitable abuse by terrorist groups. This method allows groups to cast a wide net to raise funds online, either through social media or dedicated crowdfunding websites (discussed in more detail below). This activity is difficult to detect and may result in individuals wittingly or unwittingly donating to a terrorist cause. This vulnerability is amplified by the fact that anyone can purport to raise money online using the pretext of a humanitarian cause, and the money must be tracked through to the end destination to be identified as funding terrorism.

Accordingly, although some NPOs have been misused to facilitate terrorist financing, Treasury and other U.S. government agencies note that the vast majority of U.S.-based tax-exempt charitable organizations face little or no risk of being abused for TF. This risk is substantially mitigated by the adoption of due diligence measures by charitable NPOs, Treasury’s actions to identify and designate sham charitable organizations, and efforts to ensure NPOs have access to financial services.

**EMERGING TRENDS**

**Crowdfunding & Online Fundraising**

Crowdfunding and online fundraising are used domestically and transnationally for a variety of purposes including by charities or NPOs, business owners, and peer-to-peer exchanges.\textsuperscript{138} The use of crowdfunding is substantial and growing: the global crowdfunding market is projected to reach $34.6 billion by 2026.\textsuperscript{139} It involves many different actors, cross-border elements, and technological developments that can be exploited for TF purposes.\textsuperscript{140} Notably, the majority of crowdfunding activity is legitimate. This status can make it more difficult for law enforcement attempting to investigate potential TF cases with a crowdfunding and online fundraising nexus. Compounding this issue, the anonymity, speed of transfers, and global reach of this method to collect and move funds make it an

\begin{itemize}
\item In 2023, Treasury designated an environmentalist organization called Green Without Borders for providing support to, and collaborating with Hizballah in Lebanon.\textsuperscript{134} Hizballah utilized outposts associated with Green Without Borders to hide weapons training and munitions tunnels, and thus provided cover to Hizballah’s activities.\textsuperscript{135}
\item In 2022, the United States sanctioned a foreign NPO called World Human Care, established by the designated terrorist group Majelis Mujahidin Indonesia (MMI).\textsuperscript{136} World Human Care did engage in some humanitarian activities, but the organization was established by MMI primarily to raise funds for its sympathizers in Syria.\textsuperscript{137}
\end{itemize}
attractive option for terrorist organizations.\(^{141}\)

In the context of DVE, individuals who perpetrate attacks typically act alone or in a small group without seeking outside support or financing. Despite support voiced for these incidents, association is not a crime and thus donations to DVE or ideologically driven groups itself may not be sufficient cause for legal action. Further, some of the activities funded through these platforms may be constitutionally protected in the United States and would not be illegal unless tied to a specific act of violence or other unlawful act. As such, crowdfunding and online fundraising are typically legal activities employed to collect membership fees and fund programming. Over the past several years, DVEs and like-minded supporters have raised and moved millions of dollars using online crowdfunding platforms.\(^{142}\)

Like domestic actors, international terrorist actors are successful in soliciting donations online. Terrorists continue to use encrypted apps like Telegram for communication as well as coordinating fundraising efforts, inhibiting law enforcement access to these communications. Also, fundraising campaigns often employ both fiat and virtual currencies, making it difficult to trace the origination of the transactions.

Crowdfunding through social media also represents a significant challenge for authorities. Online crowdfunding on these platforms can be done under the guise of legitimate charitable donations, making it difficult to identify as terrorist financing.\(^{143}\) Vigilant monitoring is required to ensure illicit fundraising posts are quickly identified and taken down by social media companies. Further, some social media companies have now integrated their own payment mechanisms, creating another potential opportunity to transfer funds in support of terrorist activities. Additionally, the anonymity social media can provide a user can obscure the true identity of someone raising funds for illicit purposes.

Crowdfunding sees the convergence of many terrorist financing vulnerabilities: the overlap of social media, encrypted messaging platforms, peer-to-peer payments, virtual assets, and digitally enabled fundraising platforms. Utilizing more than one of these methods can obfuscate the source of funds or identity of the original transferrer. Many of these sectors are not required to apply AML/CFT measures as financial institutions, though they may intersect with an obligated entity at some point in the life cycle of the transaction.

\(^{141}\) Id.

\(^{142}\) See, e.g., ADL Crowdfunding Report: How Bigots and Extremists Collect and Use Millions in Online Donations | ADL.

\(^{143}\) See, for example, see FinCEN Alert, FIN-2023-Alert006, October 20, 2023 (identifying as a red flag indicator “A customer that is a charitable organization or nonprofit organization (NPO) solicits donations but does not appear to provide any charitable services or openly supports Hamas’s terrorist activity or operations. In some cases, these organizations may post on social media platforms or encrypted messaging apps to solicit donations, including in virtual currency.”
Conclusion

The terrorism and terrorist financing threat has evolved significantly since Treasury’s first iteration of the TFRA in 2015. Terrorist organizations and violent extremist movements have shifted to a more diffuse, less hierarchical, networked structure facilitated by online communication, in which individuals may self-radicalize and become inspired by an ideology from across the globe. In the financing context, this means attacks by such radicalized individuals are smaller scale and require less outside financing, creating significant challenges for financial institutions and law enforcement looking to prevent attacks. However, terrorist organizations will still look to battle-tested methods of raising, moving, and using funds. As noted in the 2022 NTFRA, the threat of DVEs and financing of associated attacks continues to be the most pressing challenge for USG authorities.

While the world has seen significant successes in the past twenty-five years in the fight against the global scourge of terrorism, the October 7, 2023, Hamas attacks unambiguously demonstrated the awful consequences of underestimating the lethality of a group that has been developing a sophisticated financial enterprise in the background of other threats that were thought to be more acute. Even as new security challenges arise, terrorist adversaries adapt to our efforts, and new terrorist threats emerge around the world and here at home, the United States remains committed to evolving to meet this challenge and countering the next decade of terrorist threats.
Participants

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

• **Department of Homeland Security**
  • Office of Strategy, Policy, and Plans,
    ▪ Office of Counterterrorism Threat Prevention and Law Enforcement

• **Department of Justice (DOJ)**
  • Criminal Division
  • National Security Division
  • Federal Bureau of Investigation (FBI)
    ▪ Counterterrorism Division
    ▪ Criminal Investigative Division

• **Department of State (DOS)**
  • Bureau of Counterterrorism

• **Department of the Treasury**
  • Office of Terrorism and Financial Intelligence
    ▪ 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)
  • Internal Revenue Service (IRS)
    ▪ Criminal Investigation (CI)
    ▪ Tax Exempt & Government Entities Division (TEGE)

• **National Counterterrorism Center (NCTC)**
• **Staff of the Federal Functional Regulators**\(^{144}\)

---

\(^{144}\) This includes staff of the Commodity Futures Trading Commission (CFTC), the Federal Deposit Insurance Corporation, the Board of Governors of the Federal Reserve System, the National Credit Union Administration, the Office of the Comptroller of the Currency, and the Securities and Exchange Commission.
Methodology and Terminology

The terminology and methodology of the 2024 NTFRA are based on the guidance of the FATF, which is the international standard-setting body for anti-money laundering and countering the financing of terrorism (AML/CFT) safeguards. This guidance lays out a process for conducting a TF risk assessment at the national level.145 The underlying concepts for this risk assessment are threats (the terrorists who are most active in raising or moving funds through the United States or U.S. financial system), vulnerabilities (weaknesses that facilitate TF), consequences (the effect of a vulnerability if successfully exploited by a threat), and risks (the synthesis of threat, vulnerability, and consequence). This approach uses the following key concepts:

- **Threat:** A threat is a person, a group of people, or activity with the potential to cause harm by raising, moving, storing, or using funds and other assets (whether from legitimate or illegitimate sources) for terrorist purposes. In the TF context, this includes terrorist groups and their facilitators, as well as radicalized individuals seeking to exploit the U.S financial system to raise, move, and use funds.

- **Vulnerability:** A vulnerability can be exploited to facilitate TF, both in the raising of funds for terrorist networks and the movement of funds to terrorists and terrorist organizations. It may relate to a specific financial product used to move funds, a weakness in regulation, supervision, or enforcement, or reflect unique circumstances that may impact opportunities for terrorist financiers to raise or move funds or other assets. There may be some overlap in the vulnerabilities exploited for both money laundering (ML) and TF.

- **Consequence:** Consequence refers to the impact or harm that a TF threat may cause if it can exploit a vulnerability and be operationalized. Not all TF methods have equal consequences. The methods that raise or move the greatest amount of money most effectively often present the greatest potential TF consequences. However, it may require only a small amount of funds to execute a terrorist act with devastating human consequences. Therefore, the 2024 NTFRA focuses on threats and vulnerabilities in determining TF risks.

- **Risk:** Risk is a function of threat, vulnerability, and consequence. It represents a summary judgment, taking into consideration the effect of mitigating measures, including regulation, supervision, and enforcement.

The 2024 NTFRA relies on an analysis of criminal prosecutions, Treasury designations, financial institution reporting, threat assessments and advisories, and other information available to the U.S. government, along with a review of information on TF from international bodies such as the Financial Action Task Force (FATF) and nongovernmental organizations (NGOs). This information was used to determine (1) the terrorist groups or movements that are most active in raising and moving funds through the United States and the U.S. financial system, and the methods and typologies used by those groups to raise and move funds, (2) which characteristics of financial products, services, or market participants facilitate the raising or movement of funds by or on behalf of terrorists or terrorist organizations, and (3) the extent to which domestic laws and regulations, law enforcement investigations and prosecutions, regulatory compliance and supervision, enforcement activity, and international outreach and coordination mitigate identified TF threats and vulnerabilities. This research and analysis was then used to identify the resulting TF risks facing the United States. Data collected is current as of January 31, 2024.

