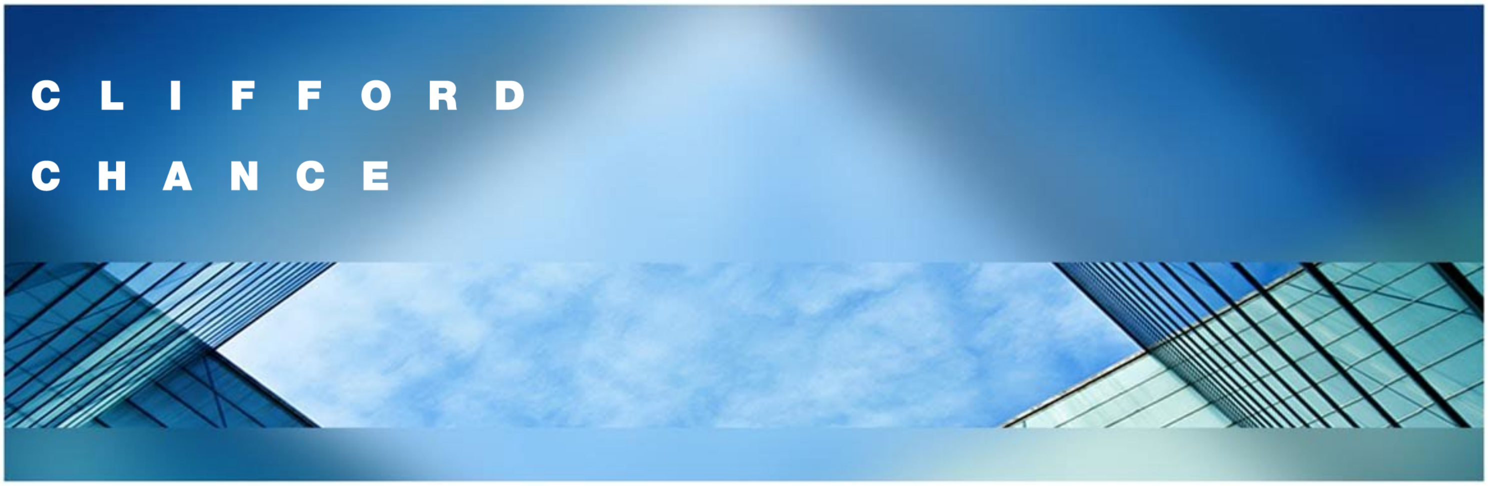


IMPACT OF FINCEN PRIORITIES STATEMENT ON FCPA/ANTI-BRIBERY, CRYPTOCURRENCY, AND EXPORT CONTROLS

The U.S. Department of Treasury's Financial Crimes Enforcement Network ("FinCEN") issued its national priorities in the Government's efforts to combat money laundering and terrorist financing. FinCEN has made statements about priorities in the past, although not pursuant to a statutory mandate. Although still broad, the new statutorily mandated priorities are more specific than those listed by FinCEN around five years ago. FinCEN used to note at the bottom of its enforcement-related press releases that its focus was "on compromised financial institutions and their employees; significant fraud; third-party money launderers; transnational organized crime and security threats; and cyber threats."

Now, instead of a shorter list of catch-all categories, the new FinCEN priorities include both catch-all categories and specific areas of focus, some of which have had more recent exposure, such as domestic terrorism financing, human trafficking, and human smuggling. FinCEN provides details of specific activities of concern in all of the priorities. Whether this means that activities not specified in each category are not priorities is something that FinCEN might need to clarify in the regulations.

These priorities were compiled after consultation with the Department of Treasury's Offices of Terrorist Financing and Financial Crimes ("TFFC") and Foreign Assets Control ("OFAC"), the Attorney General, federal and state financial regulators, and national security agencies.

The priorities are:

- corruption;
- cybercrime;
- foreign and domestic terrorist financing;

Key issues

- FinCEN issued its priorities for AML/CFT in advance of its final rules.
- The priorities include corruption, cybercrime, and digital currencies and their role in facilitating money laundering and terrorist financing.
- FinCEN also emphasizes that the scope of compliance goes beyond just FinCEN's rulemaking and includes compliance with sanctions programs from the Government.

- fraud;
- transnational criminal organization activity;
- drug trafficking organization activity;
- human trafficking and human smuggling; and
- proliferation financing.

Cognizant of client priorities, we provide below an overview of corruption, cybercrime and cryptocurrency aspects, and discuss related export control implications.

A NEW FOCUS ON MONEY LAUNDERING'S EFFECTS ON GLOBAL AND DOMESTIC CORRUPTION

The Government's focus on identifying and eliminating corruption is not new—it is an effort that arguably began in earnest in 1977 with the enactment of the Foreign Corrupt Practices Act ('FCPA"). What is new, however, is the inclusion of combating corruption through AML/CFT means and regulations.

In its statement, FinCEN reiterates what President Biden stated on June 3, 2021, in the National Security Study Memorandum, emphasizing that both foreign and domestic corruption hinders global economic growth, threatens national security, and fuels instability. These were all motivators in passing and amending the FCPA in the past as well. Now, the Government has linked corruption to money laundering, stating that "[c]orrupt 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."

