Financial Crimes Enforcement Network
U.S. Department of the Treasury

Anti-Money Laundering and Countering the Financing of Terrorism National Priorities

June 30, 2021

The Financial Crimes Enforcement Network (FinCEN),[1] after consulting with the U.S. Department of the Treasury's (Treasury's) Offices of Terrorist Financing and Financial Crimes, Foreign Assets Control (OFAC), and Intelligence and Analysis, as well as the Attorney General, Federal functional regulators,[2] relevant state financial regulators, and relevant law enforcement and national security agencies, is issuing these first government-wide priorities for anti-money laundering and countering the financing of terrorism (AML/CFT) policy (the "Priorities"). These Priorities are being issued pursuant to Section 5318(h)(4)(A) of the Bank Secrecy Act (BSA),[3] as amended by Section 6101(b)(2)(C) of the Anti-Money Laundering Act of 2020 (the "AML Act").[4] As required by Section 5318(h)(4)(C) of the BSA, the Priorities are consistent with Treasury's 2018 and 2020 National Strategy for Combating Terrorist and Other Illicit Financing (the "National Strategy").[5]

As explained in more detail below, the Priorities are, in no particular order: (1) corruption; (2) cybercrime, including relevant cybersecurity and virtual currency considerations; (3) foreign and domestic terrorist financing; (4) fraud; (5) transnational criminal organization activity; (6) drug trafficking organization activity; (7) human trafficking and human smuggling; and (8) proliferation financing. The establishment of these Priorities is intended to assist all covered institutions[6] in their efforts to meet their obligations under laws and regulations designed to combat money laundering and counter terrorist financing.

1. Congress has authorized the Secretary of the Treasury (the "Secretary") to administer the BSA. The Secretary has delegated to the Director of FinCEN the authority to implement, administer, and enforce compliance with the BSA and associated regulations. *See* Treasury Order 180–01 (January 14, 2020).
2. 31 U.S.C. § 5318(h)(4)(A) (as amended by AML Act § 6101(b)(2)(C)) uses the term Federal functional regulator "as defined in section 509 of the Gramm-Leach-Bliley Act (15 U.S.C. 6809))."
3. Section 6003(1) of the AML Act of 2020, Division F of the National Defense Authorization Act for Fiscal Year 2021, Pub. L. 116-283 (January 1, 2021), defines the BSA as comprising Section 21 of the Federal Deposit Insurance Act (12 U.S.C. 1829b), Chapter 2 of Title I of Pub. L. 91-508 (12 U.S.C. 1951 et seq.), and Subchapter II of Chapter 53 of Title 31, United States Code.
4. The AML Act was enacted as Division F, §§ 6001-6511, of the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, Pub. L. 116-283 (2021).
5. *See* Treasury, *National Strategy for Combating Terrorist and Other Illicit Financing*, December 20, 2018; Treasury, *National Strategy for Combating Terrorist and Other Illicit Financing*, February 6, 2020.
6. Covered institutions are financial institutions required by BSA regulations to maintain an AML program. *See* 31 CFR §§ 1020.210(a) (banks); 1020.210(b) (banks without a Federal functional regulator); 1021.210 (casinos and card clubs); 1022.210 (money services businesses); 1023.210 (brokers or dealers in securities); 1024.210 (mutual funds); 1025.210 (insurance companies); 1026.210 (futures commission merchants and introducing brokers in commodities); 1027.210 (dealers in precious metals, precious stones, or jewels); 1028.210 (operators of credit card systems); 1029.210 (loan or finance companies); and 1030.210 (housing government sponsored enterprises).

FinCEN will issue regulations at a later date that will specify how financial institutions should incorporate these Priorities into their risk-based AML programs.[7] FinCEN recognizes that not every Priority will be relevant to every covered institution, but each covered institution should, upon the effective date of future regulations to be promulgated in connection with these Priorities, review and incorporate, as appropriate, each Priority based on the institution's broader risk-based AML program. FinCEN, in coordination with relevant federal and state regulators, has also issued two statements to provide additional guidance to all covered institutions on the applicability of these Priorities at this time, before regulations are promulgated.

I. Methodology

To develop the Priorities, which focus on threats to the U.S. financial system and national security, FinCEN consulted with a number of stakeholders including those with which it was required to consult pursuant to the AML Act. FinCEN also considered a variety of sources of information, including the 2018 and 2020 National Strategies and related risk assessments, prior FinCEN advisories and guidance documents, economic and trade sanctions actions, notices issued by FinCEN and other Treasury components, and previous feedback from law enforcement and covered institutions through the BSA Advisory Group.[8] References to these sources throughout the Priorities are solely intended to provide background information, and FinCEN is not incorporating by reference these additional sources into the Priorities.

