

Debevoise Insight: The Federal Government's Focus on Anti-Money Laundering Compliance Continues

July 12, 2021

The anti-money laundering (“AML”) regulatory landscape continues to evolve quickly, with important [developments](#) seemingly every week – most notably in connection with implementation of the [Anti-Money Laundering Act of 2020](#) (the “AML Act”). In this Debevoise In Depth, we survey and summarize the most recent such developments and provide context about the federal government’s broader efforts to revise the United States’ AML compliance¹ framework.

Publication of National AML Priorities

On June 30, 2021, the Financial Crimes Enforcement Network (“FinCEN”) [issued government-wide AML and countering the financing of terrorism \(“CFT”\) priorities](#) (the “Priorities”), as required by the AML Act. The Priorities were issued with additional statements to [banks](#) and [non-bank financial institutions](#) on their expected use and applicability.

The Priorities do not, in themselves, change compliance obligations for financial institutions but, as also required by the AML Act, FinCEN will issue further regulations addressing how the Priorities should inform AML/CFT compliance efforts. To that end, in its statements accompanying the Priorities, FinCEN noted that institutions “may wish to start considering how they will incorporate” the Priorities into their compliance programs. We discuss each of the priorities in turn below in the order that FinCEN listed them.

Corruption

FinCEN warns financial institutions that bad actors may seek to take advantage of vulnerabilities in the U.S. financial system to launder assets and disguise the proceeds of corrupt activity. According to FinCEN, corruption threatens democracy and contributes to human rights abuses across the globe.

¹ A special thank you to Tejas Dave and Jeremy Lin, summer associates at Debevoise & Plimpton LLP, who contributed to this Debevoise In Depth.

This focus on corruption is not new for FinCEN, which in recent years has issued advisories regarding corruption in [Venezuela](#), [Nicaragua](#) and [South Sudan](#). In these advisories, FinCEN explains various steps that the U.S. government has taken to combat foreign corruption, including the imposition of sanctions, and outlines risk-based efforts that financial institutions should take to limit exposure to funds and assets associated with corruption.

The fight against corruption has been a broader Biden Administration priority. On June 3, 2021, President Biden [issued](#) a [National Security Study Memorandum](#) declaring that combatting corruption is a core national security priority. In so doing, the administration signaled a redoubled emphasis on anti-corruption efforts, including initiatives to shift enforcement resources to the anti-corruption front and strengthen cross-border coordination in investigating such matters.

Cybercrime (including cybersecurity and issues relating to virtual currency)

FinCEN defines cybercrime broadly to include any “illegal activity that involves a computer, another digital device, or a computer network.” Not surprisingly given recent events, the Priorities focus specifically on ransomware as an “acute concern.”

This, too, is not a new area of interest for FinCEN. The Priorities reference, for example, earlier [advisories](#) on ransomware and cyber-assisted frauds perpetuated during the COVID-19 global pandemic.

[Statements](#) by Brian Nelson, the nominee for Treasury Undersecretary for Terrorism and Financial Intelligence, during his June 2021 nomination hearing further underscore that cybercrime and virtual currency are key priority areas for Treasury Department leadership. To that end, FinCEN [announced](#) last week the appointment of the agency’s first-ever Chief Digital Currency Advisor, Michele Korver, who “brings a wealth of digital currency expertise,” including from the U.S. Justice Department’s Criminal Division, showing FinCEN’s further commitment and focus on cybercrime and digital assets.

FinCEN is not the only federal agency focused on cybercrime and the use of Bank Secrecy Act tools to fight cybercrime. On May 12, 2021, the Securities and Exchange Commission (“SEC”) entered into a [settlement order](#) with GWFS Equities (“GWFS”) — the first SEC enforcement action stemming from a failure to report cyber-events. In particular, the SEC enforcement action found that (a) GWFS failed to file suspicious activity reports (“SARs”) in situations where it knew that third parties had attempted to

or in fact had gained access to accounts and (b) many of the SARs that GWFS did file failed to include sufficient information to make the SARs useful.²

Foreign and domestic terrorist financing

The Priorities explain that preventing terrorist financing is, of course, a bedrock goal of the AML/CFT regime and that financial institutions aid in this effort by making effective SAR filings. FinCEN also distinguishes between international and domestic terrorism, the latter of which is a [growing concern](#) across the federal government.

Fraud

FinCEN identifies fraud as the largest single source of illicit proceeds in the United States, and the Priorities encourage financial institutions to remain vigilant in efforts to detect and prevent fraudulent activity. This follows earlier advisories on various types of fraud, including [COVID-19](#) scams and [email compromise](#) schemes.