---

## List of Acronyms

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AGAAVE</td>
<td>Anti-Government or Anti-Authority Violent Extremist</td>
</tr>
<tr>
<td>AML/CFT</td>
<td>Anti-Money Laundering/Countering the Financing of Terrorism</td>
</tr>
<tr>
<td>ANF</td>
<td>Al-Nusrah Front</td>
</tr>
<tr>
<td>AQ</td>
<td>al-Qa’ida</td>
</tr>
<tr>
<td>AQIM</td>
<td>al-Qa’ida in the Islamic Maghreb</td>
</tr>
<tr>
<td>BSA</td>
<td>Bank Secrecy Act</td>
</tr>
<tr>
<td>CBDC</td>
<td>Central Bank Digital Currency</td>
</tr>
<tr>
<td>CFTC</td>
<td>Commodity Futures Trading Commission</td>
</tr>
<tr>
<td>CVC</td>
<td>Convertible Virtual Currency</td>
</tr>
<tr>
<td>DHS</td>
<td>Department of Homeland Security</td>
</tr>
<tr>
<td>DOJ</td>
<td>Department of Justice</td>
</tr>
<tr>
<td>DVE</td>
<td>Domestic Violent Extremist</td>
</tr>
<tr>
<td>FATF</td>
<td>Financial Action Task Force</td>
</tr>
<tr>
<td>FBI</td>
<td>Federal Bureau of Investigation</td>
</tr>
<tr>
<td>FCM</td>
<td>Future Commission Merchant</td>
</tr>
<tr>
<td>HTS</td>
<td>Hayat Tahrir al-Sham</td>
</tr>
<tr>
<td>IC</td>
<td>Intelligence Community</td>
</tr>
<tr>
<td>IJO</td>
<td>Islamic Jihad Organization</td>
</tr>
<tr>
<td>IRGC</td>
<td>Islamic Revolutionary Guard Corps</td>
</tr>
<tr>
<td>ISIS</td>
<td>Islamic State of Iraq and Syria</td>
</tr>
<tr>
<td>ISIS-DRC</td>
<td>ISIS- Democratic Republic of the Congo</td>
</tr>
<tr>
<td>ISIS-K</td>
<td>ISIS-Khorasan</td>
</tr>
<tr>
<td>MMI</td>
<td>Majelis Mujahidin Indonesia</td>
</tr>
<tr>
<td>MSB</td>
<td>Money Service Business</td>
</tr>
<tr>
<td>MVE</td>
<td>Militia Violent Extremist</td>
</tr>
<tr>
<td>NGO</td>
<td>Non-Governmental Organization</td>
</tr>
<tr>
<td>NMLRA</td>
<td>National Money Laundering Risk Assessment</td>
</tr>
<tr>
<td>NPFRA</td>
<td>National Proliferation Financing Risk Assessment</td>
</tr>
<tr>
<td>NTFRA</td>
<td>National Terrorist Financing Risk Assessment</td>
</tr>
<tr>
<td>Abbreviation</td>
<td>Full Form</td>
</tr>
<tr>
<td>--------------</td>
<td>-----------</td>
</tr>
<tr>
<td>NPO</td>
<td>Non-Profit Organization</td>
</tr>
<tr>
<td>NPRM</td>
<td>Notice of Proposed Rulemaking</td>
</tr>
<tr>
<td>ODNI</td>
<td>Office of the Director of National Intelligence</td>
</tr>
<tr>
<td>OFAC</td>
<td>Office of Foreign Assets Control</td>
</tr>
<tr>
<td>P2P</td>
<td>Person-to-Person</td>
</tr>
<tr>
<td>PIJ</td>
<td>Palestinian Islamic Jihad</td>
</tr>
<tr>
<td>RIM</td>
<td>Russian Imperial Movement</td>
</tr>
<tr>
<td>RMVE</td>
<td>Racially or Ethnically Motivated Violent Extremist</td>
</tr>
<tr>
<td>SAR</td>
<td>Suspicious Activity Report</td>
</tr>
<tr>
<td>TF</td>
<td>Terrorist Financing</td>
</tr>
<tr>
<td>UAE</td>
<td>United Arab Emirates</td>
</tr>
<tr>
<td>UN</td>
<td>United Nations</td>
</tr>
<tr>
<td>USAID</td>
<td>U.S. Agency for International Development</td>
</tr>
<tr>
<td>VA</td>
<td>Virtual Asset</td>
</tr>
<tr>
<td>VASP</td>
<td>Virtual Asset Service Provider</td>
</tr>
</tbody>
</table>
2024 National Proliferation Financing Risk Assessment
Department of the Treasury

2024 National Proliferation Financing Risk Assessment
# Table of Contents

EXECUTIVE SUMMARY ................................................................. 1

THREATS ......................................................................................... 3
  Russian Federation ................................................................. 3
  DPRK ......................................................................................... 4
  Iran ......................................................................................... 5
  People’s Republic of China (PRC) ............................................. 6
  Syria ......................................................................................... 7
  Pakistan ..................................................................................... 7
  Non-state actors ....................................................................... 7

VULNERABILITIES ......................................................................... 8
  Economic Factors ..................................................................... 8
  Legal and Regulatory Factors .................................................. 9

CASE STUDIES ............................................................................. 11
  Part One: The “traditional” procurement and revenue-raising model ........................................ 12
  Part Two: Cyber-Enabled Proliferation Financing: The “new” digital evasion model ................. 18

EMERGING TRENDS ..................................................................... 23
  Sanctions Evasion and State Complicity .................................. 23
  New & Alternative Payment Infrastructure ............................... 23
  Emerging Technologies ............................................................ 24

CONCLUSION ............................................................................... 24

PARTICIPANTS ............................................................................. 26

SCOPE & DEFINITION ................................................................. 27

METHODOLOGY ........................................................................ 28

LIST OF ACRONYMS ................................................................... 30

APPENDIX: Recent Guidance/Alert/Advisory Documents ............ 31
EXECUTIVE SUMMARY

The 2024 National Proliferation Financing (PF) Risk Assessment (NPFRA) updates the United States' two previous NPFRAs.¹ In line with the Financial Action Task Force’s (FATF’s) PF risk assessment guidance,² the United States finds that conducting an assessment to identify and better understand PF risk on a regular basis is essential to strengthen our ability to prevent individuals and entities from raising, storing, moving, and using funds, financial assets, or other economic resources in connection with the proliferation of weapons of mass destruction (WMD).³ This assessment was prepared according to Sections 261 and 262 of the Countering America’s Adversaries through Sanctions Act (P.L. 115-44) as amended by Section 6506 of the Fiscal Year 2022 National Defense Authorization Act (P.L. 117-81).

Vulnerabilities identified in the 2022 NPFRA persisted over the review period.⁴ The size of the U.S. financial system, the centrality of the U.S. dollar in global trade, and the role of U.S. manufacturers in producing military and proliferation-related technology (including dual-use items) continue to make the United States a target of exploitation by PF networks. These structural vulnerabilities are mitigated to a significant extent by a strong culture of compliance with U.S. law⁵ by U.S. financial institutions and other private sector actors, though some gaps remain. Specifically, over the review period, the United States worked to finalize the implementation of the Corporate Transparency Act (CTA) to close gaps for collection of beneficial ownership information (BOI)⁶ that will aid in investigations involving shell and front companies. The varying levels of anti-money laundering (AML), countering the financing of terrorism (CFT), and countering proliferation financing (CPF) (AML/CFT/CPF) controls for the virtual asset sector globally, as well as some compliance deficiencies with U.S. Virtual Asset Service Providers (VASPs), also make the United States vulnerable to PF networks.

Likewise, the threat actors the United States identified in 2022 still pose PF risks based on available intelligence and case studies provided by law enforcement. Over the review period, the United States has seen persistent efforts by PF networks, operating on behalf or at the direction of state actors, including the Russian Federation, Democratic People’s Republic of Korea (DPRK), Iran, the People’s Republic of China (PRC), Syria, and Pakistan, to exploit the U.S. financial system and other U.S. private sector actors to finance WMD proliferation. This activity includes both financing to procure goods for the purpose of developing WMD as well as revenue-raising that provides state actors the resources to

⁴ From January 1, 2022 to January 1, 2024.
⁵ For a more detailed description of the U.S. CPF legal and regulatory framework, see the 2022 NPFRA, pp. 2-3 and 16-17.
⁶ In the context of legal persons, beneficial owner refers to the natural person(s) who ultimately owns or controls a customer and/or the natural person on whose behalf a transaction is being conducted. It also includes those natural persons who exercise ultimate effective control over a legal person. Only a natural person can be an ultimate beneficial owner, and more than one natural person can be the ultimate beneficial owner of a given legal person.
advance their WMD activities, in violation of international and/or U.S. law (i.e., evasion of financial or trade sanctions or export controls).\footnote{FinCEN and BIS, “FinCEN and the U.S. Department of Commerce's Bureau of Industry and Security Announce New Reporting Key Term and Highlight Red Flags Relating to Global Evasion of U.S. Export Controls,” (November 6, 2023), \url{https://www.fincen.gov/sites/default/files/shared/FinCEN_Joint_Notice_US_Export_Controls_FINAL508.pdf}.}

Based on a review of the relevant data since 2022, two state actors—Russia and the DPRK—are the highest-risk threat actors and are highlighted because of the scope and sophistication of their illicit procurement and revenue-generation efforts:

- **Russia’s illegal, unprovoked, and unjustified full-scale invasion of Ukraine in February 2022 cast a spotlight on its illicit procurement of a variety of goods and technologies with military applications, including delivery systems and dual-use items. As demonstrated by the case studies in this assessment, as well as recent U.S. government action, Russia continues to utilize complex transnational networks in Türkiye, the United Arab Emirates (UAE), the PRC, and other countries, to acquire much-needed technology and equipment for its war economy.\footnote{Department of the Treasury, “Treasury Imposes Sanctions on More than 150 Individuals and Entities Supplying Russia's Military-Industrial Base,” December 12, 2023, \url{https://home.treasury.gov/news/press-releases/jy1978}.} In response, the United States and its allies and partners have launched an unprecedented multilateral effort to detect, disrupt, and, where possible, prosecute these activities.\footnote{For relevant guidance and alerts released in response to Russia’s further invasion of Ukraine, see Appendix.}
  - Specifically, the new amendment to E.O. 14024 authorizes the imposition of U.S. sanctions on foreign financial institutions that are either (1) facilitating significant transactions on behalf of persons designated for operating in certain key sectors of the Russian economy that support the country’s military-industrial base; or (2) facilitating significant transactions or providing services involving Russia’s military-industrial base, including those relating to specific manufacturing inputs and technological materials that Russia is seeking to obtain from foreign sources. The White House, “Executive Order on Taking Additional Steps with Respect to the Russian Federation’s Harmful Activities,” (December 22, 2023), \url{https://www.whitehouse.gov/briefing-room/presidential-actions/2023/12/22/executive-order-on-taking-additional-steps-with-respect-to-the-russian-federations-harmful-activities/}. See the accompanying Compliance Advisory, Department of the Treasury, OFAC, “Guidance for Foreign Financial Institutions on OFAC Sanctions Authorities Targeting Support to Russia’s Military-Industrial Base,” (December 22, 2023), \url{https://ofac.treasury.gov/media/932436/download?inline}.}

- **The DPRK continued to conduct malicious cyber activity and deploy information technology (IT) workers to, at least in part, fund its WMD capabilities.\footnote{Department of the Treasury, “Treasury Targets DPRK Malicious Cyber and Illicit IT Worker Activities,” (May 23, 2023,) \url{https://home.treasury.gov/news/press-releases/jy1498}.} This activity included efforts to illicitly raise revenue in fiat currency and virtual assets, including hacking of VASPs and, to a lesser extent, ransomware attacks.