Consistent with Treasury's 2018 National Money Laundering Risk Assessment, which informs the National Strategy, "threats" for purposes of these Priorities are predicate crimes associated with money laundering.[9] These threats exploit some perceived "vulnerability" in the U.S. financial system that may be in law, regulation, supervision, or enforcement, or may stem from a unique attribute of a product, service, or jurisdiction.[10]

In consultation with the agencies and offices listed above, FinCEN will update the Priorities at least once every four years, as required by the AML Act,[11] to account for new and emerging threats to the U.S. financial system and national security.

---

7. 31 U.S.C. § 5318(h)(4)(D) as amended by AML Act § 6101(b)(2)(C).
8. As required under section 1654 of the Annunzio-Wylie Anti-Money Laundering Act of 1992, the BSA Advisory Group consists of representatives from federal agencies and other interested persons and financial institutions subject to the regulatory requirements of the BSA.
9. *See* Treasury, *National Money Laundering Risk Assessment*, December 20, 2018, at 6.
10. *Id*. (defining "vulnerability"). The National Strategy sets forth in detail ten vulnerabilities of the U.S. financial system. *See* Treasury, *National Strategy for Combating Terrorist and Other Illicit Financing*, February 6, 2020, at 12-36.
11. 31 U.S.C. § 5318(h)(4)(B) (as amended by AML Act § 6101(b)(2)(C)).

II. AML/CFT Priorities

The Priorities reflect longstanding and continuing AML/CFT concerns previously identified by FinCEN and other Treasury components and U.S. government departments and agencies. The Priorities include predicate crimes that generate illicit proceeds that illicit actors may launder through the financial system. As such, money laundering is linked to all of the Priorities and is not specifically enumerated below as a separate Priority. Combating money laundering remains core to FinCEN and TFI's missions.

A) Corruption

As explained in the National Security Study Memorandum issued by President Biden on June 3, 2021, corruption fuels instability and conflict and undermines economic growth.[12] It has been estimated that corruption reduces global gross domestic product by between 2 and 5 percent.[13] Corruption, both domestic and foreign, threatens U.S. national security by eroding citizens' faith in government, distorting economies, and weakening democratic institutions.

Corrupt actors and their financial facilitators may seek to take advantage of vulnerabilities in the U.S. financial system to launder their assets and obscure the proceeds of crime. Corruption rots democracy from the inside and is increasingly weaponized by authoritarian states to undermine their own democratic institutions as well as disrupt democratic processes in other nations through foreign influence campaigns.[14] Misappropriation of public assets, bribery, and other forms of corruption affects individuals and entities across the world, threatens the national security of the United States and the global financial system, degrades the rule of law, perpetuates conflict, and deprives innocent civilians of fundamental human rights.

Corruption undermines democratic institutions and underpins many of the global challenges of our time, to include serious human rights abuse, and has a disproportionate impact on the poor and most vulnerable. For all of these reasons, countering corruption is a core national security interest of the United States.[15] Addressing the money laundering risks associated with such corruption will bolster efforts to counter corruption.

FinCEN has issued advisories on human rights abuses enabled by corrupt senior foreign political figures and their financial facilitators with respect to Nicaragua, South Sudan, and Venezuela.[16] These advisories, while focused on specific foreign jurisdictions, can help covered institutions comply with their BSA obligations by identifying typologies and red flags, but the jurisdictions noted in those advisories are not the only ones at risk of corruption.

12. *See* The White House, *National Security Study Memorandum Establishing the Fight Against Corruption as a Core United States National Security Interest* (NSSM-1), June 2021.
13. *Id.*
14. *Id.*
15. *Id.*
16. *See* FinCEN, *Advisory to Financial Institutions on the Risk of Proceeds of Corruption from Nicaragua*, October 4, 2018; FinCEN, *Advisory on Political Corruption Risks in South Sudan*, September 6, 2017; FinCEN, *Advisory on Widespread Public Corruption in Venezuela*, September 20, 2017.

