CLIENT ALERT

FinCEN Issues Major Anti-Money Laundering Act Announcements and Appoints New Chief Digital Currency Advisor

Jul.14.2021

Agency Issues First National Priorities for Anti-Money Laundering and Counter-Terrorist Financing, Completes Assessment on Potential No-Action Letter Process, Provides 180-Day Update on AML Act Implementation, and *Appoints First-Ever Chief Digital Currency Advisor*

On June 30, 2021, the Financial Crimes Enforcement Network ("FinCEN") issued its first-ever Anti-Money Laundering and Countering the Financing of Terrorism National Priorities (the "Priorities"). FinCEN was required to do this by the Anti-Money Laundering Act of 2020 ("AMLA"), enacted on January 1, 2021, as part of the National Defense Authorization Act of 2021. FinCEN identified the following as anti-money laundering ("AML") and countering the financing of terrorism ("CFT") priorities, in no particular order:

- Corruption;
- Cybercrime, including cybersecurity and virtual currency considerations;
- Foreign and domestic terrorist financing;
- Fraud;
- Transnational criminal organization activity;
- Drug trafficking organization activity;
- Human trafficking and human smuggling; and
- Proliferation financing.

FinCEN Acting Director Michael Mosier said that these represent the "most significant AML/CFT threats currently facing the United States." Financial institutions will be required to incorporate these priorities into their AML programs after FinCEN finalizes implementing regulations, which must occur by December 27, 2021. FinCEN and federal and state banking regulators also issued a parallel interagency statement emphasizing that they will not examine banks for incorporation of the Priorities until after FinCEN issues implementing regulations. However, in the interim, these regulators suggest that covered financial institutions may wish to start considering how they will incorporate the Priorities into their AML 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."

On June 30th, FinCEN also announced that it had submitted to Congress its assessment of no-action letters, which the AMLA also required. FinCEN concluded that it should undertake a rulemaking to establish a no-action letter process as a supplement to other forms of guidance and relief available from the agency. On the same day, FinCEN's Acting Director also issued an update on FinCEN's progress implementing the AMLA in the first 180 days following its enactment.

Finally, on July 6, 2021, FinCEN announced that Michele Korver is now serving as the agency's first-ever Chief Digital Currency Advisor. Korver joins FinCEN from the Department of Justice's ("DOJ") Criminal Division, Money Laundering and Asset Recovery Section, where she served as Digital Currency Counsel. According to Acting Director Mosier, Korver will bolster FinCEN's leadership role in the digital currency regulatory space by working with other parties "toward strategic and innovative solutions to prevent and mitigate" illicit practices unique to the virtual currency sector and to maximize its potential for financial expansion.

FinCEN's National AML/CFT Priorities List

FinCEN developed the Priorities in consultation with DOJ, federal and state banking regulators, and relevant national security agencies. The Priorities represent areas for which FinCEN believes covered financial institutions should assess their risk and make appropriate changes to their AML programs to address any such risk. In addition to the implementing regulations that FinCEN must promulgate by the end of December this year, federal banking agencies suggested in their parallel statement that they also may promulgate their own rules to address these Priorities. FinCEN also will update the Priorities every four years, as required by the AMLA, to "account for new and emerging threats to the U.S. financial system and national security." We summarize briefly below the eight Priorities, and points for covered financial institutions to consider in advance of forthcoming regulations. Covered financial institutions should keep in mind that FinCEN's Priorities do not displace existing risks facing covered institutions, who must still implement risk-based AML programs that address risks not covered by the Priorities.

Corruption

FinCEN emphasized points made in President Biden's National Security Study Memorandum issued on June 3, 2021, stating that "[c]orruption, both domestic and foreign, threatens U.S. national security by eroding citizens' faith in government, distorting economies, and weakening democratic institutions." FinCEN said that corrupt actors and their financial facilitators may exploit vulnerabilities in the U.S. financial system to launder the proceeds of crime, including bribes. FinCEN declared the money laundering risks associated with corruption to be a threat to U.S. national security.

Covered financial institutions may wish to consult FinCEN's advisories on human rights abuses enabled by corrupt political figures in Nicaragua, South Sudan, and Venezuela, and determine whether the typologies and red flags identified by FinCEN can assist covered financial institutions in assessing Bank Secrecy Act ("BSA") risks associated with these and other countries. To the extent that a corruption risk is present at a covered financial institution, it may wish to ensure that its AML program addresses it. This includes risks associated with politically-exposed persons (referred to in BSA rules as "senior foreign political figures)".