- **Russia and the DPRK have collaborated on arms purchases and military assistance in direct violation of United Nations Security Council Resolutions (UNSCRs). Specifically, the DPRK has provided military equipment and munitions to Russia for use in its full-scale invasion of Ukraine. The United States is concerned that, in exchange for such materiel, Moscow will provide military assistance to Pyongyang to expand its WMD program.\footnote{Department of State, “U.S.-Japan-ROK Joint Statement Condemning DPRK-Russia Arms Transfer,” (October 25, 2023), \url{https://www.state.gov/u-s-japan-rok-joint-statement-condemning-dprk-russia-arms-transfers/}.}
As with the National Risk Assessments for Money Laundering and Terrorist Financing, the 2024 NPFRA informs the forthcoming 2024 National Strategy to Combat Terrorist and Other Illicit Financing, which will discuss interagency progress on further strengthening the U.S. AML/CFT/CPF regime and will seek to assist individuals and entities subject to U.S. law in remaining vigilant against efforts to evade those laws through a variety of deceptive practices described in these assessments. These risk assessments also inform and complement the National AML/CFT Priorities issued by the Financial Crimes Enforcement Network (FinCEN).

**Threats**

This section identifies the PF threat actors facing the United States and summarizes significant geopolitical and security developments since the 2022 NPFRA. State-sponsored or -affiliated actors continue to pose the most significant PF threat to the United States. Their WMD programs can leverage significant technical expertise to design and execute clandestine procurement and revenue-raising schemes at scale, even if they are subject to comprehensive multilateral and U.S. sanctions and export controls.

**Russian Federation**

Russia maintains the largest and most capable nuclear weapons stockpile in the world, as well as significant conventional capabilities, both of which it continues to expand and modernize. Russia’s unlawful invasion of Ukraine is the most significant geopolitical change since the 2022 NPFRA and has raised Russia’s PF threat profile. Because of heavy battlefield losses, Russia has engaged with close partners to replenish its stocks of conventional weapons. Those losses have also increased Russia’s reliance on nuclear, cyber, and space capabilities to maintain deterrence and project power elsewhere.

Since February 2022, Russia has pulled back from its role or fully suspended its participation in certain international arms control and WMD mechanisms, including treaties. Russia has said it is suspending its participation in the New Strategic Arms Reduction Treaty (New START), which the United States has called legally invalid and irresponsible. The United States continues to certify that Russia is in breach of its commitments to the Chemical Weapons Convention, based on Russia’s use of chemical weapons in targeted assassinations, support for the Assad regime’s use of chemical weapons, and its ongoing, undeclared offensive chemical weapons program. In November 2023, Russia revoked its ratification of the Comprehensive Nuclear-Test-Ban Treaty, which prohibits any testing of nuclear explosive devices and is a cornerstone of preventing nuclear proliferation, a step condemned by the Secretary...
General of the United Nations as well as the United States.\textsuperscript{19}

Due in large part to the imposition of sanctions by the United States and its allies and partners, Russia faces a degraded ability to fund its defense priorities generally.\textsuperscript{20} Based on the case studies below, Russia has prioritized overseas procurement of goods and technologies it may not be able to source directly because of multilateral sanctions pressure targeting its military-industrial complex. This course of action directly implicates U.S. financial institutions and other private sector entities. As demonstrated by the case studies, in some instances this is because the goods themselves are produced in the United States, and the underlying transactions are with accounts held by U.S. businesses in U.S. financial institutions. In other cases, Russia may illicitly procure goods from other jurisdictions, in which case the transaction chain touches U.S. jurisdiction through correspondent accounts with U.S. banks.

Russian PF networks leverage front and shell companies to place orders for needed components. These networks often then obfuscate the end-user and destination for the goods, routing shipments through third countries before they are ultimately delivered to customers in Russia. Recent U.S. designations highlight the multinational networks of illicit actors that participate in procuring goods for Russia’s military-industrial purposes.\textsuperscript{21}

\textit{Russia’s Procurement Relationship with the DPRK and Iran}

As a direct consequence of its battlefield losses, Russia has sought out cooperative procurement relationships with other states of proliferation concern including the DPRK and Iran. These activities directly undermine the integrity of the global nonproliferation regime. With respect to the DPRK, the United States and its partners have accused Russia of violating numerous UNSCRs by procuring military equipment and munitions from Pyongyang.\textsuperscript{22} The United States has also accused Tehran of exporting Unmanned Aerial Vehicles (UAVs) in violation of UNSCR 2231 in support of Russia’s further invasion of Ukraine, though the United States has not linked this proliferation to the use of WMD.\textsuperscript{23}

\textbf{DPRK}

According to the 2023 Director of National Intelligence (DNI) Annual Threat Assessment, the DPRK continued to augment its WMD capability over the review period, most publicly through the testing in 2022 and 2023 of multiple types of Intercontinental Ballistic Missiles (ICBMs), including the use of such technology to launch a military satellite.\textsuperscript{24} According to the Intelligence Community, the Kim Jong-Un


\textsuperscript{23} Department of State, “The United States Imposes Sanctions on Russian Entities Involved in UAV Deal With Iran,” (December 9, 2022), \url{https://ua.usembassy.gov/the-united-states-imposes-sanctions-on-russian-entities-involved-in-uav-deal-with-iran/}.

\textsuperscript{24} DNI, \textit{Threat Assessment}, p. 20; Secretary of State Antony Blinken, “Designating Supporters of DPRK Weapons Programs Together with Allies,” (November 30, 2023), \url{https://www.state.gov/designating-supporters-of-dprk-weapons-programs-together-with-allies/}.  

regime sees the possession of nuclear weapons as critical for its survival and to deter perceived threats from its neighbors and the United States.

The DNI Threat Assessment noted that the regime will increase its use of methods like cyber theft and illicit trade to raise revenue to support its strategic priorities, including its WMD program. The U.S. government has cited public estimates of the revenue the DPRK has generated through these means. According to the UN Panel of Experts, the DPRK attempted to steal as much as $2 billion between 2015 and 2019 through cyber means. According to private industry estimates, the DPRK stole up to $1.7 billion in virtual assets in 2022 alone. It is important to note that these are just estimates, as the nature of the activity means any figure will not incorporate all proceeds and may include revenue misattributed to DPRK-linked actors.

The September 2023 report of the DPRK UN Panel of Experts documents Pyongyang’s ongoing access to the international financial system through overseas banking representatives, joint ventures, cooperative entities, and illicit business activities. In November 2023, OFAC announced the designation of eight individuals associated with DPRK state-owned weapons exporters, financial institutions, and front companies, including the Reconnaissance General Bureau, the DPRK’s main foreign intelligence agency, and the Foreign Trade Bank (FTB), the DPRK’s primary foreign exchange bank.

**Iran**

The United States has continued to monitor Iran’s resumption of nuclear activities. According to the DNI Threat Assessment, Iran is increasing the size and enrichment level of its uranium stockpile and is conducting advanced centrifuge research and development. According to the International Atomic Energy Agency (IAEA), Iran has taken steps detrimental to the implementation of the Non-Proliferation Treaty Safeguards Agreement, including the withdrawal of designations of inspectors, which negatively impacts IAEA verification activities. However, the Intelligence Community assesses that Iran has not undertaken the key nuclear weapons development activities that would be necessary to produce a testable nuclear device, though its current research and development trajectory brings it closer to producing the fissile material for completing a device following a decision to do so.

---


26 UN Panel of Experts, 1718 Committee, Midterm report of the Panel of Experts submitted pursuant to resolution 2683 (2023), (September 12, 2023), https://www.un.org/securitycouncil/sanctions/1718/panel_experts/reports. Generally, DPRK banking representatives are individuals working on behalf of or at the direction of a DPRK bank or financial institution. They are often working abroad and U.N. member states are obliged to expel such individuals, as their activity is a violation of UNSCRs.


28 DNI, Threat Assessment, p. 18. According to State Department statements, “The production of high-enriched uranium by Iran has no credible civilian justification and the reported production at the Fordow Fuel Enrichment Plant and the Pilot Fuel Enrichment Plant further carries significant proliferation-related risks.” Department of State, “Joint Statement on the Latest Iranian Nuclear Steps Reported by the IAEA,” (December 20, 2023), https://www.state.gov/joint-statement-on-the-latest-iranian-nuclear-steps-reported-by-the-iaea/#:~:text=The%20production%20of%20high%20enriched,carries%20significant%20proliferation%20risks.

29 IAEA, “IAEA Director General’s Statement on Verification in Iran,” (September 16, 2023), https://www.iaea.org/newscenter/pressreleases/iaea-director-generals-statement-on-verification-in-iran-0.
In October 2023, the United Nations’ restrictions on Iran’s missile-related activities under UNSCR 2231 expired. The United States and partner countries remain committed to countering Iran’s procurement, development, and proliferation of missiles, UAVs, and other military weapons. On October 18, 2023, the Departments of the Treasury and State jointly acted to sanction the actors involved in Tehran’s missile and conventional arms activities and issued accompanying guidance to alert persons and businesses globally to Iran’s ballistic missile procurement activities. The United States also joined 46 other Proliferation Security Initiative countries in affirming their shared commitment to Iranian ballistic missile-related counterproliferation efforts, regardless of the status of UNSCR 2231.

As referenced in the Russia threat section, the United States also remains focused on Iran’s acquisition, development, procurement, and proliferation of UAVs, which Tehran has provided to Russia, as well as affiliated groups in the Middle East. It has also done so to (1) Iranian-aligned militia groups in Iraq, who have used UAVs to attack US forces in Iraq and Syria, and (2) the Houthis in Yemen, who have used the weapons to conduct strikes inside Yemen and against countries in the region, including Saudi Arabia, the UAE, a likely attempt to strike targets in Israel, and against commercial shipping in the Red Sea. Iran relies on foreign procurement of critical components for its UAVs.