B) Cybercrime, including Relevant Cybersecurity and Virtual Currency Considerations

Cybercrime is broadly defined as any illegal activity that involves a computer, another digital device, or a computer network. Cybercrime includes common cybersecurity threats like social engineering, software vulnerability exploits, and network attacks. Cybercrime is a significant illicit finance threat: the size, reach, speed, and accessibility of the U.S. financial system make covered institutions attractive targets to criminals, including terrorists and state actors. These actors target covered institutions' websites, systems, and employees to steal customer and commercial credentials and proprietary information, defraud covered institutions and their customers, and disrupt business functions. Foreign interference in democratic processes, such as elections and election infrastructure, is often conducted through cyber-enabled methods. Treasury is particularly concerned about cyber-enabled financial crime, ransomware attacks, and the misuse of virtual assets that exploits and undermines their innovative potential, including through laundering of illicit proceeds.

FinCEN has issued advisories with respect to ransomware and COVID-19-related cybercrime, including cyber-enabled financial crime, to alert covered institutions to predominant trends, typologies, and potential indicators.[17] Regarding the COVID-19 pandemic, FinCEN advised covered institutions that criminals increasingly exploited the pandemic through phishing campaigns and the compromise of remote applications to facilitate extortion, business email compromise (BEC), and other fraudulent schemes, especially against financial and health care systems.[18] Ill-gotten gains from these illicit activities often are laundered through a variety of methods, including rapid transfers through accounts controlled by the cyber actors or money mules.[19] Covered institutions are uniquely positioned to observe the suspicious activity that results from cybercrime, including cyber-enabled financial crime. FinCEN recently issued a fact sheet to encourage covered institutions to share such information with one another under a safe harbor provision of the BSA that offers protections from civil liability, in order to better identify and report potential money laundering or terrorist financing.[20]

---

17. *See* FinCEN, *Advisory on Ransomware and the Use of the Financial System to Facilitate Ransom Payments,* October 1, 2020; FinCEN, *Advisory on Cybercrime and Cyber-Enabled Crime Exploiting the Coronavirus Disease 2019 (COVID-19) Pandemic*, July 30, 2020. Ransomware attacks are a tactic deployed by criminals to block access to computer systems or data to extort ransom payments from victims in exchange for decrypting the information and restoring victims' access to their systems or data and for refraining from leaking data or taking further actions intended to harm the victim. Some ransomware groups are forming partnerships, or "ransomware cartels," in organized ventures to share advice, code, trends, techniques, practices, and leaked data over shared platforms.

18. *See* FinCEN, *Advisory on Cybercrime and Cyber-Enabled Crime Exploiting the Coronavirus Disease 2019 (COVID-19) Pandemic*, July 30, 2020.

19. A money mule is "a person who transfers illegally acquired money on behalf of or at the direction of another." *See* FinCEN, *Advisory on Imposter Scams and Money Mule Schemes Related to Coronavirus Disease 2019 (COVID-19)*, July 7, 2020.

20. *See* USA PATRIOT Act of 2001, Pub. L. No. 107-56, § 314(b) (2001); 31 CFR § 1010.540; FinCEN, *FinCEN Director Emphasizes Importance of Information Sharing Among Financial Institutions*, December 10, 2020.

As evidenced by recent attacks on the nation's fuel and food supplies, ransomware is a particularly acute concern, as criminals increasingly use sophisticated attacks to target various sectors, including government, finance, education, energy, and health care. Countering ransomware has been identified as a top priority for the United States, which is committed to working with like-minded partners around the world to disrupt and deter ransomware actors, including by developing cohesive and consistent policies towards ransom payments and enabling rapid tracing and interdiction of virtual currency proceeds.[21] According to law enforcement and reporting from covered institutions and others in the private sector, ransomware attacks increased dramatically in 2020 and 2021 in both scale and sophistication, posing a threat to the U.S. health care system and other critical infrastructure, as well as U.S. national security and economic prosperity. In some instances, ransomware campaigns have been associated with adversary governments, sanctioned entities, or jurisdictions with weak AML/CFT regimes and high AML/CFT and sanctions risks, such as Russia, North Korea, and Iran. OFAC issued an advisory[22] in late 2020 highlighting the sanctions risks associated with ransomware payments related to malicious cyber-enabled activities. OFAC has designated numerous malicious cyber actors under its sanctions programs in response to aggressive and harmful malicious cyber activities by state actors targeting U.S. government and private sector networks.

