FinCEN Issues Government-Wide AML/CFT Priorities: **Four Things To Know**

On Wednesday, June 30, 2021, the Financial Crimes Enforcement Network ("FinCEN") released its first set of government-wide priorities for anti-money laundering and countering the financing of terrorism ("AML/CFT") (the "Priorities"). The release identifies eight priorities, covering money laundering related to: (i) corruption and kleptocracy; (ii) cybercrime, including as it relates to cybersecurity and virtual currency; (iii) international and domestic terrorist financing; (iv) fraud; (v) transnational organized crime; (vi) drug trafficking; (vii) human trafficking and smuggling; and (viii) arms proliferation.

FinCEN developed the Priorities pursuant to Section 6101 of the Anti-Money Laundering Act of 2020 ("AMLA"), which required FinCEN to establish AML/CFT priorities on which financial institutions could rely in allocating resources within their own AML programs. As required by the AMLA, FinCEN consulted with the federal banking agencies and the U.S. Department of Justice, among other government agencies, prior to publishing the Priorities.

This alert summarizes four key takeaways from the Priorities.

1 The Priorities Cover the Field of Known AML Risks

The Priorities address a range of known AML risks, encompassing the following areas.

- **Corruption.** Echoing other recent statements from the Biden Administration (summarized in our client alert, here), the Priorities recognize anti-corruption efforts as "a core national security interest of the United States." The Priorities thus further reinforce our view that Foreign Corrupt Practices Act ("FCPA") and related anti-corruption enforcement will increase in the years ahead. Global banks should expect continued scrutiny of their control frameworks for corruption-related AML risks, which can affect businesses spanning private banking, investment banking, and transaction banking.
- **Cybercrime.** As discussed below, the Priorities prominently discuss cybercrime and cybersecurity, as well as the illicit use of virtual currencies.
- **Terrorist Financing.** The Priorities "remind[]" covered institutions of their existing obligations to identify and file SARs on potential terrorist financing transactions and to follow applicable requirements for reporting violations. As discussed below, the Priorities emphasize both international and domestic terrorist financing.
- **Fraud.** The Priorities note that fraud schemes, which are increasingly internet-enabled, continue to "generate the largest share of illicit proceeds in the United States." The Priorities define fraud broadly, and specifically flag schemes related to business email compromise, email account compromise, and COVID-19, as well as schemes conducted by foreign state actors to fund influence campaigns in the United States.
- **Transnational Criminal Organizations, Drug Trafficking, and Human Trafficking and Smuggling.** The Priorities emphasize that transnational criminal organizations "are priority threats due to the crime-terror nexus and [their] engagement in a wide range of illicit activities." The Priorities also discuss access to the financial system by drug traffickers, human traffickers, and smugglers,

highlighting FinCEN's observation of "a substantial increase in complex schemes to launder proceeds from the sale of narcotics by facilitating the exchange of cash proceeds from Mexican [drug trafficking organizations] to Chinese citizens residing in the United States."

- **Proliferation Financing.** Emphasizing weapons of mass destruction and other arms proliferation activities involving Iran, North Korea, and Syria, the Priorities identify global correspondent banking as "a principal vulnerability and driver of proliferation financing risk within the United States due to its central role in processing U.S. dollar transactions." FinCEN's emphasis on proliferation financing aligns with recent statements by the Financial Action Task Force and others.

2 The Priorities Highlight Domestic Terrorism as an Evolving Risk Area

The Priorities identify domestic terrorism as an "ongoing threat to Americans," describing "racially or ethnically motivated violent extremists . . . and antigovernment or anti-authority violent extremists" as among "the most lethal domestic violent extremist (DVE) threats." The emphasis on domestic terrorism is expected, but also poses unique challenges for financial institutions, including banks that operate only domestically and thus may previously have been viewed as being exposed to only limited terrorist financing risk.

Financial institutions may need to employ different and potentially more nuanced tools to monitor for domestic terrorist financing as compared to international terrorist financing. For example, whereas surveillance models for international terrorist financing may make use of jurisdiction-based risk ratings, that may not be possible for domestic terror financing. Moreover, institutions may find it challenging to differentiate between domestic terrorist groups and groups that are engaging in disfavored or offensive, but nonetheless legal, political activities. The Priorities acknowledge that law enforcement actors have themselves faced "challenges" in detecting and disrupting domestic terrorists' activities before they occur.

3 The Priorities Identify Cybercrime As Another Key Area to Watch

Noting recent ransomware attacks on the nation's fuel and food supplies, the Priorities emphasize the need to combat ransom-related activity, which it notes has broadly targeted a variety of government and non-governmental sectors. The Priorities also assert that there is a growing use of convertible virtual currencies to pay for illicit goods and drugs, and to hide the origin of illicit funds, including use of virtual currencies by some of the "highest-priority threat actors," such as North Korea-linked actors.

The Priorities direct institutions to multiple cybercrime and virtual currency advisories issued by FinCEN and other agencies in recent years, including advisories concerning: COVID-19-related cybercrime; phishing and cyber compromise schemes; sanctions-related risks in ransomware payments; and the use of virtual currencies "to layer transactions to hide the origin of money derived from illicit activity."

4 Financial Institutions Should Begin Considering Strategies to Incorporate the Priorities

Under forthcoming rules, expected to be promulgated pursuant to the AMLA within the next 180 days, financial institutions will be required incorporate the Priorities into their AML control frameworks. Under the AMLA, this process is intended to allow financial institutions to evaluate risks and target resources in a manner consistent with the Priorities. It is open to question, however, whether the Priorities are sufficiently specific and defined to allow for the type of targeting contemplated by Congress when it passed the AMLA.

Nevertheless, together with the Priorities, FinCEN issued a joint statement with federal and state banking regulators that encourages banks to "start considering how they will incorporate the . . . Priorities" into their AML programs. At the same time, the statement clarifies that the Priorities alone do not change existing Bank Secrecy Act ("BSA") requirements or supervision and examination practices for banks, and that any such change will await the forthcoming rulemaking. The federal bank regulators noted, in this regard, that they plan to revise their own BSA/AML regulations, as well.

In addition to the interagency statement issued with banking regulators, FinCEN issued a statement concerning non-bank financial institutions ("NBFIs"), which similarly noted that the Priorities alone do not create "an immediate change in the [BSA] requirements or supervisory expectations for covered NBFIs," but that NBFIs "may wish to start considering how they will incorporate the . . . Priorities into their risk-based AML programs."

While the Priorities are undoubtedly broad, it will be important for financial institutions to closely review FinCEN's release and consider whether their control frameworks adequately address related risks. Financial institutions should also closely track, and consider submitting comments as part of, the forthcoming rulemaking processes that will codify the role the Priorities should play in financial institution AML programs.

For further information on the Priorities or the AMLA more generally, please contact the following members of Covington's Financial Institutions and White Collar practices:

Lanny Breuer	+1 202 662 5674	lbreuer@cov.com
Arlo Devlin-Brown	+1 212 841 1046	adevlin-brown@cov.com
James Garland	+1 202 662 5337	jgarland@cov.com
Nikhil Gore	+1 202 662 5918	ngore@cov.com
Jeremy Newell	+1 212 841 1296	jnewell@cov.com
Michael Nonaka	+1 202 662 5727	mnonaka@cov.com
Addison Thompson	+1 415 591 7046	athompson@cov.com
D. Jean Veta	+1 202 662 5294	jveta@cov.com
Alan Vinegrad	+1 212 841 1022	avinegrad@cov.com
Neal Modi	+1 202 662 5668	nmodi@cov.com