People’s Republic of China (PRC)

The PRC continues to pursue its goal of building a military that can protect its territory and government, make it a preeminent player in regional affairs, offset U.S. military superiority, and project power globally. The PRC has clearly stated its ambition to strengthen its “strategic deterrent,” and continued throughout 2022 and 2023 to accelerate the modernization, diversification, and expansion of its nuclear forces, and develop its cyber, space, and counterspace capabilities. To support its military modernization efforts, the Intelligence Community assesses that the PRC and those acting on behalf of PRC governmental entities will continue to engage in economic espionage and cyber theft to acquire technology and know-how. Analysis from the Department of Defense (DOD) supports this view, pointing to “multiple U.S. criminal indictments since 2015 involving espionage by PRC nationals, naturalized U.S. citizens or permanent resident aliens from the PRC, as well as U.S. citizens, for their efforts to illegally acquire information and technology to advance [Chinese military] modernization.”


33  DNI, Annual Threat Assessment, p. 7.


35  DNI, Annual Threat Assessment, p. 9.

**Syria**

The United States and its partners continue to seek accountability for the Assad regime’s past use of chemical weapons.\(^\text{37}\) Syria’s capabilities have been built in part on illicit procurement and fundraising which, in the past, transited the U.S. financial system. This assessment does not include any case studies that demonstrate this activity during the review period, but U.S. financial institutions and other private sector entities should remain vigilant of the sanctions and export control risk arising from the activities of the Syrian government.

**Pakistan**

In testimony for the 2022 DNI Annual Threat Assessment, the Director of the Defense Intelligence Agency noted that Pakistan will continue to perceive nuclear weapons as key to its national survival in the face of neighboring India’s nuclear arsenal and conventional force superiority. To this end, Pakistan has continued its ballistic missile development. In October 2023, the United States, for the first time, imposed blocking sanctions under E.O. 13382 on three PRC-based suppliers to Pakistan’s ballistic missile program.\(^\text{38}\) While the PRC remains a key defense partner for Pakistan, individuals and entities acting on behalf of Pakistan have engaged in illicit procurement for specific U.S.-origin goods, violating relevant U.S. export control laws and where the underlying transactions have passed through U.S. financial institutions.

**Non-state actors**

The 2018 and 2022 NPFRAs noted that the United States remains concerned about the efforts of terrorist groups and other non-state actors to acquire WMD capabilities. In November 2022, with significant support from the United States and like-minded countries, the UN Security Council renewed the mandate for UNSCR 1540, focusing on preventing the proliferation of WMDs, knowledge, or precursor material to non-state actors.\(^\text{39}\) In March 2023, the United States released a National Security Memorandum (NSM) on WMD Terrorism and Advance Nuclear and Radioactive Material Security.\(^\text{40}\) The NSM seeks to provide a framework to prevent non-state actors from acquiring WMD and related materials. To date, we have not assessed that those efforts have involved exploitation of the U.S. financial system, placing those activities outside the scope of this assessment.

---


\(^{38}\) Department of State, “United States Sanctions Entities Contributing to Ballistic Missile Proliferation,” [https://www.state.gov/united-states-sanctions-entities-contributing-to-ballistic-missile-proliferation/#:~:text=13382%20for%20having%20engaged%2C%20or%2C%20in%20engaged%2C%20or%2C%20including%20any%20efforts%20to](https://www.state.gov/united-states-sanctions-entities-contributing-to-ballistic-missile-proliferation/#:~:text=13382%20for%20having%20engaged%2C%20or%2C%20in%20engaged%2C%20or%2C%20including%20any%20efforts%20to). See also the updates to the SDN List at Treasury, OFAC, “Balkans-related Designations and Designation Removal; Non-Proliferation Designations,” (October 20, 2023), [https://ofac.treasury.gov/recent-actions/20231020](https://ofac.treasury.gov/recent-actions/20231020).


Vulnerabilities

Consistent with the findings of the 2018 and 2022 NPFRA, the case studies in the threats section demonstrate that weapons proliferators and procurement agents seek to illegally acquire U.S. technology, including dual-use items, and access to the international and U.S. financial system to disguise their payments for goods and services, or to raise funds to evade U.S. and UN sanctions to at least partially support WMD programs. This activity often involves the falsification of BOI, obfuscating end-user/end-use and ultimate destination, and is challenging to detect for both the public and private sector as shell and front companies are routinely used to either illegally acquire goods or to transship goods to a third country for diversion. More recently, some state actors, such as the DPRK, have resorted to illicit cyber activity and deployment of IT workers as additional revenue streams. These vulnerabilities were highlighted in the 2022 NPFRA, and threat actors continued to exploit them in the review period.

Economic Factors

The U.S. financial system's size, sophistication, stability, and openness makes it particularly vulnerable to misuse by illicit proliferation networks. The financial sector in the United States provides access to a broad range of financial services to private sector actors, including banks in foreign countries, through correspondent banking and other financial services relationships. While this access is important for promoting international commerce, trade, and overall economic growth, proliferators have exploited it to raise, store, move, and use funds.

The preeminence of the U.S. financial system is due to the U.S. dollar’s status as the preferred currency for many functions of the global economy, especially for holding international reserves, serving its use as a “currency anchor,” and facilitating cross-border transactions. According to Federal Reserve analysis, the U.S. dollar is overwhelmingly the world’s most frequently used currency in global trade, accounting for 96% of trade invoicing in the Americas, 74% in the Asia-Pacific, and 79% in the rest of the world. Additionally, about 60% of international and foreign currency claims (primarily loans) and liabilities (primarily deposits) are U.S. dollar denominated. While other currencies have seen a relative increase in their share of these categories, the relatively stable dominance of the U.S. dollar means that a significant volume of global illicit procurement or sanctions evasion activity occurs in U.S. dollars and transits U.S. bank accounts.

Industrial and technological factors also contribute to proliferation networks seeking to illicitly acquire goods from firms based in the United States. The United States has the largest defense sector in the world. According to the Congressional Research Service, the defense industrial base is generally understood to comprise all organizations and facilities that provide the U.S. DOD with materials, products, and services. The same analysis cites a figure from the National Defense Industrial Association that this universe includes nearly 60,000 companies employing approximately 1.1 million people as of 2021.


Many of these firms produce high-quality military technology and dual-use items, including for export. Such arms sales and transfers are subject to robust controls, including a comprehensive export control regime administered by the Department of Commerce and with oversight by the Department of State and DOD. But as demonstrated in the case studies, PF networks pursue a variety of obfuscation techniques to evade those controls. These networks deliberately falsify export-related paperwork, including license applications, bills of lading, insurance, and other documentation, making it difficult for U.S. manufacturers to confirm the intent to divert items to improper end-users.

Legal and Regulatory Factors
As documented in the 2018 and 2022 NPFRAs, the United States maintains a robust legal regime for AML/CFT/CPF, sanctions, and export controls. All natural and legal U.S. persons must comply with OFAC and State Department sanctions and Department of Commerce export control regulations. Additionally, U.S. financial institutions and other entities with AML program requirements under the BSA must mitigate PF risk through the appropriate, risk-based implementation of their BSA requirements, including customer due diligence, transaction monitoring, and the filing of suspicious activity reports (SARs).

Notwithstanding those strengths, previous NPFRAs also identified gaps in the U.S. AML/CFT/CPF framework that, based on case study analysis, contributed to the ability of proliferation networks to conduct their activity. While U.S. financial institutions generally have a strong track record of compliance with U.S. and UN sanctions, these gaps can make those efforts less effective or more difficult to implement. Therefore, U.S. authorities have prioritized new legislation, regulations (including recent rulemaking), and guidance to address or mitigate these gaps.

Beneficial Ownership. Proliferation networks routinely create legal entities to obfuscate financial activity linked to states of proliferation concern. Domestically, since the Customer Due Diligence Rule became applicable in May 2018, the United States has required financial institutions to identify and verify the identity of the beneficial owners of companies opening accounts, and this BOI has been available to law enforcement agencies as appropriate. The United States, however, has not required companies formed or doing business in the United States to report BOI to the U.S. government. The CTA, enacted as part of the Anti-Money Laundering Act of 2020, established a legal framework for the U.S. government to require the reporting of BOI directly to FinCEN.

Specifically, the CTA requires certain U.S. and foreign companies registered to do business in the United States to disclose BOI to FinCEN. The CTA also requires FinCEN to build a secure, non-public

---


45 This would be outside of what is collected under FinCEN’s CDD rule by financial institutions, such as banks and broker-dealers. https://www.fincen.gov/resources/statutes-and-regulations/cdd-final-rule#:~:text=The%20CDD%20Rule%20requires%20these,Rule%20has%20four%20core%20requirements.
database to store the BOI and to disclose reported BOI to authorized government authorities and financial institutions subject to safeguards and controls. Pursuant to the final BOI Reporting Rule, implementing the reporting requirements of the CTA and effective January 1, 2024, FinCEN began accepting BOI. In parallel, in December 2023, FinCEN issued a final BOI Access Rule to establish who may request and receive BOI, how recipients may use it, and how they must secure it. This rule becomes effective on February 20, 2024. Considering the impact of the CTA, future risk assessments will continue to monitor the ability of proliferation networks to create legal entities in the United States considering the impact of the CTA.

Compounding the absence of a BOI reporting framework in the United States prior to January 1, 2024, the lack of effective implementation of the FATF standard related to beneficial ownership transparency for legal entities on a worldwide basis exacerbates PF risk as the inability of some jurisdictions to share this information naturally hinders cross-border investigations. According to the FATF’s Report on the State of Effectiveness and Compliance with the FATF Standards, only slightly more than half of countries have the necessary laws and regulations to understand, assess the risks of, and verify the beneficial owners or controllers of companies. Even fewer—9%—meet the effectiveness requirements of the relevant Immediate Outcome.

Virtual Assets. PF networks often seek to exploit the lack of effective implementation of AML/CFT/CPF measures for illicit finance through virtual assets across jurisdictions. Uneven (and often inadequate) regulation and supervision internationally allow VASPs and illicit actors to engage in regulatory arbitrage, which could potentially expose the U.S. financial system to VASPs with deficient or nonexistent AML/CFT/CPF controls operating abroad. Based on FATF assessments, jurisdictions are making limited progress (73 out of 98 jurisdictions rated as only partially or not compliant), and a FATF-administered survey found that many jurisdictions had not taken basic steps to assess risk or determine an approach to virtual assets.