FinCEN notes that, while a substantial financial innovation, convertible virtual currencies (CVCs)[23] also have grown as the currency of preference in a wide variety of online illicit activity. In addition to being the preferred form of payment for buying ransomware tools and services, online child exploitation material, illicit drugs and other illicit goods online, and for paying ransoms to the perpetrators of ransomware attacks, CVCs often are used to layer transactions to hide the origin of money derived from illicit activity.[24] Criminals use a number of techniques to obscure the source of illicit funds when conducting transactions involving CVCs, including the use of mixers and tumblers.[25] CVCs have been used by some of the highest-priority threat actors to advance their illegal activities and nuclear weapons ambitions. For example, North Korea-linked cyber actors likely have stolen hundreds of millions of dollars' worth of CVCs since 2019 through cyber operations against CVC service providers, laundered stolen CVC value through other CVC service providers and CVC wallets, and used the proceeds to help fund weapons of mass destruction and ballistic missile programs.[26] Victim institutions, and institutions used for laundering stolen funds,

---

21. White House Press Briefing, *Press Briefing by Press Secretary Jen Psaki, June 2, 2021*, June 2, 2021.
22. *See* OFAC, *Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments*, October 1, 2020.
23. *See* FinCEN, *Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies*, May 9, 2019, for additional information related to CVCs.
24. *See* Treasury, *National Money Laundering Risk Assessment*, December 20, 2018, at 3.
25. Mixing or tumbling involves the use of mechanisms to break the connection between an address sending CVC and the addresses receiving CVC. *See* FinCEN, *Advisory on Illicit Activity Involving Convertible Virtual Currency*, May 9, 2019.
26. *See* Treasury, *Treasury Sanctions Individuals Laundering Cryptocurrency for Lazarus Group*, March 2, 2020.

are based in several countries, highlighting the global nature of financial crimes involving CVCs. In 2019, FinCEN issued an advisory to help covered institutions identify and report suspicious activity concerning how criminals and other bad actors exploit CVCs.[27]

In 2016, FinCEN issued an advisory with respect to cybercrime that set out typologies and red flags for covered financial institutions' BSA/AML compliance and cybersecurity units, and encouraged greater cooperation between those units.[28]

C) Terrorist Financing

Since the September 11, 2001 terrorist attacks, the threat posed by international and domestic terrorism has evolved significantly. Internationally, the Islamic State of Iraq and Syria (ISIS), Al Qaeda, Lebanese Hizballah, and Iran's Islamic Revolutionary Guard Corps remain significant and persistent terrorist threats to U.S. interests and allies. Domestically, the Intelligence Community assesses that racially or ethnically motivated violent extremists (RMVEs)—primarily those advocating for the superiority of the white race—and anti-government or anti-authority violent extremists are the most lethal domestic violent extremist (DVE) threats.[29] Additionally, the National Strategy for Countering Domestic Terrorism, issued on June 15, 2021, highlights the ongoing threat to Americans posed by domestic terrorism.[30]

Terrorists require financing to recruit and support members, fund logistics, and conduct operations. Preventing such financing, therefore, is essential to counter the threat of terrorism successfully. Covered institutions are reminded of existing obligations to identify and file SARs on potential terrorist financing transactions, as appropriate, and follow applicable requirements for reporting violations requiring immediate attention.[31] Terrorist financing includes lone actors using small amounts of money to self-fund attacks, as well as more complex schemes and networks that may be embedded within existing money laundering methods used to support logistical networks, operatives, and the procurement of material. In 2015 and 2018, Treasury raised awareness of the issue by publishing a National Terrorist Financing Risk Assessment and addressed the associated vulnerabilities in the 2020

---

27. *Id.*

28. *See* FinCEN, *Advisory to Financial Institutions on Cyber-Events and Cyber-Enabled Crime*, October 25, 2016.

29. Office of the Director of National Intelligence, Department of Justice, and Department of Homeland Security, *Joint Comprehensive Threat Assessment on Domestic Violent Extremism*, March 1, 2021, at 2. For additional information on the threat posed by domestic terrorists, see Federal Bureau of Investigation, Department of Homeland Security, *Strategic Intelligence Assessment and Data on Domestic Terrorism*, May 2021.

30. *See* The White House, *National Strategy For Countering Domestic Terrorism*, June 15, 2021.

31. *See* 31 CFR §§ 1020.320 (banks); 1021.320 (casinos and card clubs); 1022.320 (money services businesses); 1023.320 (brokers or dealers in securities); 1024.320 (mutual funds); 1025.320 (insurance companies); 1026.320 (futures commission merchants and introducing brokers in commodities); 1029.210 (loan or finance companies); and 1030.210 (housing government sponsored enterprises).