Cybercrime, including Relevant Cybersecurity and Virtual Currency Considerations

FinCEN broadly defines cybercrime as "any illegal activity that involves a computer, another digital device, or a computer network." FinCEN explains that covered financial institutions are "attractive targets" to criminals, including terrorists and state actors, and that cybercriminals may target covered institutions' websites, systems, and employees to unlawfully obtain access credentials and proprietary information, engage in fraud, and disrupt business operations. FinCEN expressed particular concern about cyber-enabled financial crime, ransomware attacks, and misuse of virtual assets (or cryptocurrencies) to launder criminal proceeds.

FinCEN directed financial institutions to its previous advisories on ransomware and COVID-19 related cybercrime for information on the trends and typologies of cybercrime, including phishing, remote application compromise, and business email compromise, particularly involving financial and health care systems. FinCEN noted that covered institutions are uniquely positioned to identify cybercrime-related suspicious activity and encouraged them to lawfully share that information with other financial institutions under the BSA.

FinCEN indicated that ransomware is a "particularly acute concern," and that countering ransomware is a "top priority" for the U.S. government. In particular, FinCEN noted a dramatic rise in the scale and sophistication of ransomware attacks from 2020 to 2021, and that these sometimes are associated with adversary regimes and sanctioned parties. FinCEN pointed out that ransomware attacks now pose a national security threat to U.S. health care systems and other "critical infrastructure," as well as a threat to the U.S. economy (see our alerts last month on the evolution of ransomware from a cybersecurity issue to a financial crimes and national security threat and the need for ransomware response plans). FinCEN and the Treasury Department's Office of Foreign Assets Control ("OFAC") both issued advisories in October 2020 highlighting sanctions and AML risks associated with ransomware payments. Among other risks, FinCEN recognized that convertible virtual currencies ("CVCs") are a "substantial financial innovation" but are the preferred payment method for ransomware-related activities, child exploitation, and illegal drugs. OFAC, for its part, noted that sanctioned persons are increasingly involved in ransomware attacks, and that paying ransoms to such parties may result in liability.

Given FinCEN's increased prioritization of cybercrime, and in particular the use of virtual currency to further it, covered institutions may wish to ensure that they have fully incorporated FinCEN's guidance on reporting suspicious activity involving cyber-events, and including cyber-related information in all suspicious activity reports ("SAR"), and its guidance for SAR filing relating to cybercrime (in 2016) and virtual currency (in 2019). Separately, covered institutions may wish to consider including specific consideration of cybercrime in their AML risk assessments, and establishing methods for dealing with the information problems associated with virtual currency transactions. Finally, they may wish to pay attention in particular to transactions that appear to represent ransomware payments, and the risks that such payments may involve sanctioned persons or jurisdictions.

Terrorist Financing: International & Domestic

FinCEN reminded covered financial institutions of their existing obligations to report suspicious activity involving potential terrorist financing transactions, including appropriately identifying those transactions that may require immediate attention. FinCEN declared the prevention of terrorist financing as "essential to counter the threat of terrorism successfully." Covered institutions should ensure their AML/CFT programs include an up-to-date sanctions compliance component, including sanctions screening against government lists and country-based sanctions. For international terrorism, FinCEN identified the Islamic State of Iraq and Syria ("ISIS"), Al Qaeda, Lebanese Hizballah, and Iran's Islamic Revolutionary Guard Corps ("IRGC") as key threats. FinCEN focused on the funding of overseas terrorists and terrorist groups from the U.S. through banks, money services businesses, and cash couriers, but also highlighted that small-dollar donations in virtual assets were becoming a more regular form of support. FinCEN also noted a movement away from complex attacks toward less sophisticated attacks by self-radicalized and "homegrown" attackers. FinCEN also, for the first time ever, described the threat posed by domestic terrorism, noting that such activity can be based on purported political or religious beliefs to support criminal activities, and that some groups have focused on "accessible targets" such as "civilians, law enforcement and the military, symbols or members of the U.S. government, houses of worship, retail locations, and mass public gatherings." Covered financial institutions may wish to

evaluate their AML programs to account for these evolving international terrorist financing typologies and to consider methods to detect and report potential domestic terrorist financing.