Transnational criminal and drug trafficking organizations

According to the Priorities, transnational criminal organizations and drug trafficking organizations continue to be “priority threats.” Combatting these organizations has been a longstanding focus of FinCEN and other [federal agencies](#).

With respect to drug trafficking, which FinCEN describes as a “significant public health emergency,” the Priorities explain that schemes to launder the proceeds of drug sales continue to grow more complex. In particular, FinCEN highlights as a growing threat complex schemes deployed by Mexican, Colombian and other drug trafficking organizations that rely on Chinese citizens residing in the United States, who facilitate front companies or use couriers to deposit funds into the U.S. banking system. According to FinCEN, these schemes allow drug trafficking organizations to repatriate proceeds from China to the United States, thus sidestepping Chinese capital flight restrictions.

Human trafficking and human smuggling

FinCEN highlights how human trafficking and smuggling networks use a variety of methods to move illicit proceeds, from cash smuggling by individual victims to professional money laundering networks and criminal organizations. As with other priorities, this is not a new concern for FinCEN; it has issued [several advisories](#) on human trafficking and human smuggling in recent years.

² The settlement order found that GWFS failed to submit nearly 130 SARs and failed to include required information in nearly 297 SARs. According to the SEC, the filed SARs lacked sufficient information to address the questions who, what, when, where, and why, and the SARs did not include data such as URL addresses and IP addresses, which the SEC believes that GWFS possessed.

Proliferation financing

Similar to terrorist financing, FinCEN notes that countering proliferation financing has long been an area of focus—to prevent the U.S. financial system from being used to support the pursuit of weapons of mass destruction and/or the development of state-sponsored weapons programs. As a counter-measure to these potential risks, FinCEN reminds U.S. financial institutions that they must be aware of and comply with economic and trade sanctions administered by the Office of Foreign Assets Control.

Report on the Use of No-Action Letters

The AML Act required FinCEN to draft a report assessing whether it should establish a process for issuing no-action letters. Such letters, which have been deployed for many years by the SEC and other federal regulators, would provide a mechanism for FinCEN to respond to inquiries and concerns regarding specific conduct and provide public guidance on the associated issues.

On June 30, 2021, FinCEN published the required [report](#) and issued an accompanying [press release](#). The agency concluded that no-action letters would be “a useful complement” to FinCEN’s current processes and indicated its intention to conduct a public rulemaking to implement a framework for issuing no-action letters.

FinCEN Implementation of the AML Act

Publication of the AML Priorities and issuance of the report on no-action letters constitute important milestones in the implementation of the AML Act. To this end, FinCEN issued a [press release](#) on June 30, 2021 summarizing these and other “Achievements to Date.” The agency highlights, among other things: publication of an advance notice of proposed rulemaking on the AML Act’s beneficial ownership disclosure provisions; issuance of a notice on trade in antiquities and art; an innovation and emerging technologies briefing for Congress; and creation of subcommittees of the Bank Secrecy Act Advisory Group on innovation and technology and information security and confidentiality.

FFIEC Manual Update

In a development unrelated to implementation of the AML Act of 2020, on June 21, 2021, the Federal Financial Institutions Examination Council (“FFIEC”) [published](#)

additional updates to its BSA/AML Examination Manual, following similar actions in [February 2021](#) and [April 2020](#). This latest installment includes updated sections on: (1) Purchase and Sale of Monetary Instruments Recordkeeping; (2) Special Measures; (3) Reports of Foreign Financial Accounts (“FBAR”); and (4) International Transportation of Currency or Monetary Instruments Reporting (“CMIR”).

As with earlier updates, although many of the revisions were technical, all sections have now been updated to indicate expressly that an institution’s AML controls should be “commensurate with [its] risk profile.” The sections on FBAR and CMIR received the most significant updates; each was nearly entirely rewritten, providing significantly more detail on how examiners will select samples of accounts and transactions when conducting testing of an AML program.

* * *

Please do not hesitate to contact us with any questions.

WASHINGTON, D.C.



Satish M. Kini
smkini@debevoise.com



Andrew Field
afield@debevoise.com



Jonathan R. Wong
jrwong@debevoise.com

NEW YORK



David G. Sewell
dsewell@debevoise.com



Zila Reyes Acosta-Grimes
zracosta@debevoise.com



Brenna Rae Glanville
brglanville@debevoise.com