National Strategy.[32] As a countermeasure to these potential risks, covered institutions must comply with required sanctions programs and, as part of their risk-based AML programs, also should be aware of terrorists and terrorist organizations that are included on sanctions lists issued by the U.S. government.

i. International Terrorism

The most common type of international terrorism activity in the United States involves individuals who knowingly provide funds to overseas terrorists, terrorist groups, or their supporters abroad.[33] Most terrorist groups still primarily rely on banks, money services businesses, and cash couriers to transfer funds, though some more regularly seek small-dollar donations in digital assets.[34]

Disrupting terrorist networks, such as those supporting Al Qaeda and Hizballah, and preventing an ISIS resurgence are vitally important for the security of the United States and its allies.[35] Rather than fund complex attacks, ISIS and Al Qaeda now rely more on self-radicalized individuals and homegrown violent extremists who carry out relatively low-cost and unsophisticated but deadly attacks using knives, firearms, improvised explosive devices, or automobiles. In addition, U.S. authorities have identified U.S.-based individuals who raise and send money to support violence overseas or who travel to Iraq and Syria as foreign terrorist fighters.[36]

ii. Domestic Terrorism

DVEs are individuals based and operating primarily within the territorial jurisdiction of the United States who seek to further their ideological goals wholly or in part through unlawful acts of force or violence.[37] The intelligence and law enforcement communities conducted a comprehensive assessment of the domestic terrorism threat and assessed that RMVEs and

---

32. *See* Treasury, *National Terrorist Financing Risk Assessment*, June 12, 2015; Treasury, *National Terrorist Financing Risk Assessment*, December 20, 2018; Treasury, *National Strategy for Combatting Terrorist and Other Illicit Financing*, February 6, 2020.
33. *See* Treasury, *National Terrorist Financing Risk Assessment*, December 20, 2018, at 2.
34. *See* Treasury, *National Strategy for Combating Terrorist and Other Illicit Financing*, February 6, 2020, at 11.
35. *See* The White House, *Interim National Security Strategic Guidance*, March 2021, at 11.
36. *See* U.S. Department of State, *Country Reports on Terrorism*, June 24, 2020, at 3.
37. Domestic terrorism, as defined by 18 U.S.C. § 2331(5), means activities that "(A) involve acts dangerous to human life that are a violation of the criminal laws of the United States or of any State; (B) appear to be intended—(i) to intimidate or coerce a civilian population; (ii) to influence the policy of a government by intimidation or coercion; or (iii) to affect the conduct of a government by mass destruction, assassination, or kidnapping; and (C) occur primarily within the territorial jurisdiction of the United States." However, "[m]ere advocacy of political or social positions, political activism, use of strong rhetoric, or generalized philosophic embrace of violent tactics may not constitute violent extremism, and may be constitutionally protected." Office of the Director of National Intelligence, Department of Justice, and Department of Homeland Security, *Joint Comprehensive Threat Assessment on Domestic Violent Extremism*, March 1, 2021, at 3-4.

militia violent extremists present the most lethal DVE threats.[38] RMVEs use or threaten to use force or violence in furtherance of ideological agendas derived from bias—often related to race or ethnicity—against given population groups.[39] They purport to use both political and religious justifications to support racially or ethnically based ideological objectives and criminal activities, and have used or threatened acts of violence to promote their agendas.[40] Militia violent extremists use or threaten to use force or violence in furtherance of an anti-government or anti-authority violent extremist ideology, including opposition to abuses of power by the government.[41]

Some DVEs have focused on accessible targets like civilians, law enforcement and the military, symbols or members of the U.S. government, houses of worship, retail locations, and mass public gatherings. DVEs' selection of these types of targets, in addition to the insular nature of DVEs' radicalization and mobilization to violence and their limited discussions with others, challenges law enforcement to detect and disrupt the activities of DVEs before they occur.[42]

D) Fraud

As previously noted in Treasury's National Money Laundering Risk Assessments, the crimes that generate the bulk of illicit proceeds in the United States are fraud, drug trafficking, human smuggling, human trafficking, organized crime, and corruption.[43] Among those, fraud—such as bank, consumer, health care, securities and investment, and tax fraud—is believed to generate the largest share of illicit proceeds in the United States.[44] Health care fraud alone is estimated to generate proceeds of approximately $100 billion annually.[45] Increasingly, fraud schemes are internet-enabled, such as romance scams, synthetic identity fraud, and other forms of identity theft.[46] Proceeds from fraudulent activities may be laundered through a variety of methods, including transfers through accounts of offshore legal entities, accounts controlled by cyber actors, and money mules.