Fraud

FinCEN stated that fraud, in particular "bank, consumer, health care, securities and investment, and tax fraud—is believed to generate the largest share of illicit proceeds in the United States," exceeding other types of crime such as drug trafficking and human smuggling. Fraud schemes are more commonly Internet-enabled, and the proceeds of such schemes may be laundered through offshore legal entities, accounts controlled by cyber criminals, and money mules. FinCEN also highlighted the use of fraud by foreign intelligence agencies and their proxies to influence political campaigns and to facilitate espionage activity, such as establishing front companies and gaining access to sensitive information on U.S. individuals, technology, and intellectual property. FinCEN directed financial institutions to its earlier advisories on COVID-19 related fraud and business email compromise ("BEC") fraud. In addition to reviewing this Priority and ensuring that they have addressed the related risks in their AML programs, covered financial institutions may wish to consider whether their AML programs can detect fraud involving foreign intelligence actors. Further, covered financial institutions may wish to evaluate the interaction between their AML/CFT group and their fraud organizations to ensure potentially fraudulent activity is appropriately reported as suspicious activity. FinCEN previously has identified the failure to do so as the basis for significant civil penalties.

Transnational Criminal Organization Activity, Drug Trafficking Organization Activity, and Human Trafficking and Human Smuggling

FinCEN noted that Transnational Criminal Organizations ("TCOs"), including drug trafficking organizations ("DTOs"), represent "priority threats" due to their involvement in a wide range of criminal activities, including, among other illicit activities, cybercrime, drug trafficking, fraud, human smuggling, and weapons trafficking. FinCEN pointed to Mexican and Russian TCOs as being active in the United States, with TCOs in Africa and Asia becoming more relevant. FinCEN stated that these organizations increasingly use professional money laundering networks that launder proceeds generated by others, without regard to the predicate criminal activity. It also noted that certain states host these groups, under a variety of arrangements, enabling activities that destabilize other jurisdictions.

FinCEN highlighted that Mexican and Colombian DTOs continue to operate sophisticated schemes to import illegal drugs into the United States, and that DTOs also launder their criminal proceeds through the United States. Increasingly, FinCEN said, DTOs rely more on Asia-based professional money laundering networks to facilitate the exchange of U.S. and Chinese currency, or to serve as currency brokers in trade-based money laundering schemes. With respect to human smuggling and human trafficking, FinCEN noted that these organizations use professional money launderers as well, and may have logistics-based criminal proceeds derived from the housing and transportation of victims. Covered financial institutions may wish to consider which of these threats affect their institutions and which of the described typologies may be relevant, and to address these in their AML programs.

Proliferation Financing

FinCEN's final Priority is proliferation financing by those who seek to "exploit the U.S. financial system to move funds that will be used either: (1) to acquire weapons of mass destruction or delivery systems or their components; or (2) in the furtherance or development of state-sponsored weapons programs, including the evasion of United Nations or U.S. sanctions." FinCEN noted

that global correspondent banking is a "principal vulnerability and driver" of proliferation financing risk in the United States. FinCEN encouraged covered financial institutions to review previous advisories issued by the Treasury Department (including both FinCEN and OFAC) regarding proliferation financing risk. Covered financial institutions may wish to ensure that their risk-based AML programs account for the various economic and trade sanctions administered by OFAC, the Department of Commerce's Bureau of Industry and Security, and the Department of State's Bureau of International Security and Nonproliferation.

FinCEN's Assessment on the Use of No-Action Letters

FinCEN completed its assessment (the "Assessment") "on whether to establish a process for the issuance of no-action letters in response to inquiries concerning the application of [AML/CFT] laws and regulations to specific conduct," including as to whether FinCEN or a functional regulator intends to bring an enforcement action with respect to such conduct. FinCEN concluded that it should undertake a rulemaking to establish a FinCEN-specific no-action letter process to supplement forms of regulatory guidance and relief it currently offers. In reaching its conclusion, FinCEN consulted with numerous state and federal banking regulators, including the Federal Reserve and Office of the Comptroller of the Currency, as well as the DOJ and the Commodity Futures Trading Commission.

While it remains to be seen what no-action letter process FinCEN ultimately adopts, this appears to be a welcome development for covered financial institutions, fintechs, and companies operating in the digital assets space. These entities – particularly those considering offering novel and innovative products and services – may benefit from additional opportunity to engage with FinCEN on proposed or current activities and to receive definitive statements that FinCEN will not take enforcement action.

Historically, no-action letters are generally issued by a federal regulatory agency, through which the agency states that it does not plan to take enforcement action against a submitting party for the specific conduct described by the submitting party. Currently, FinCEN offers two forms of regulatory guidance or relief: (1) administrative rulings; and (2) exceptive or exemptive relief. An administrative ruling is a written determination by FinCEN "interpreting the relationship between [Title 31 of the Code of Federal Regulations, Chapter X] and each situation for which such a ruling has been requested," provided it meets certain requirements. Administrative rulings are binding on FinCEN if there is a specified situation addressed and it also has precedential value for others who may wish to rely on it, but only if FinCEN makes the administrative ruling public. If the ruling is not publicized by FinCEN, then the ruling has no precedential value for similarly-situated parties. Exceptive relief, on the other hand, is a decision by FinCEN to grant an exemption, or exception, from the requirements of Chapter X. Exceptive relief is not precedential, applies only to certain transactions or types of transactions, and may be revoked by FinCEN or the Treasury Secretary. A no-action letter would represent a new form of regulatory relief from FinCEN, in that FinCEN would exercise its enforcement discretion to determine "that it would not take an enforcement action against the submitting party for engaging in the specific conduct described in the request."