While VASPs in the United States are subject to AML/CFT/CPF and sanctions obligations, there are cases in which VASPs fail to comply with them. In some cases, VASPs may not implement AML/CFT/CPF controls or other processes to identify customers, enabling misuse by illicit actors, including PF networks. Additionally, VASPs may perceive that they are not subject to U.S. regulatory requirements for AML/CFT/CPF based on their geographic location or the services they provide. As demonstrated by recent enforcement actions, including those referenced in the case studies section below and in the National Money Laundering Risk Assessment, some firms do not adopt AML/CFT/CPF programs to adequately mitigate risks within the sector.

The United States also recognizes the risks posed by the extensive use of CVC mixing services by a variety of illicit actors throughout the world. In October 2023, FinCEN issued a notice of proposed rulemaking (NPRM) pursuant to section 311 of the USA PATRIOT Act that identifies international convertible virtual currency mixing (CVC mixing) as a class of transactions of primary money laundering concern.

---


FinCEN identified CVC mixing as a primary money laundering concern in part for its use to launder proceeds of large-scale CVC theft and heists and support the proliferation of WMD, in particular, by the DPRK. FinCEN’s proposal would require covered financial institutions to implement certain recordkeeping and reporting requirements on transactions that covered financial institutions know, suspect, or have reason to suspect involve CVC mixing within the United States or jurisdictions outside of it.

### Case Studies

The NPFRA, like the risk assessments for money laundering and terrorist financing, relies on a case study approach to describe the intersection of threats and vulnerabilities. This case studies section is divided into two parts.

Part One describes activities that fit traditional PF typologies, where networks seek to acquire goods or raise revenue by exploiting financial institutions and products generally used in global commerce – such as open account wire transfers, where banks will process the transactions between two parties involved in the buying/selling of goods but otherwise will not have access to supporting documentation describing, for example, the nature and purpose of the transaction or the underlying goods or services changing hands. A critical component of these methods is the utilization of the maritime sector to facilitate the illicit movement of proliferation-sensitive goods or natural resources trade in violation of UN or U.S. sanctions.

Part Two describes cyber-enabled proliferation financing, the digital revenue-raising model that previous risk assessments have also documented but that we describe more prominently here. In these cases, networks affiliated with states of proliferation concern use cyber capabilities, such as cyber-enabled theft or ransomware attacks, to raise and move money by conducting attacks on financial institutions, including VASPs. In the case of the DPRK, these activities are complemented by information technology (IT) workers who use fraudulent means to conceal their identities and contract out their services on digital platforms, earning income that would otherwise be legitimate if it were not for the underlying fraud and violations of DPRK-related sanctions.

---


Part One: The “traditional” procurement and revenue-raising model

This part presents case studies of the “traditional” procurement and revenue-raising model, which is characterized by efforts of PF networks to mimic legitimate commercial trade.\(^{52}\) The 2022 NPFRA presented this activity in a series of case studies on (1) misuse of legal entities and (2) exploitation of the maritime sector. Based on private sector feedback on the overlap of this activity in PF schemes, those two sections are combined in this assessment.

To disguise their activity as legitimate commerce, proliferation networks leverage corporate entities to gain access to financial services, including correspondent banking. While specific typologies will vary across networks, PF networks often create multiple front or shell companies in the United States and third-country jurisdictions. Once they create that financial structure, these networks will also exploit the maritime sector to either transport goods needed for a state’s proliferation efforts or to move commodities that generate revenue for such a program (as in the cases of the DPRK, Iran, and Russia, especially considering the G7+ imposed price cap).\(^{53}\)

Recent U.S. guidance and alerts, with typologies, red flags, and case studies, have informed this assessment. In November 2023, FinCEN and the Department of Commerce’s Bureau of Industry and Security released a Joint Notice on the global evasion of U.S. export controls.\(^{54}\) The Joint Notice provided an overview of how financial institutions, including those involved in the maritime sector and other entities conducting business with U.S. persons or U.S.-origin goods, should exercise vigilance against the financing of illicit procurement. Additionally, in December 2023, the Departments of Commerce, the Treasury, Justice, State, and Homeland Security released a Quint-Seal Compliance Note on “Know Your Cargo” best practices in the maritime sector.\(^{55}\) The Compliance Note offers potential indicators of sanctions and export control evasion and encourages transportation companies, maintenance companies, insurance providers, financial institutions, and other entities involved in cargo transport to adopt appropriate compliance measures to guard against deceptive practices, including those mentioned in the case studies below.

\(^{52}\) For additional context see p. 17 of the 2022 NPFRA.
\(^{55}\) Department of Commerce, Department of the Treasury, Department of Justice, Department of State, and Department of Homeland Security, “Quint-Seal Compliance Note: Know Your Cargo: Reinforcing Best Practices to Ensure the Safe and Compliant Transport of Goods in Maritime and Other Forms of Transportation,” (December 11, 2023), [https://ofac.treasury.gov/media/932391/download?inline](https://ofac.treasury.gov/media/932391/download?inline).
Russian Federation

**November 2023 Russian Illicit Procurement Scheme**

**Criminal Prosecution**

In November 2023, the Department of Justice (DOJ) announced the unsealing of an indictment and criminal complaint outlining charges in two separate criminal conspiracies related to the unlawful export of dual-use technologies to Russia.

According to court documents, a Brooklyn, New York resident and two Canadian nationals were charged in a sanctions evasion and export control scheme. The defendants used two corporate entities registered in Brooklyn to facilitate the scheme and unlawfully source, purchase, and ship millions of dollars’ worth of dual-use electronics from U.S. manufacturers to sanctioned end-users in Russia. Two of the defendants allegedly purchased electronic components from U.S. manufacturers and distributors under the auspices of the two companies and arranged for the items to be sent to various locations in Brooklyn. They then unlawfully shipped the items to a variety of intermediary corporations located in other countries, including Türkiye, Hong Kong, India, China, and the UAE, where they were rerouted to Russia.

Separately, two individuals from St. Petersburg, Russia; and one individual from Brooklyn were charged with conspiracy and other offenses related to an export control scheme to benefit companies affiliated with the Russian military, including SMT-iLogic, a sanctioned Russian entity that has been identified as part of the supply chain for producing Russian military drones used in Russia’s war against Ukraine. The defendants allegedly used a corporate entity to facilitate their illegal export control scheme. According to court documents, between October 22, 2021, and February 22, 2022, corporate accounts controlled by one of the individuals allegedly received wire transactions from iLogic totaling approximately $273,000. These funds were then allegedly used almost entirely to make payments to a Brooklyn-based electronics distributor or to pay that individual’s credit cards, which he used to buy goods from the Brooklyn-based company.

**December 2022 Russian Illicit Procurement Scheme**

**Criminal Prosecution**

In December 2022, DOJ unsealed a 16-count indictment charging two U.S. nationals and five Russian nationals—including a suspected Federal Security Service officer—with conspiracy and other charges related to a global procurement and money laundering scheme on behalf of the Russian government in which the defendants allegedly conspired to obtain military-grade and dual-use technologies from U.S. companies. According to the indictment, these items included ammunition and the transfer of highly sensitive and heavily regulated electronic components, some of which can be used in the development of nuclear and hypersonic weapons, quantum computing, and other military applications. At the center of the procurement network was Serniya Engineering, a Moscow-based firm.

---

that was already subject to U.S. sanctions and placed on Commerce’s Entity List for acting on behalf of Russian defense and intelligence entities.

According to the indictment, the five individuals allegedly unlawfully purchased and exported highly sensitive and heavily regulated electronic components to Russia. To execute the scheme, the co-defendants allegedly created shell companies and associated bank accounts in the New York City area to route shipments and layer financial transactions. The U.S.-based co-defendants would then allegedly fabricate shipping documents and invoices, repackaging and reshipping items to intermediate destinations around the world before their ultimate arrival in Russia. According to the indictment, common transshipment points included Estonia, among other jurisdictions. Payments were also layered, with money being transferred to accounts in the names of shell companies held at different banks in jurisdictions throughout the world.

**May 2023 Russian Illicit Procurement Scheme**

**Criminal Prosecution**

In May 2023, the DOJ unsealed a criminal complaint charging a Greek national with wire fraud conspiracy and smuggling. The defendant was head of a collection of defense and technology companies in the Netherlands and Greece. According to the complaint, since 2017 this individual had allegedly been involved in smuggling U.S.-origin military and dual-use technologies to Russia in violation of U.S. law. These highly regulated and sensitive components allegedly included advanced electronics and sophisticated testing equipment used in military applications, including quantum cryptography and nuclear weapons testing, as well as tactical battlefield equipment. As described in the complaint, the Russian end-users allegedly included Russian intelligence and military research and development entities.

As alleged, the defendant conspired with a network of companies orchestrated by the Russian intelligence services to fraudulently acquire and then smuggle U.S.-origin military and dual-use technologies to aid the Russian defense and security sectors, by procuring sensitive equipment meeting NATO specifications designed for tactical battlefield conditions as well as components with applications in space-based and cryptographic communications.

To further this illicit procurement scheme, the defendant allegedly signed false end-use statements and provided them to U.S. companies, certifying that the individual’s company was the end user of the requested items, and that the goods would not be reexported elsewhere or used for weapons development.

---


Criminal Prosecution

In December 2023, DOJ unsealed an indictment charging an Iranian national and a PRC national with a scheme to procure U.S.-manufactured dual-use microelectronics for the IRGC’s UAV program. OFAC also sanctioned the Iranian national, as well as related individuals and entities based in Iran, Malaysia, Hong Kong, and Indonesia for their participation in the procurement network. The PRC national had been designated in October 2023.

According to the DOJ press release, the defendants allegedly used a web of foreign front companies to illegally purchase and export from the United States to Iran dual-use microelectronics that are commonly used in UAV production, including high electron mobility transistors, monolithic microwave integrated circuit power amplifiers, and analog-to-digital converters. To effect this scheme, the defendants allegedly used the foreign companies to obfuscate the end-destination for the goods. For example, between June and September 2015, they caused an unwitting French company to purchase from a U.S. company several pieces of analog-to-digital converters with applications in wireless and broadband communications, radar and satellite subsystems, multicharrier, multimodal cellular receivers, antenna array positioning and infrared imaging. The PRC national then caused a division of the French company to ship the analog-to-digital converters to Hong Kong, where they were reexported to Iran.