---

38. *See* Office of Director of National Intelligence, Department of Justice, and Department of Homeland Security, *Joint Comprehensive Threat Assessment on Domestic Violent Extremism*, March 1, 2021. Additionally, on May 14, 2021, the Department of Homeland Security (DHS) issued a National Terrorism Advisory System Bulletin due to a heightened threat environment across the United States, including from DVEs. *See* DHS, *National Terrorism Advisory System Bulletin*, May 14, 2021.
39. Federal Bureau of Investigation, Department of Homeland Security, *Strategic Intelligence Assessment and Data on Domestic Terrorism*, May 2021, at 15.
40. *Id*.
41. *See* Office of Director of National Intelligence, Department of Justice, and Department of Homeland Security, *Joint Comprehensive Threat Assessment on Domestic Violent Extremism*, March 1, 2021
42. *See* FBI Director Christopher A. Wray, *Oversight of the Federal Bureau of Investigation: The January 6 Insurrection, Domestic Terrorism, and Other Threats*, March 2, 2021.
43. *See* Treasury, *National Money Laundering Risk Assessment*, December 20, 2018, at 2.
44. *Id*.
45. *Id*.
46. *Id*.

FinCEN has issued several fraud-related advisories, in particular with respect to BEC, email account compromise, and COVID-19. In 2019, FinCEN noted that BEC and email account compromise schemes were among a growing trend of cyber-enabled crime, with 32,000 reported cases involving almost $9 billion in attempted theft from BEC fraud schemes affecting U.S. financial institutions and their customers.[47] More recently, fraud related to the COVID-19 pandemic has been of particular concern, and has been the subject of six FinCEN Advisories, including: economic impact payment, health insurance and health care, unemployment insurance, counterfeit COVID-19 vaccine, pump-and-dump and other market manipulation schemes, and cyber-enabled fraud schemes.[48] The Department of Justice is aggressively pursuing a wide range of COVID-19-related fraud schemes.[49]

Also of concern are foreign intelligence entities and their proxies, which employ illicit financial practices to fund influence campaigns and facilitate a range of espionage activity by establishing front companies, and conducting targeted investments to gain access to sensitive U.S. individuals, information, technology and intellectual property.[50]

E) Transnational Criminal Organization Activity

Transnational criminal organizations (TCOs) operating in the United States,[51] including drug trafficking organizations (DTOs), are priority threats due to the crime-terror nexus and TCOs' engagement in a wide range of illicit activities, including cybercrime, drug trafficking, fraud, wildlife trafficking, human smuggling, human trafficking, intellectual property theft, weapons trafficking, and corruption.[52] Treasury has noted that a number of TCOs operate in the United States, and Mexican and Russian TCOs operating in the United States remain priority threats.[53] In addition, certain Africa- and Asia-based TCOs become more significant

---

47. *See* FinCEN, *Advisory to Financial Institutions on E-Mail Compromise Fraud Schemes*, September 6, 2016; FinCEN, *Updated Advisory on Email Compromise Fraud Schemes Targeting Vulnerable Business Practices*, July 16, 2019. To request immediate assistance in recovering BEC-stolen funds, covered institutions should file a complaint with the Federal Bureau of Investigation's Internet Crime Complaint Center (IC3), or contact the nearest United States Secret Service field office.

48. For a list of FinCEN COVID-19-related advisories, alerts, and notices, *see FinCEN COVID-19-Related Advisories and Alerts*. FinCEN encourages covered institutions to use FinCEN-provided key terms and filing instructions when filing SARs for fraudulent activities, crimes, and cyber and ransomware attacks related to COVID-19. *See* FinCEN, *Consolidated COVID-19 Suspicious Activity Report Key Terms and Filing Instructions*, February 24, 2021.

49. *See* Department of Justice, *Justice Department Takes Action Against COVID-19 Fraud*, March 26, 2021.

50. Director of National Intelligence, *National Counterintelligence Strategy of the United States of America 2020-2022*, January 7, 2020, at 8-9.

51. Transnational organized crime refers to "self-perpetuating associations of individuals who operate transnationally for the purpose of obtaining power, influence, monetary, or commercial gains, wholly or in part by illegal means, while protecting their activities through a pattern of corruption or violence or through a transnational organization structure and the exploitation of transnational commerce or communication mechanisms."10 U.S.C. § 284(i)(6).

