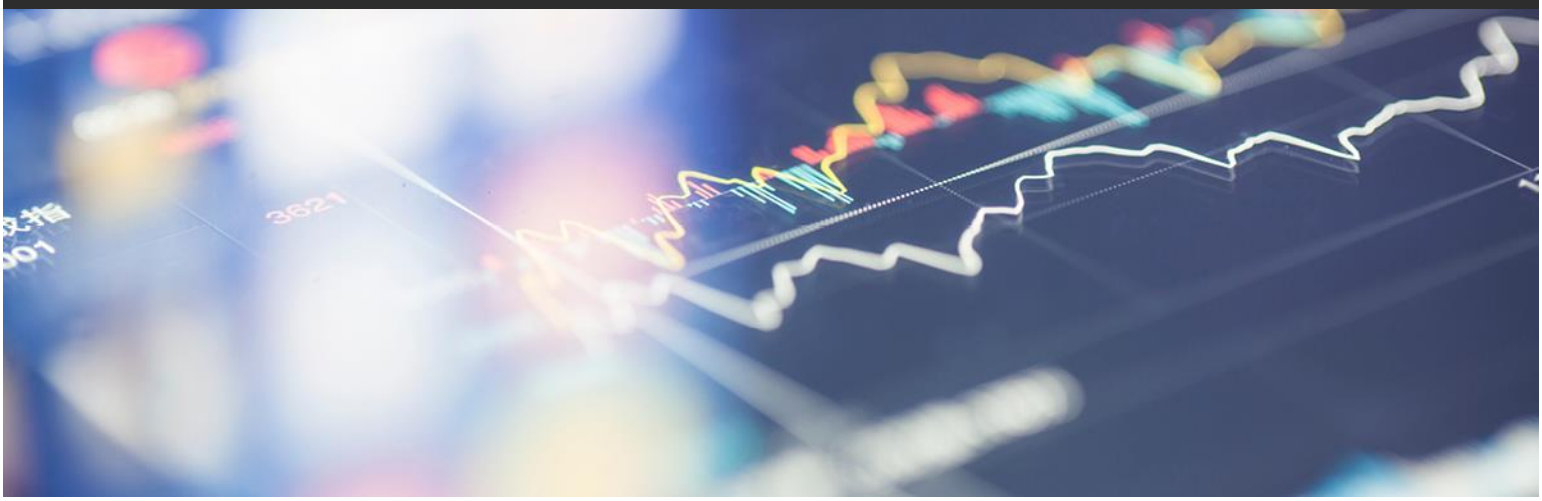
GT GreenbergTraurig

Alert | Financial Regulatory & Compliance/ White Collar Defense & Special Investigations



July 2021

FinCEN Identifies New Anti-Money Laundering (AML) National Priorities

On June 30, 2021, the U.S. Department of the Treasury's Financial Crimes Enforcement Network (FinCEN), in consultation with the U.S. attorney general, federal functional regulators, relevant state financial regulators, and relevant national security agencies, announced new federal anti-money laundering and counter–terrorism financing (AML/CFT) priorities, in accordance with the Anti-Money Laundering Act of 2020 (AML Act). Under the AML Act, once FinCEN promulgates regulations to implement these new AML/CFT priorities—which is expected to occur within the next 180 days—financial institutions that are subject to the Bank Secrecy Act's (BSA's) AML program requirement will need to incorporate these priorities, as appropriate, into their risk-based AML programs, and compliance with this incorporation requirement will be a measure on which financial institutions are examined by their regulators.

The eight AML/CFT priorities identified by FinCEN will look familiar to professionals in the AML compliance space, as they reflect forms of illicit finance that have received frequent attention from FinCEN and other federal regulators in recent years:

1) Corruption. Noting the recent National Security Study Memorandum issued by President Biden on June 3, 2021, FinCEN observes that fighting corruption is now a core U.S. national security interest. Identification of corruption as a top AML priority confirms that the Biden administration will use its regulatory and law enforcement authority to address the ways in which the U.S.

financial system is used to facilitate foreign bribery, misappropriation of public assets, and other forms of destabilizing corruption.