United States v. Behrouz Mokhtari

Criminal Prosecution

In July 2023, Behrouz Mokhtari was sentenced to 41 months in prison followed by three years of supervised release after pleading guilty to violating U.S. sanctions against Iran. According to his plea, Mokhtari used his management positions and/or maintained ownership control over multiple businesses in Iran and the UAE. He used this network of businesses to illegally provide services to Iranian entities, such as the refinement and transport of petrochemical products. Mokhtari and his co-conspirators used the network’s bank accounts in the UAE to process these U.S. dollar transactions.

In a separate conspiracy lasting from about February 2013 until at least June 2017, Mokhtari and a number of Iranian nationals agreed to conduct illicit shipments of petrochemical products to and from Iran, utilizing his front company, East & West Shipping Inc., in Panama to do so.

In furtherance of the scheme, Mokhtari created a Panama-based front company, East & West Shipping Inc., to purchase two liquid petroleum gas (LPG) tanker vessels to transport Iranian petrochemical

---

products in international commerce on behalf of, and to benefit, Iranian entities associated with the Government of Iran. Mokhtari arranged for the sale of one of the vessels to be scrapped, with the funds sent to two bank accounts controlled by Mokhtari. Mokhtari ultimately used some of the proceeds to purchase a home in California.63

Mokhtari was ordered to forfeit approximately $2,862,598 in proceeds derived from his criminal activity as well as a residence he purchased in Campbell, California, for over $1.5 million using such proceeds.64

*United States vs. Saber Fakih*65

**Criminal Prosecution**

In January 2022, an individual who had been based in the United Kingdom, Saber Fakih, pleaded guilty to violations of IEEPA and the Iranian Transactions and Sanctions Regulations arising from a scheme to export an Industrial Microwave System (IMS) and counter-drone system to Iran without having obtained an OFAC license.

According to Fakih’s Statement of Offense, he agreed to provide to an Iranian national with an IMS system from an unnamed U.S. company. Saber Fakih acted as an intermediary to mask the Iranian national’s role in the scheme. That individual then arranged for money to purchase the IMS to be deposited into an account in the UAE, which was then sent in three wires through the United States to an individual in Canada, and then ultimately to the U.S. manufacturer. Based on instructions from his co-conspirators, Fakih misrepresented to the manufacturer that the IMS was destined for an end-user in Dubai, UAE.

*May 2023 Iranian Ballistic Missile Procurement*  

**Criminal Prosecution**

In May 2023, the United States announced the indictment of a PRC national associated with Li Fangwei (a.k.a. Karl Lee)66 charging the individual with sanctions evasion, money laundering, and bank fraud offenses based on his alleged participation in a scheme to use Sinotech Dalian Carbon and Graphite Manufacturing Corporation (Sinotech Dalian), an OFAC-designated entity, to provide materials used in the production of weapons of mass destruction, specifically ballistic missile components, for Iran’s program.

According to charging documents, between at least March 2019 and September 2022, the individual allegedly participated in a scheme to use Sinotech Dalian, including through transactions involving the U.S. financial system, to supply isostatic graphite, which is used in the manufacture of rocket nozzles and reentry vehicle nose tips in ICBMs, to Iranian entities. To obfuscate Sinotech Dalian’s role in this alleged scheme, the defendant allegedly created a bank account in the name of a front company, which received two transfers from a U.S. bank totaling over $15,000.

63 Plea agreement, p. 5.
66 For more information on Karl Lee, see the 2018 NPFRA, p. 21.
Multiple Jurisdictions

*Toll Holdings*

Enforcement Action

In April 2022, OFAC entered a settlement agreement with Toll Holdings, an Australia-headquartered international freight forwarding and logistics company for apparent violations of multiple sanctions programs, including processing transactions involving the DRPK, Iran, and Syria. Toll Holdings caused nearly 3,000 payments through itself, its affiliates, providers, or suppliers to be processed by U.S. financial institutions for the benefit of sanctioned individuals or entities, or for the benefit of individuals or entities located in sanctioned jurisdictions. Toll’s compliance function did not have policies and controls in place commensurate with the complexity of its operations, which included almost 600 invoicing, data, payment, and other system applications spread across its various business units.

According to the enforcement action, after one of Toll’s banks raised concerns over Toll’s compliance with U.S. sanctions, Toll tried to mitigate their risk exposure by ceasing all business with U.S.-sanctioned countries as of June 2016. However, Toll did not implement the compliance policies and procedures necessary to prevent payments involving sanctioned persons, nor did it test whether shipments involved persons located in U.S.-sanctioned countries. It was not until February 2017 that Toll introduced additional controls to finally prevent shipments to or from sanctioned countries.

*MidFirst Bank*

Enforcement Action

In July 2022, OFAC issued a finding of violation to MidFirst Bank for violations of the Weapons of Mass Destruction Proliferators Sanctions Regulations. MidFirst Bank maintained accounts and allowed 34 payments involving two individuals to be processed for 14 days after they had been added to OFAC’s List of Specially Designated Nationals and Blocked Persons (the SDN List).

According to the Finding of Violation, MidFirst Bank staff misunderstood how their third-party vendor software handled screening the entirety of their customer database against the SDN List. The third-party vendor would screen the customer database once a month, and only do daily screenings for new customers, or existing customers who made certain changes to their account information (e.g., change of address).

---


Part Two: Cyber-Enabled Proliferation Financing: The “new” digital evasion model

As described earlier in the NPFRA, the DPRK continues to advance its illicit exploitation of new financial technology, including virtual assets to raise and move money. The 2018 and 2022 NPFRA noted how the DPRK used, stole, and laundered virtual assets to fund its illicit weapons programs, and that activity has accelerated during the review period. According to U.S. government-issued advisories, DPRK cyber actors target a variety of organizations in the blockchain technology and virtual asset industry, including virtual asset exchanges, decentralized finance (DeFi) protocols, blockchain bridge developers, virtual asset trading companies, venture capital funds investing in virtual assets, and individual holders of large amounts of virtual assets or non-fungible tokens (NFTs). They also seek to exploit CVC mixing activities.

The DPRK has also developed an additional revenue stream by deploying IT workers. According to May 2022 Treasury, State, and FBI-issued guidance, the DPRK has dispatched thousands of highly skilled IT workers around the world (located primarily in Russia and the PRC) to generate revenue that contributes to its WMD and ballistic missile programs. These IT workers take advantage of existing demands for specific IT skills, such as software and mobile application development, to obtain freelance employment contracts from clients around the world, including in North America, Europe, and East Asia. In many cases, DPRK IT workers represent themselves as U.S.-based and/or non-North Korean teleworkers. The workers may further obfuscate their identities and/or location by subcontracting work to non-North Koreans.

---

69 For enforcement actions involving VASPs with significant compliance deficiencies Treasury can conclude that if ordinary residents of comprehensively sanctioned jurisdictions like DPRK and Iran can access these platforms, governmental entities in those countries can and, in some cases based on reporting from other sources, do use them to move assets. This is directly applicable in the virtual asset context, as cybercriminals associated with both governments have conducted ransomware attacks, almost certainly demanding virtual assets as payment, and DPRK cybercriminals have stolen hundreds of millions of dollars’ worth of virtual assets.


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


Maui ransomware

Civil asset forfeiture complaint

In July 2022, based on victim reporting from a Kansas medical center that was the victim of a never-before-seen ransomware variant, the DOJ announced a complaint to forfeit seized virtual assets paid as ransom to DPRK hackers or otherwise used to launder such ransom payments. In May 2022, the FBI filed a sealed seizing warrant for virtual assets, which was then worth approximately $500,000 and hosted in the exchange accounts of PRC-based money launderers. A portion of the seized funds included virtual assets paid by the Kansas medical center, another health care provider in Colorado, and other victims in the United States and abroad.

Also in July 2022, the FBI, the Cybersecurity and Infrastructure Security Agency (CISA), and the Department of the Treasury released a joint Cybersecurity Advisory to provide technical details on the Maui ransomware and provided recommended mitigation measures for those entities likely to be targeted to protect their critical infrastructure.

April 2023 DPRK Money Laundering

Criminal Prosecution

In April 2023, the DOJ unsealed two indictments charging a DPRK FTB representative for his role in money laundering conspiracies designed to generate revenue for the DPRK using virtual assets. The individual allegedly conspired with two over-the-counter traders to launder stolen virtual assets and used funds to purchase goods on behalf of the DPRK government in U.S. dollars via Hong Kong-based front companies.

The individual was separately charged with a conspiracy involving various North Korean IT workers to launder the proceeds of illegal IT development work. These IT workers used fake personas to get jobs, including jobs at U.S. blockchain development companies. The workers asked to be paid in virtual assets, such as stablecoins, like USD Tether and USD Coin, which are pegged to the U.S. dollar. After receiving payment, the workers funneled their earnings back to North Korea through the FTB representative.

DPRK IT Workers Seizure

Civil asset forfeiture complaint

In October 2023, under a court order issued in the Eastern District of Missouri, the DOJ seized 17 website domains used by DPRK IT workers in a scheme to defraud U.S. and foreign businesses, evade sanctions, and fund the development of the DPRK government’s weapons program.

---


As alleged in court documents, the DPRK dispatched thousands of skilled IT workers to live abroad, primarily in China and Russia. Once established, they acted to deceive U.S. and other businesses worldwide into hiring them as freelance IT workers. These workers used pseudonymous email, social media, payment platform and online job site accounts, as well as false websites, proxy computers located in the United States and elsewhere, and witting and unwitting third parties to generate millions of dollars a year on behalf of designated entities directly involved in the DPRK’s UN-prohibited WMD programs.

Certain DPRK IT workers designed the 17 seized website domains to appear as domains of legitimate, U.S.-based IT services companies, thereby helping the IT workers hide their true identities and location when applying online to do remote work for U.S. and other businesses worldwide. In reality, this specific group of DPRK IT workers, who worked for the PRC-based Yanbian Silverstar Network Technology Co. Ltd. and the Russia-based Volasys Silver Star, had previously been sanctioned in 2018 by Treasury.77

Coinciding with the announced website seizures, the DOJ also announced: (i) the court-authorized seizure of approximately $1.5 million in revenue from the IT Workers’ criminal scheme; and (ii) a partnership with the Republic of Korea and U.S.-based online freelance work and payment service platforms, which resulted in the shutdown of thousands of the IT Workers’ fraudulent accounts on those platforms.