52. *See* The White House, *Strategy to Combat Transnational Organized Crime*, July 19, 2011.

53. *See* Treasury, *National Money Laundering Risk Assessment*, December 20, 2018, at 17.

each year as TCOs worldwide continue to employ a variety of money laundering methods to avoid detection.[54] Malign state actors who provide TCOs safe haven or other support in return for financial or political gain, or assurances of their own security, enable TCOs' malign activity, including foreign election interference, attempts to stoke social unrest, and other profit-driven criminal acts—most often perpetrated online—that undermine public confidence and threaten the social fabric of foreign nations. Increasingly, these organizations turn to professional money laundering networks that receive a fee or commission for their laundering services, and often use their specialized expertise to launder proceeds generated by others, regardless of the predicate criminal activity.[55]

F) Drug Trafficking Organization Activity

Illicit drugs continue to generate significant proceeds for DTOs. The proceeds, which may be laundered in or through the United States, and the drugs themselves, contribute to a significant public health emergency.[56] Mexican DTOs' distribution of fentanyl to the United States has increased, while direct shipments from China have decreased, though China remains a significant source of precursor chemicals.[57] Drug cartels in Mexico and Colombia also operate as sophisticated independent DTOs trafficking cocaine and other drugs to the United States.[58] DTOs rely more on professional money laundering networks in Asia (primarily China) that facilitate exchanges of Chinese and U.S. currency or serve as money brokers in trade-based money laundering (TBML) schemes.[59] There has been a substantial increase in complex schemes to launder proceeds from the sale of narcotics by facilitating the exchange of cash proceeds from Mexican DTOs to Chinese citizens residing in the United States, including the use of front companies or couriers to deposit cash derived from the sale of narcotics into the banking system.[60] These schemes allow DTOs to repatriate proceeds to Mexico and sidestep Chinese capital flight restrictions.[61]

---

54. *Id*.
55. *Id*. at 12.
56. *Id*.
57. *See* Drug Enforcement Administration, *National Drug Threat Assessment*, March 2, 2021, at 14. See also FinCEN, *Advisory to Financial Institutions on Illicit Financial Schemes and Methods Related to the Trafficking of Fentanyl and Other Synthetic Opioids*, August 21, 2019 (guidance on reporting fentanyl and opioid trafficking).
58. *See* Treasury, *National Money Laundering Risk Assessment*, December 20, 2018, at 17-19.
59. *See* Treasury, *National Strategy for Combating Terrorist and Other Illicit Financing*, February 6, 2020, at 10. For additional information on TBML schemes generally, *see* FinCEN, *Update on U.S. Currency Restrictions in Mexico: Funnel Accounts and TBML*, May 28, 2014; FinCEN, *Advisory to Financial Institutions on Filing Suspicious Activity Reports regarding Trade-Based Money Laundering*, February 18, 2010.
60. *See, e.g.*, Department of Justice, *Three Indicted for International Money Laundering Scheme Pairing Mexican Drug Traffickers and Chinese Nationals*, October 18, 2019.
61. *See* Treasury, *National Strategy for Combating Terrorist and Other Illicit Financing*, February 6, 2020, at 24.

In 2019, FinCEN issued an advisory related to the trafficking of fentanyl and other synthetic opioids, which contained an extensive discussion of typologies, case studies, and red flags.[62]

G) Human Trafficking and Human Smuggling

Financial activity from human trafficking[63] and human smuggling[64] activities can intersect with the formal financial system at any point during the trafficking or smuggling process. FinCEN, in collaboration with law enforcement agencies, nonprofit organizations, and members of the financial industry, issued two advisories identifying financial and behavioral red flags of human trafficking, as well as financial red flags associated with human smuggling.[65]

As described in these advisories and other U.S. government reports, human trafficking and human smuggling networks use a variety of mechanisms to move illicit proceeds, ranging from cash smuggling by individual victims to sophisticated cash smuggling operations through professional money laundering networks and criminal organizations.[66] The illicit proceeds from human trafficking can include income associated with logistics, such as housing and transportation of victims, as well as earnings from the exploitation of victims. Human traffickers and smugglers have established shell companies to hide the true nature of a business. Human traffickers and human smugglers receive payments in a variety of ways, such as funnel accounts and TBML schemes.