2) 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. Among the forms of cybercrime highlighted by FinCEN as areas of risk for regulated entities are ransomware schemes (including schemes targeting critical infrastructure), compromises of remote applications to facilitate extortion, business email compromise (BEC), and other fraudulent schemes, especially against financial and health care systems. FinCEN also notes the prevalent use of convertible virtual currencies (CVCs) in these types of crimes.

3) Foreign and domestic terrorist financing. FinCEN identifies both foreign and domestic terrorist financing as federal priorities. On the international side, FinCEN notes that most international terrorist groups still primarily rely on banks, money services businesses, and cash couriers to transfer funds, though some regularly seek small dollar donations in digital assets. On the domestic side, FinCEN notes the U.S. intelligence community's assessment that racially or ethnically motivated violent extremists and anti-government violent extremists pose the most lethal domestic threat.

4) Fraud. Fraud—whether consumer, health care, bank, securities and investment, or tax—is believed to generate the largest share of illicit proceeds in the United States. FinCEN notes that fraud schemes are increasingly internet-enabled, and funds are laundered through a variety of methods, including offshore legal entities, accounts controlled by cyber actors, and money mules. FinCEN also singles out for special concern the illicit financial practices of foreign intelligence entities and their proxies to fund influence campaigns and facilitate espionage activity.

5) Transnational criminal organization activity. Transactional criminal organizations (TCOs) are a priority threat due to their crime-terror nexus. FinCEN notes that TCOs commonly use professional money laundering networks to obscure the source of illicit proceeds before introducing those funds into the mainstream economy.

6) Drug trafficking organization activity. FinCEN notes that drug trafficking remains a persistent threat, but it involves greater reliance on professional money laundering networks, including trade-based money laundering, in Asia (primarily China). FinCEN also has seen a substantial increase in money laundering schemes involving the exchange of cash proceeds from Mexican traffickers to Chinese citizens residing in the United States, including the use of front companies or couriers to deposit cash into the banking system.

7) Human trafficking and human smuggling. FinCEN notes that financial activity from human trafficking and human smuggling activities can intersect with the formal financial system at any point during the trafficking or smuggling process, and the illicit proceeds from such activity can include income associated with logistics, such as housing and transportation of victims, as well as earnings from the exploitation of victims. These proceeds are often laundering through shell companies and trade-based money laundering schemes.

8) Proliferation financing. State actors such as Iran, North Korea, and Syria have networks of individuals and entities, including trader brokers and front companies, working on their behalf to exploit the U.S. financial system to acquire weapons of mass destruction or further state-sponsored weapons programs that evade U.S. and U.N. sanctions. According to FinCEN, global

correspondent banking is the principal vulnerability and driver of proliferation financing within the United States.

Contemporaneously with the issuance of these AML/CFT Priorities, FinCEN, jointly with other regulators, released two interagency statements—one directed at banks and another to non-bank financial institutions—to confirm that the release of the AML/CFT Priorities has no immediate effect on covered institutions' obligations under the BSA. **Financial institutions will not be expected to incorporate the priorities into their risk-based AML programs until FinCEN issues final implementing regulations sometime during the latter half of 2021, and bank examiners will not examine for the incorporation of the AML/CFT until the effective date of final revised regulations**. Nonetheless, as FinCEN observes, financial institutions may wish to start considering how they will incorporate the AML/CFT Priorities into their risk-based BSA compliance programs, such as by assessing the potential related risks associated with the products and services they offer, the customers they serve, and the geographic areas in which they operate, in preparation for any new requirements when those final rules are published.

FinCEN will update the Priorities at least once every four years, as required by the AML Act, to account for new and emerging threats to the U.S. financial system and national security.

Authors

This GT Alert was prepared by:

- Carl A. Fornaris | +1 305.579.0626 | fornarisc@gtlaw.com
- Kyle R. Freeny | +1 202.331.3118 | freenyk@gtlaw.com
- Marina Olman-Pal | +1 305.579.0779 | olmanm@gtlaw.com