Multiple Jurisdictions

Sinbad.io Mixer

Designation78

In November 2023, OFAC designated Sinbad.io (Sinbad), a virtual asset mixer that served as a key money-laundering tool for the Lazarus Group, a DPRK-sponsored hacking group. According to the OFAC press release, Sinbad processed millions of dollars’ worth of virtual assets that the Lazarus Group had stolen, including through the high-profile heists from Horizon Bridge, Axie Infinity, and Atomic Wallet. As with illicit mixers like Blender.io, which some industry experts believe to be a predecessor mixer, Sinbad operated on the Bitcoin blockchain and indiscriminately facilitated illegal transactions by obfuscating their origin, destination, and counterparties.

August 2023 Tornado Cash Mixer

Criminal Prosecution

In August 2023, the DOJ unsealed an indictment charging a Russian national and a Washington man with creating, operating, and promoting Tornado Cash, a virtual asset mixer that allegedly facilitated more than $1 billion in money laundering transactions, and laundered hundreds of millions of dollars for the Lazarus Group, the sanctioned North Korean cybercrime organization. The Tornado Cash service allegedly advertised to customers that it provided untraceable and anonymous financial transactions, and the defendants allegedly chose not to implement know-your-customer or AML programs as required by law. Even after Treasury designated Tornado Cash in August 2022, the two individuals allegedly helped the Lazarus Group to transfer criminal proceeds from a virtual asset wallet that had been designated by OFAC as blocked property. Each individual is charged with one count of

conspiracy to commit money laundering, one count of conspiracy to operate an unlicensed money transmitting business, and one count of conspiracy to violate the International Economic Emergency Powers Act.

**Bittrex**

**Enforcement Action**

In October 2022, OFAC settled with Bittrex, Inc., a Washington-based online virtual asset exchange and hosted wallet service for over $24 million for apparent violations of multiple sanctions programs. FinCEN separately settled with Bittrex for $29 million for willful violations of the BSA's AML and suspicious activity report (SAR) reporting requirements. This was the first joint enforcement action undertaken by OFAC and FinCEN against a VASP.

According to the OFAC enforcement action, Bittrex did not maintain any internal controls that would have prevented customers resident in sanctioned jurisdictions including the Russian-occupied Crimea region of Ukraine, Cuba, Iran, Sudan, and Syria from accessing its platform. For example, Bittrex did not screen for Internet Protocol addresses, which would have shown customers transacting on its platform from these jurisdictions. Neither did it use information the customers themselves provided—such as physical addresses or passport information—that would have confirmed their presence in a sanctioned jurisdiction. Finally, Bittrex retained a third-party vendor who screened transactions for hits against OFAC’s SDN list and other lists but did not scrutinize customers or transactions for a nexus to sanctioned jurisdictions.

According to the FinCEN consent order, in addition to Bittrex's sanctions compliance deficiencies, the company failed to maintain an effective AML program. Despite a significantly high transaction volume, Bittrex assigned two employees to manually review transactions for suspicious activity. The result was that Bittrex did not file a single SAR between 2014 and May 2017. The hiring of additional employees generated only one SAR between May 2017 and November 2017. Among other types of suspicious activity, Bittrex failed to identify transactions with darknet marketplaces like AlphaBay, Agora, and Silk Road 2, and did not report transactions connected to ransomware attacks. Finally, Bittrex failed to fully address the risks from certain anonymity-enhanced virtual assets.

**Binance**

**Criminal Prosecution; Enforcement Actions**

In November 2023, Binance Holdings Limited pleaded guilty and agreed to pay more than $4 billion to resolve DOJ’s investigation into violations related to the BSA, failure to register as a money transmitting business, and violations of IEEPA. Binance’s founder and chief executive officer, Changpeng Zhao, pleaded guilty to failing to maintain an effective AML program, in violation of

---

the BSA. As part of the plea agreement, Zhao resigned as CEO. Binance’s guilty plea was part of coordinated resolutions with FinCEN, OFAC, and the CFTC (as of this writing the SEC has pending charges against Binance). As part of the agreement, in addition to the monetary penalties, Binance agreed to retain an independent compliance monitor for three years and remediate and enhance its AML and sanctions compliance programs.

As noted in FinCEN’s consent order and other related documents, due in part to Binance’s failure to implement an effective AML program, illicit actors used Binance’s exchange in various ways, including conducting transactions that obfuscated the source and ownership of virtual assets; transferring illicit proceeds from ransomware variants; and moving proceeds of darknet market transactions, exchange hacks, and various internet-related scams.

As also noted in FinCEN’s consent order and other related documents, Binance also knew that U.S. sanctions laws prohibited U.S. persons—including its U.S. customers—from trading with its customers subject to U.S. sanctions, including customers in comprehensively sanctioned jurisdictions, such as Iran. Binance knew that it had a significant number of users from comprehensively sanctioned jurisdictions and a substantial number of U.S. users and that its matching engine would necessarily cause U.S. users to transact with users in sanctioned jurisdictions in violation of U.S. law. Nonetheless, Binance did not implement controls that would prevent U.S. users from trading with users in sanctioned jurisdictions. Because of Binance’s internationally weak implementation of its controls, between January 2018 and May 2022, Binance willfully caused over $898 million in trades between U.S. users and users ordinarily resident in Iran.

Additionally, as noted in FinCEN’s consent order and other related documents, Binance users effected transactions with Iranian virtual asset exchanges without filing SARs: Binance user wallets effected a significant volume of direct transactions with various Iranian virtual asset exchanges, each worth more than $2,000, and in the aggregate worth the equivalent of over half a billion dollars. This total also includes several transactions with virtual asset wallets associated with sanctioned entities and individuals. No SARs were filed with FinCEN.

---


87 “Binance and CEO Plead Guilty to Federal Charges in $4B Resolution.”

Emerging Trends

The United States maintains a strong legislative and regulatory framework to counter PF in direct response to the complexity of the proliferation threats and vulnerabilities discussed in this and prior NPFRAs. WMD proliferators and their procurement networks will continue to target the U.S. for its dual-use technology and will use a mix of existing and emerging trends to purchase and export such technology and goods. WMD state actors will also continue to target U.S. companies and individuals to raise revenue illicitly to support their programs. Russia's need for military components to support its war in Ukraine sets a new stage in its relationship with the DPRK, accelerating PF threats. Other trends referenced below include the search for alternatives to reliance on the U.S. dollar for global trade and new technologies that may pose a proliferation risk. The United States will continue to target PF sanctions evaders and procurement networks, seeking new tools and skills as necessary as will be described in our policy response in the Illicit Finance Strategy.

Sanctions Evasion and State Complicity

As documented in the 2022 NPFRA, a significant volume of evasion activity that PF networks engage in is enabled by countries ignoring their responsibilities under relevant UNSCRs, which undermines the tenets of global arms control through the lack of effective implementation of international sanctions and export control requirements, or the broader measures required to prevent proliferation to non-state actors under UNSCR 1540). The United States has previously publicly stated that Russia and the PRC have failed to hold the DPRK accountable for its multiple violations of UNSCRs related to ballistic missile testing. The review period saw persistent efforts by the Russian Federation to engage in bilateral arms deals with Iran and DPRK, which the United States assesses are violations of UN and/or U.S. sanctions. In the case of the DPRK, where the arms embargo is a cornerstone of the UN sanctions regime, the unwillingness of a permanent member of the Security Council to enforce undermines the credibility of international measures to restrict the DPRK’s development of WMD.

New & Alternative Payment Infrastructure

The Treasury and its interagency partners are studying the potential risks from new and alternative payment systems, as some countries seek to develop strategies to avoid U.S. jurisdiction and evade U.S. sanctions specifically. These systems include the growth of local currency settlement to avoid dollar-clearing, the growth of alternatives to the Society for Worldwide Interbank Financial Telecommunication (SWIFT) payment messaging system, or the development of a Central Bank Digital Currency (CBDC). In its report on the Future of Money and Payments, Treasury documented how bad actors could evade U.S. sanctions using foreign CBDCs or virtual assets, including stablecoins.


However, Treasury continues to assess that U.S. adversaries would find it difficult to translate those alternative payment systems into an at-scale replacement for U.S. global financial leadership and the strength of U.S. currency because these systems could not replicate the foundations of U.S. strength, including strong economic performance; sound macroeconomic policies and institutions; open, deep, and liquid financial markets; institutional transparency; commitment to a free-floating currency; and strong and predictable legal systems.  

**Emerging Technologies**

As described in the National Biodefense Strategy, advances in life sciences and biotechnology, while offering multiple benefits for public health, can also bring new security risks from potential intentional misuse that require mitigation. Big data, artificial intelligence, and genomic modification, to take some examples, represent potential new threats from state and non-state actors. Potential adversaries could also use the same biological and chemical science advancements created to develop life-saving medical countermeasures to develop new or enhanced agents. Technologies intended to reduce testing and production inefficiencies, such as biofoundries and additive manufacturing, create opportunities to reduce the development footprint and increase the number of proliferation pathways available to malign actors. The United States will remain vigilant of such misuse and whether illicit actors could misuse the U.S. financial system to develop or deploy these capabilities. It will also support the efforts of multilateral and international organizations to advance work in this area.

**Conclusion**

Over the review period, the United States faced evolving efforts from PF networks associated with previously acknowledged states of proliferation concern. Two states in particular, Russia and the DPRK, presented a significantly higher threat. Russia’s ongoing illegal war in Ukraine has accelerated that country’s illicit procurement, including components produced in the United States. The DPRK has leveraged its significant malicious cyber activity capabilities and its deployment of fraudulent IT workers to raise revenue.

Some vulnerabilities persisted from the two prior NPFRAs, including the size of the U.S. financial system, the centrality of the U.S. dollar in global trade, and the role of U.S. manufacturers in the production of military and proliferation-related technology (including dual-use items) continue to make the United States a target of exploitation by PF networks. These structural vulnerabilities are mitigated to a significant extent by a strong culture of compliance with U.S. law by U.S. financial institutions and other private sector actors, though some gaps remain. Specifically, over the review period, the United States worked to finalize the implementation of the CTA. The full implementation of the CTA will help facilitate law enforcement investigations and make it more difficult for illicit actors to hide behind anonymous shell companies created in the United States or foreign entities registered to do business in the United States. The varying levels of AML/CFT/CPF controls for the virtual asset sector globally and some

---

92 Ibid., p. 34.
compliance deficiencies with U.S. VASPs made the United States vulnerable to PF networks.

In response to these vulnerabilities, the United States will continue to explore avenues to improve its AML/CFT/CPF regime. As documented in this NFPRA, the U.S. government has made significant progress on closing loopholes in the collection of BOI information through implementing the CTA, working domestically and through the FATF to improve AML/CFT/CPF compliance within the virtual asset sector, and communicating red flags and typologies associated with illicit procurement efforts through alerts and advisories.

