Davis Polk

Treasury publishes national risk assessments on illicit finance risks

March 9, 2022 | Client Update | 8-minute read

The U.S. Treasury Department's latest national risk assessments highlight the most significant illicit finance risks in the United States financial system.

On March 1, 2022, the United States Department of the Treasury (the Treasury) published the 2022 National Risk Assessments (NRAs) on Money Laundering (NMLRA), Terrorist Financing (NTFRA) and Proliferation Financing (NPFRA), providing the Treasury's analysis of the most significant illicit finance threats, vulnerabilities, and risks to the United States financial system. The NRAs, which follow previous publications in 2015 and 2018, draw on findings from law enforcement, regulatory agencies, and intelligence communities, and will guide national policies and priorities with respect to anti-money laundering (AML), countering the financing of terrorism (CFT), and countering proliferation financing.[1] The NRAs address changes to the illicit finance landscape that were the result of the COVID-19 pandemic, the rise in cybercrimes such as ransomware attacks, and the increasing adoption of digital payment systems and financial services. In the coming weeks, the Treasury will publish its 2022 National Strategy for Combatting Terrorist and Other Illicit Finance, which will lay out the Treasury's strategy for addressing the risks identified in the NRAs.

The national money laundering risk assessment

The NMLRA is organized around two primary topics: (1) the primary money laundering threats within the U.S. financial system (i.e., the predicate crimes most associated with money laundering); and (2) the most significant money laundering vulnerabilities and risks.

Primary money laundering threats

According to the NMLRA, fraud, cybercrime, drug trafficking, professional money laundering, corruption, and human trafficking and smuggling are the most significant money laundering threats facing the United States.[2] Consistent with the 2015 and 2018 NMLRAs, fraud remains "the largest driver of money laundering activity in terms of the scope of activity and magnitude of illicit proceeds." Although the Treasury has consistently identified predicate crimes such as fraud, drug trafficking, and corruption as significant money laundering threats, the 2022 NMLRA departs from previous assessments by specifically highlighting cybercrime and professional money laundering as areas of primary concern. New areas of focus in the NMLRA include:

- **COVID-19-related fraud and scams.** According the NMLRA, the COVID-19 pandemic "significantly accelerated the transition from in-person financial activities to online account opening, payments, and lending," which in turn increased the risk of online fraud, "and led to a dramatic spike in the number of stimulus, healthcare, bank, elder, and government fraud schemes and scams exploiting the COVID-19 pandemic."[3]
- **Synthetic identity theft.** The FBI identified synthetic identity theft (SIF) as the fastest growing financial crime in the United States. SIF involves the use of a combination of real and fake personally identifiable information (including stolen social security numbers) "to fabricate a person or entity in order to commit a dishonest act for personal or financial gain." Criminals use synthetic identities to open banking and credit card accounts, make fraudulent purchases, and "gain access to the U.S. financial sector anonymously."

- **Cybercrimes.** Since the 2018 NMLRA, incidents of cybercrime have significantly increased, including ransomware attacks, the harvesting of personal and financial information through data breaches, and business email compromise, which involves the use of fake corporate email accounts to trick employees into transferring funds into bank accounts that they believe to belong to trusted partners. The prevalence and scale of ransomware attacks has also increased—FinCEN analysis of suspicious activity report (SAR) data found "a 42 percent increase in ransomware-related SARs in the first six months of 2021 compared to all of 2020."
- **Professional money laundering.** The NMLRA reports that professional money laundering organizations (PMLOs), which include money brokers and organized criminal groups, remain a significant money laundering threat. PMLOs engage in a range of illicit activities, including "conducting money pickups of drug proceeds in the United States, transporting the cash, depositing the money into the retail banking system, and/ or transferring the money to different individuals or entities."
- **Wildlife trafficking.** The Treasury reports that U.S. financial institutions are vulnerable to money laundering connected to wildlife trafficking, "given the importance of the U.S. dollar and financial system to international trade and finance, the difficulty of identifying underlying illicit connections, and a lack of financial intelligence on these types of crimes."

Significant money laundering vulnerabilities and risks

In addition to the money laundering threats discussed above, the NMLRA identifies a number of money laundering risks and vulnerabilities facing the U.S. financial system. The lack of transparency in the beneficial ownership of corporate entities continues to facilitate the laundering of illicit proceeds and hamper law enforcement investigations. The NMLRA notes that the new U.S. requirements to report beneficial ownership information to the federal government, which FinCEN is currently implementing, "are expected to help facilitate law enforcement investigations and make it more difficult for illicit actors to hide behind corporate entities registered in the United States."[4] That said, the lack of transparency into corporate entities organized in foreign jurisdictions and the misuse of trusts, both domestically and abroad, present a persistent money laundering risk.

Finally, the NMLRA highlights the increasing use of virtual assets to launder criminal funds. Although the use of virtual assets in money laundering remains "far below" the use of fiat currency, the NMLRA notes that the "number of users and market capitalization of virtual assets" has substantially grown since 2018, as has the use of Virtual Asset Service Providers (VASPs) "to launder the proceeds of drug trafficking, fraud, and cybercrime, including ransomware attacks." Although VASPs are generally subject to AML program requirements under the Bank Secrecy Act, many VASPs organized and operating outside of the United States fail to implement adequate AML/CFT controls, which in turn poses a substantial threat to the U.S. financial system.