As part of the Assessment, FinCEN also considered whether any no-action letter process would include a statement as to whether other "relevant Federal functional regulators" would take an enforcement action. This is important because many federal financial regulators have parallel authorities that they use to enforce compliance with the requirements of the BSA. FinCEN concluded that it lacked the authority to make statements about the enforcement authorities of other agencies. Conversely, FinCEN noted that coordinating with such agencies to issue joint statements in response to every request it received might unduly delay the granting of relief from rules administered by FinCEN. At the same time, FinCEN recognized that federal

functional regulators, as well as the DOJ and state regulators, may in particular cases be affected by, and thus have a stake in, how FinCEN rules. The agency decided to pursue an approach of consulting with these agencies on a discretionary, *ad hoc* basis as appropriate.

While FinCEN provided some initial estimates for a no-action letter process, such as 90 to 120 days for straightforward requests, it said that any timing for issuing a no-action letter could be impacted if it and other regulators disagree on whether FinCEN should issue a no-action letter or the scope of such a letter. FinCEN also noted current resources limitations also could delay any no-action process, and that, absent additional resources, it would not be able to process such requests in a reasonable timeframe without impacting other FinCEN work. It pointed out that that other agencies sometimes took months to more than a year to issue no-action letters, depending on the complexity of the request.

While FinCEN did not state when it might commence a rulemaking process for a no-action letter procedure, it indicated that it will provide opportunity for public comment. Covered institutions and those who are contemplating engaging in BSA-regulated activity may wish to consult with counsel and submit comments reflecting business or industry concerns.

FinCEN's AMLA 180-Day Update

In its 180-day update, FinCEN highlighted several of the agency's achievements since the passage of the AMLA, including the issuance of the AML/CFT Priorities and its No-Action Letter Assessment. FinCEN said that it will continue to issue additional regulations required under the AMLA, and institutions should anticipate further rulemaking regarding, among other things, a beneficial ownership database, the potential application of the BSA to the arts and antiquities trade, and digital assets and virtual currencies.

FinCEN's New Chief Digital Currency Advisor

By appointing Michelle Korver as FinCEN's first-ever Chief Digital Currency Advisor, FinCEN has further bolstered its virtual assets expertise. FinCEN already is unusual in having a chief officer, Acting Director Michael Mosier, with extensive work experience in the digital assets sector.

While at the DOJ, Korver was a key advisor on digital currency matters, investigations, and charging decisions. She served as a contributor to the DOJ's first-ever Cryptocurrency Enforcement Framework, which set forth various threats posed by virtual currencies, the current legal regime applicable to virtual currencies, and challenges and strategies for enforcement against unlawful activity involving virtual currencies. Korver also served as a U.S. delegate to the Financial Action Task Force, which is currently addressing virtual assets and virtual asset service providers, and developed cryptocurrency seizure and forfeiture policy and legislation.

FinCEN has been one the most active regulators of virtual currency, and the addition of Korver suggests a desire to continue that trend. It remains to be seen if Korver's move to FinCEN also reflects an intent to bring a more "prosecutorial" mindset to virtual currency enforcement. Virtual asset companies or those considering entering into the space may wish to consult with counsel to ensure their operations or proposed operations comply with the AMLA and FinCEN's virtual currency guidance, and also account for FinCEN's recently announced Priorities.

For more information, please contact the professional(s) listed below, or your regular Crowell & Moring contact.

Caroline E. Brown
Partner – Washington, D.C.
Phone: +1 202.624.2509
Email: cbrown@crowell.com

Kelly T. Currie
Partner – New York
Phone: +1 212.895.4257
Email: kcurrie@crowell.com

Carlton Greene
Partner – Washington, D.C.
Phone: +1 202.624.2818
Email: cgreene@crowell.com

Rebecca Monck Ricigliano
Partner – New York
Phone: +1 212.895.4268
Email: rricigliano@crowell.com

Anand Sithian
Counsel – New York
Phone: +1 212.895.4270
Email: asithian@crowell.com

Nicole Sayegh Succar
Counsel – New York
Phone: +1 (212) 803-4031
Email: nsuccar@crowell.com