Given the devastating consequences to international peace and security that would arise from the use of a WMD, the United States will continue to identify additional measures to strengthen the U.S. CPF regime.
Participants

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

- **Department of Commerce**
  - Bureau of Industry and Security (BIS)

- **Department of Defense (DOD)**
  - Office of the Under Secretary of Defense for Policy

- **Department of Energy**
  - National Nuclear Security Administration

- **Department of Homeland Security**
  - Countering Weapons of Mass Destruction/Strategy, Plans & Policy
  - Homeland Security Investigations

- **Department of Justice (DOJ)**
  - Criminal Division
  - Federal Bureau of Investigation (FBI)
  - National Security Division

- **Department of State**
  - Bureau of Economic and Business Affairs
  - Bureau of International Security and Nonproliferation

- **Department of the Treasury**
  - Financial Crimes Enforcement Network (FinCEN)
  - Office of Foreign Assets Control (OFAC)
  - Office of Intelligence and Analysis (OIA)
  - Office of Terrorist Financing and Financial Crimes

- **Staff of the Federal Functional Regulators**\(^95\)

---

\(^95\) This includes staff of the Commodity Futures Trading Commission (CFTC), the Federal Deposit Insurance Corporation, the Board of Governors of the Federal Reserve System, the National Credit Union Administration, the Office of the Comptroller of the Currency, and the Securities and Exchange Commission.
Scope & Definition

The United States continues to scope the NPFRA based on the FATF’s definition from its 2021 guidance on conducting PF risk assessments, where proliferation finance is defined as:

raising, moving, or making available funds, other assets or economic resources, or financing, in whole or in part, to persons or entities for purposes of WMD proliferation, including the proliferation of their means of delivery or related material (including both dual-use technologies and dual-use goods for non-legitimate purposes).\(^{96}\)

In U.S. law, a WMD is defined as:

(A) any destructive device as defined in section 921 of 18 U.S.C. § 921;
(B) any weapon that is designed or intended to cause death or serious bodily injury through the release, dissemination, or impact of toxic or poisonous chemicals, or their precursors;
(C) any weapon involving a biological agent, toxin, or vector (as those terms are defined in section 178 of 18 U.S.C. § 178); or
(D) any weapon that is designed to release radiation or radioactivity at a level dangerous to human life;

As described further in the Vulnerabilities section, the NPFRA focuses exclusively on how proliferation networks working on behalf of nation-states exploit the U.S. financial system. This definition scopes in activities that the United States considers:

(1) illicit procurement, meaning the attempt to directly acquire goods, technology, or know-how as an input into a WMD program; as well as
(2) more indirect types of PF, which can generally fall under the rubric of revenue generation activity where proliferation networks, often operating on behalf or at the direction of states under comprehensive United Nations and U.S. sanctions, engage in illicit financial activity that generates proceeds that, in turn, support, directly or indirectly,\(^{97}\) WMD activities. Consequently, proliferation networks may commit offenses implicating U.S. anti-money laundering, sanctions, or export controls.

This assessment is not a global PF risk or threat assessment. U.S. financial institutions and other U.S. businesses and individuals operating in foreign jurisdictions should complement their consultation of this risk assessment with other resources those jurisdictions may provide (including the jurisdiction's own risk or threat assessments, guidance, and all relevant law and regulations governing AML/CFT/CPF).

---

\(^{96}\) FATF PF Risk Assessment Guidance, p.8, footnote 7.

\(^{97}\) As described in the case studies, in some cases individuals and entities may operate a couple of steps removed from those who are designated.
Methodology

The 2024 NFPRA follows the FATF methodology, where PF risk is a function of the following:

- **Threat**: A threat refers to individuals or entities, or activity undertaken by those individuals and entities, with the potential to cause harm. The threats, which may include nation-state authorities, those acting under their control or on their behalf, or those wittingly or unwittingly supporting either, are the ones who exploit the U.S. financial system to move funds, assets, or other economic resources that could be used to: (1) directly acquire WMDs, their delivery systems, or the goods, technology, or know-how to allow them to build WMDs or their delivery systems, or (2) support a WMD program through a variety of revenue-raising activities.

- **Vulnerability**: To acquire or expand their WMD capabilities, a threat actor must exploit aspects of a jurisdiction or a private sector entity to obtain components or financial services it would otherwise be prohibited from acquiring. These vulnerabilities may arise from weaknesses or loopholes in national laws or regulations, effectiveness issues impeding the ability of national authorities to properly investigate or disrupt proliferation networks, or unique circumstances that make a particular jurisdiction especially vulnerable to this kind of activity.

- **Consequence**: A consequence derives directly from a threat capitalizing on a vulnerability. In the context of PF, the consequence would be funds, assets, or other economic resources being made available to a proliferation network such that it can be used to acquire or augment a specific WMD capability.

- **Risk**: Risk is a function of threat, vulnerability, and consequence. It represents a summary judgment, considering the effect of mitigating measures, including regulation, supervision, and enforcement.

Further in line with the prior assessments, the NPFRA is based on a review of public and private sector publications, government datasets, and analyses. Data collected are current as of January 31, 2024. These sources include the following:

- A review of relevant Bank Secrecy Act (BSA) data collected by FinCEN that was potentially indicative of proliferation or sanctions evasion activity as seen by U.S. financial institutions as well as alerts and advisories derived from that data (see Appendix);

- U.S. sanctions designations and enforcement actions related to WMD activity (including evasion by proliferating entities or states);

---

98 The United States takes a broader view of PF risk than what the FATF Standards require and what the 2021 FATF PF Guidance conveys. That guidance restricts a consideration of threat, vulnerability, and consequence in the context of UN-targeted financial sanctions. The United States has a view of PF risk which includes both United Nations targeted financial sanctions and sectoral sanctions, as well as sanctions imposed under U.S. law, and restrictions imposed through U.S. export control authorities. FATF, PF Risk Assessment Guidance, p. 7, paragraph 11.

99 As with prior assessments, the authors consulted classified sources of information to verify conclusions reached through a consultation of information available in the public domain.

100 With respect to information collected from pending law enforcement cases, the charges in an indictment or similar charging documents are merely allegations. A defendant is presumed innocent until proven guilty beyond a reasonable doubt in a court of law. A seizure warrant is based on allegations. The government bears the burden of proving forfeitability in a civil forfeiture proceeding.

101 For more information on BSA data please see Department of the Treasury, FinCEN, “What is the BSA Data?,” [https://www.fincen.gov/what-bsa-data](https://www.fincen.gov/what-bsa-data).
• Export control violation cases, particularly where a financing element related to WMD was present or the item being procured was identified as being controlled for WMD or military end-use or end-user reasons;

• Publicly available law enforcement documentation relating to criminal cases arising from WMD procurement or sanctions evasion, including prosecutions of money laundering cases in which the specified unlawful activity violated the International Emergency Economic Powers Act (IEEPA) and related regulations or relevant export control laws;

• Civil and criminal asset forfeiture complaints related to property that had an alleged connection to WMD procurement or sanctions evasion; and

Reports and analyses prepared by international organizations, including the United Nations and the FATF, think tanks, academic and research organizations, and media reporting.
<table>
<thead>
<tr>
<th>Acronym</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>BOI</td>
<td>Beneficial Ownership Information</td>
</tr>
<tr>
<td>CBDC</td>
<td>Central Bank Digital Currency</td>
</tr>
<tr>
<td>CISA</td>
<td>Cybersecurity and Infrastructure Security Agency</td>
</tr>
<tr>
<td>CTA</td>
<td>Corporate Transparency Act of 2021</td>
</tr>
<tr>
<td>CVC</td>
<td>Convertible Virtual Currency</td>
</tr>
<tr>
<td>DNI</td>
<td>Director of National Intelligence</td>
</tr>
<tr>
<td>DOD</td>
<td>Department of Defense</td>
</tr>
<tr>
<td>DPRK</td>
<td>Democratic People's Republic of Korea</td>
</tr>
<tr>
<td>FATF</td>
<td>Financial Action Task Force</td>
</tr>
<tr>
<td>IAEA</td>
<td>International Atomic Energy Agency</td>
</tr>
<tr>
<td>ICBM</td>
<td>Intercontinental Ballistic Missile</td>
</tr>
<tr>
<td>IEEPA</td>
<td>International Emergency Economic Powers Act</td>
</tr>
<tr>
<td>IMS</td>
<td>Industrial Microwave System</td>
</tr>
<tr>
<td>IRGC</td>
<td>Islamic Revolutionary Guard Corps</td>
</tr>
<tr>
<td>IT</td>
<td>Information Technology</td>
</tr>
<tr>
<td>NSM</td>
<td>National Security Memorandum</td>
</tr>
<tr>
<td>OFAC</td>
<td>Office of Foreign Assets Control</td>
</tr>
<tr>
<td>PF</td>
<td>Proliferation Finance</td>
</tr>
<tr>
<td>PRC</td>
<td>People's Republic of China</td>
</tr>
<tr>
<td>RGB</td>
<td>Reconnaissance General Bureau</td>
</tr>
<tr>
<td>SAR</td>
<td>Suspicious Activity Report</td>
</tr>
<tr>
<td>SDN</td>
<td>Specially Designated National</td>
</tr>
<tr>
<td>SWIFT</td>
<td>Society for Worldwide Interbank Financial Telecommunication</td>
</tr>
<tr>
<td>UAE</td>
<td>United Arab Emirates</td>
</tr>
<tr>
<td>UAVs</td>
<td>Unmanned Aerial Vehicles</td>
</tr>
<tr>
<td>UNSCRs</td>
<td>United Nations Security Council Resolutions</td>
</tr>
<tr>
<td>VASP</td>
<td>Virtual Asset Service Providers</td>
</tr>
<tr>
<td>WMD</td>
<td>Weapon of Mass Destruction</td>
</tr>
</tbody>
</table>
Appendix: Recent Guidance/Alert/Advisory Documents


March 2022 – FinCEN Advises Increased Vigilance for Potential Russian Sanctions Evasion Attempts