H) Proliferation Financing

The principal threat of proliferation financing[67] arises from proliferation support networks. These networks of individuals and entities, such as trade brokers and front companies, seek to exploit the U.S. financial system to move funds that will be used either: (1) to acquire weapons

---

62. *See* FinCEN, *Advisory to Financial Institutions on Illicit Financial Schemes and Methods Related to the Trafficking of Fentanyl and Other Synthetic Opioids*, August 21, 2019.

63. Human trafficking crimes, which are defined in Title 18, Chapter 77, focus on the act of compelling or coercing a person's labor, services, or commercial sex acts. *See* Department of Justice, Human Trafficking Prosecution Unit.

64. Human smuggling involves illegally transporting people, who have consented to their travel, into the United States and, potentially, the subsequent harboring of those individuals in the United States. While human trafficking and human smuggling are distinct crimes, individuals who are smuggled are vulnerable to becoming victims of human trafficking. *See* FinCEN, *Advisory Guidance Recognizing Activity that May be Associated with Human Smuggling and Human Trafficking*, September 11, 2014; FinCEN, *Supplemental Advisory on Identifying and Reporting Human Trafficking and Related Activity*, October 15, 2020.

65. *Id*.

66. *Id*; Department of State, *Trafficking in Persons, 20th Edition*, June 2020.

67. Proliferation financing refers to the act of providing funds or financial services which are used, in whole or in part, for the manufacture, acquisition, possession, development, export, trans-shipment, brokering, transport, transfer, stockpiling, or use of nuclear, chemical, or biological weapons and their means of delivery and related materials (including both technologies and dual use goods used for non-legitimate purposes), in contravention of national laws or, where applicable, international obligations. *See* Treasury, *National Proliferation Financing Risk Assessment*, December 20, 2018, at 3-4.

of mass destruction or delivery systems or their components; or (2) in the furtherance or development of state-sponsored weapons programs, including the evasion of United Nations or U.S. sanctions. Global correspondent banking is a principal vulnerability and driver of proliferation financing risk within the United States due to its central role in processing U.S. dollar transactions, which comprise a substantial proportion of cross-border trade.[68]

Actors engaged in the proliferation of weapons of mass destruction have developed sophisticated and diverse strategies to finance their programs. Covered institutions remain vulnerable to malign actors seeking to generate revenues and transfer funds in support of illicit conduct through gatekeepers, front or shell companies, exchange houses, or the illicit exploitation of international trade.[69] As described in multiple advisories issued by Treasury, Iran, North Korea, and Syria, in particular, have exploited vulnerabilities in global supply chains and maritime transportation to facilitate their weapons of mass destruction proliferation activities.[70] Covered institutions are encouraged to consult these advisories and FinCEN's advisories with respect to jurisdictions with AML/CFT and counter-proliferation deficiencies for additional information regarding the risk of proliferation finance.[71]

As a counter-measure to these potential risks, covered institutions must comply with sanctions programs and, as part of a risk-based AML program, should also be aware of economic and trade sanctions issued by the federal government, such as OFAC, the Department of Commerce's Bureau of Industry and Security, and the Department of State's Bureau of International Security and Nonproliferation.

For Further Information

Additional guidance, administrative rulings, and illicit finance information (including advisories and notices) can be found on FinCEN's website at https://www.fincen.gov, which also contains information on how to register for FinCEN Updates. Questions or comments regarding the contents of the Priorities should be addressed to the FinCEN Regulatory Support Section at frc@fincen.gov.

---

68. *Id*. at 40-42.

69. *See* Treasury, *Advisory on the Use of Exchange Houses and Trading Companies to Evade U.S. Economic Sanctions Against Iran*, January 10, 2013; Treasury, *Guidance to Address Illicit Shipping and Sanctions Evasion Practices*, May 14, 2020. Recent FinCEN advisories on specific actors include: *The Iranian Regime's Illicit and Malign Activities and Attempts to Exploit the Financial System*, October 11, 2018, and *North Korea's Use of the International Financial System*, November 2, 2017.

70. *See* Treasury, *Guidance to Address Illicit Shipping and Sanctions Evasion Practices*, May 14, 2020; Treasury, *Sanctions Risks Related to Petroleum Shipments involving Iran and Syria*, March 25, 2019; Treasury, *Sanctions Risks Related to North Korea's Shipping Practices*, February 23, 2018.

71. *See* FinCEN, *Advisory on the Financial Action Task Force-Identified Jurisdictions with Anti-Money Laundering and Combating the Financing of Terrorism and Counter-Proliferation Deficiencies*, March 11, 2021.