National terrorist financing risk assessment

According to the NTFRA, the United States remains susceptible to terrorist financing due to its central role in the global economy, even though the foreign terrorist threat has been "less acute" in recent years. ISIS, Al-Qa'ida, and Hizballah remain the primary sources of terrorist financing threats. Notably, the NTFRA analyzes for the first time the funding methods that support domestic violent extremists (DVE).

The Treasury observes that the most common methods of international terrorist financing involve the transfer of funds from "U.S.-based supporters to facilitators outside of the United States working on behalf of" foreign terrorist groups. Moreover, common methodologies include the use of unlicensed money services businesses and/or fund transfers under front or sham charities. Supporters of terrorist groups are also increasingly "adapting to new technologies that can better obscure financial activities, while also decentralizing their operational structure to minimize the visible flow of funds." This often involves the use of online crowdfunding platforms to solicit funds, as well as virtual assets. According to the NTFRA, "U.S. authorities have identified several instances where terrorist groups and their financial supporters solicited funds in virtual assets, usually through a social media platform or other internet-based crowdsource platform[,]" though, "terrorist use of virtual assets appears to remain limited when compared to other financial products and services."

According to the NTFRA, domestic violent extremists (DVEs) are among the most significant developments in the U.S. terrorism landscape. 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." The White House's National Strategy for Countering Domestic Terrorism cites DVEs as posing a serious and evolving threat and, consequently, the use of the U.S. financial system to facilitate the actions of DVEs is of a growing concern. According to the NTFRA, self-financing is a primary source of funds for DVEs, which presents challenges for financial institutions because the transactional activity is often difficult to distinguish from the customer's routine financial activity, based on the individual's risk profile.

National proliferation financing risk assessment

According to the NPFRA, the primary threat actors with respect to proliferation financing remain the Democratic Republic of North Korea (DPRK) and Iran. Proliferation financing typically involves the use of networks and brokers, which employ a variety of means to obscure their connection to foreign governments and engage in clandestine procurement and fundraising activities. The most common methodologies involve the exploitation of correspondent banking relationship and multiple front and shell companies. These companies "present themselves as innocuous trading firms, hiding in plain sight amid a larger global ocean of small and medium enterprises." By operating through a web of corporate structures, proliferation financing networks are able to acquire U.S.-origin items and move funds through the U.S. financial system while acting on behalf of sanctioned governments. Accordingly, the U.S. financial system's most significant vulnerabilities to proliferation financing remain the lack of legal entity transparency in many jurisdictions and the ease with which networks "can use opaque corporate entities to engage with the U.S. financial system."

Finally, the NPFRA further notes that proliferation financing networks are also "increasingly exploiting the digital economy, including through the systematic mining and trading of virtual assets, and the hacking of virtual asset service providers." As the Treasury reported in the NMLRA, the lack of adequate AML/CFT programs among some foreign VASPs significantly contribute to the risks associated with virtual assets in the U.S. financial system.

Financial institutions should consider using the NRAs to increase their understanding of the current illicit finance environment and inform their risk mitigation strategies.

If you have any questions regarding the matters covered in this publication, please contact any the lawyers listed below or your usual Davis Polk contact.

If you have any questions regarding the matters covered in this publication, please reach out to any of the lawyers listed below or your usual Davis Polk contact.

Greg D. Andres
+1 212 450 4724
greg.andres@davispolk.com

Kendall Howell
+1 202 962 7068
kendall.howell@davispolk.com

Paul Marquardt
+1 202 962 7156
paul.marquardt@davispolk.com

Tatiana R. Martins
+1 212 450 4085
tatiana.martins@davispolk.com

John B. Reynolds III
+1 202 962 7143
john.reynolds@davispolk.com

Will Schisa
+1 202 962 7129
will.schisa@davispolk.com

Daniel P. Stipano
+1 202 962 7012
dan.stipano@davispolk.com

Charles Marshall Wilson
+1 202 962 7130
charles.wilson@davispolk.com

1 The United States conducts the NRAs in accordance with the best practices recommended by the Financial Action Task Force (FATF), an inter-governmental body that issues international standards to combat illicit finance. FATF recommends that governments identify, assess, and understand the primary money laundering and terrorist financing risks facing their country and use those risks assessments to implement national strategies to prevent financial crime. *See* FATF, International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation (2021), https://www.fatf-gafi.org/content/dam/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf.

2 As the Treasury notes, the findings related to those threats align with the 2021 National AML/CFT Priorities issued by the Financial Crimes Enforcement Network (FinCEN) FinCEN, Anti-Money Laundering and Countering the Financing of Terrorism National Priorities (FinCEN, AML/CFT Priorities), (Jun. 30, 2021), https://www.fincen.gov/sites/default/files/shared/AML_CFT%20Priorities%20(June%2030%2C%202021).pdf. We discuss the National AML/CFT Priorities in the following client update.

3 As of October 2021, the DOJ charged 984 defendants in connection to 682 different fraud schemes relating to COVID-19, involving attempts to steal over $753 million from individuals and the U.S. government. Those cases included the theft of COVID relief funds, an uptick in healthcare fraud, and phishing scams that reference payments made through the CARES Act.

4 We discuss FinCEN's beneficial ownership proposed rule in the following client update.