FinCEN advises financial institutions to use the typologies and red flags identified in FinCEN's advisories on human rights abuses in Nicaragua, South Sudan, and Venezuela to comply with Bank Secrecy Act ("BSA") responsibilities and eventual final rules on countering corruption through AML/CFT efforts.

THREATS PRESENTED BY CYBERCRIME AND DIGITAL CURRENCY

With cybercrime on the rise, and with the COVID-19 pandemic presenting more opportunities to criminals, FinCEN is acutely aware of cyber-enabled financial crimes and their threat to supply chains, the U.S. healthcare system, critical infrastructure, national security, and economic prosperity. Fraudulent proceeds from these schemes are often laundered in a few ways, including through close-proximity transfers. Notably, FinCEN states that "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 advises that financial institutions should look towards advisories they have issued on ransomware and COVID-19 related cybercrime to identify trends, typologies, and red flags of cyberthreats and crime. Financial institutions should also consult a recently published fact sheet from FinCEN that encourages sharing AML/CFT strategies under the BSA's safe harbor provision offering protections from civil liability to covered financial institutions.

FinCEN also notes that convertible virtual currencies ("CVCs") are the preferred currency for illicit cyber activity. Our previous alerter on FinCEN's increased scrutiny of cryptocurrencies is available here. Virtual or digital currencies such as bitcoin and ether have facilitated payments from ransomware, child exploitation, and illicit drugs and goods. Criminals may use digital currencies to obscure the origin of funds in their accounts or wallets, utilizing mixers and tumblers to do so. The digital nature of these currencies also facilitates the global reach of criminal activity, whether it's cybercrime or funding for weapons of mass destruction and ballistic missile programs.

FinCEN recommends that financial institutions consult advisories they issued in 2016 and 2019 on cybercrime and virtual currencies to assist financial institutions in their efforts to identify suspicious activity related to CVCs and red flags of cybercrime.

RELATED EXPORT CONTROLS IMPLICATIONS

The Government's notice references relevant export controls and sanctions risks associated with these priorities. In FinCEN's discussion about cybercrime, the Government makes note of an OFAC advisory from 2020 regarding sanctions risks affiliated with making ransomware payments. Our previous alerter on this advisory is available here. FinCEN also points out that OFAC has designated malicious cyber actors under various OFAC sanctions programs because of these actors' efforts targeting the U.S. Government and private sector parties.

Similarly, in its discussion on terrorist financing, FinCEN includes a reminder that as part of their AML compliance programs, financial institutions must abide by sanctions programs and be aware of designated terrorists and terrorist organizations that are on sanctions lists.

As a catch-all, FinCEN reinforces that an essential element of AML/CFT efforts and programs at financial institutions must be in compliance with sanctions lists issued by federal agencies, including OFAC, the Department of Commerce's Bureau of Industry and Security ("BIS"), and the Department of State's Bureau of International Security and Nonproliferation.

KEY TAKEAWAYS

Financial institutions should be cognizant of the purpose and the context for these priorities. For years, FinCEN and industry have been trying to improve the AML regime by moving away from check the box compliance, and instead enabling industry to do its best where it matters most. The same day FinCEN released its priorities, the Wolfsberg Group released a statement on the importance of demonstrating effectiveness in AML programs. The Wolfsberg statement advocates for priority-based effectiveness in AML efforts instead of rote compliance with regulations. The statement essentially invites FinCEN and other regulators to incorporate this concept in the implementation of regulations based on priorities. The Wolfsberg banks and other financial institutions will need to think about how they might demonstrate effective outcomes. Financial institutions, with their counsel, should be prepared to take advantage of a comment period in the rulemaking process.

Expect whatever regulation comes out of the process on demonstrating effectiveness to impose the same or similar requirements in the crypto space as for any other part of the financial sector. FinCEN has repeatedly said that development and use of cryptocurrencies should not result in a retreat from the transparency for AML purposes. Innovators in this part of the financial sector should be reviewing their new products and services with AML effectiveness and transparency in mind. How the rules will apply will require careful analysis and further interaction with FinCEN and counsel, given rapid developments in the space. FinCEN's apparent intent to develop procedures for issuing no-action letters, in addition to its existing treatment of requests for administrative rulings, will provide additional pathways for such engagement. But any requesters for this type of relief will need to think through their requests carefully.

CLIFFORD
CHANCE

CONTACTS

Megan Gordon
Managing Partner

T +1 202 912 5021
E megan.gordon
@cliffordchance.com

David DiBari
Partner

T +1 202 912 5098
E david.dibari
@cliffordchance.com

Renée Latour
Partner

T +1 202 912 5509
E renee.latour
@cliffordchance.com

Michelle Williams
Partner

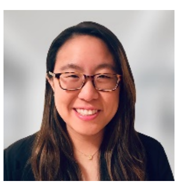
T +1 202 912 5011
E michelle.williams
@cliffordchance.com

Jamal El-Hindi
Counsel

T +1 202 912 5167
E jamal.elhindi
@cliffordchance.com

Philip Angeloff
Counsel

T +1 202 912 5111
E philip.angeloff
@cliffordchance.com



Christine Chen
Associate

T +1 202 912 5081
E christine.chen
@cliffordchance.com