WILMERHALE

FinCEN Publishes No-Action Letter Analysis and AML/CFT National Priorities

JULY 15, 2021

The Financial Crimes Enforcement Network ("FinCEN") has continued a spate of regulatory activity related to financial crimes compliance matters in the first year of the Biden Administration,[1] recapped in its recent report detailing progress in the first 180 days since Congress' passage of the Anti-Money Laundering Act of 2020 (the "AML Act").[2] Of note, in late June 2021, FinCEN announced the completion of two key deliverables required by the AML Act:

- First, FinCEN's report determining it may undertake rulemaking to create a no-action letter issuance process in at least some form, despite practical challenges involved in the endeavor.[3]

[1] *See* Press Release, FinCEN, *Message from the FinCEN Director: 180-Day Update on AML Act Implementation* (June 30, 2021), https://www.fincen.gov/news/news-releases/message-fincen-director-180-day-update-aml-act-implementation; Press Release, FinCEN, *FinCEN Statement on Financial Crimes Tech Symposium* (Feb. 4, 2021), https://www.fincen.gov/news/news-releases/fincen-statement-financial-crimes-tech-symposium; FinCEN, FIN-2021-NTC2, FinCEN Informs Financial Institutions of Efforts Related to Trade in Antiquities and Art (Mar. 9, 2021), https://www.fincen.gov/sites/default/files/2021-03/FinCEN%20Notice%20on%20Antiquities%20and%20Art_508C.pdf; Press Release. FinCEN, *FinCEN Exchange Brings Together Public and Private Stakeholders to Discuss Bank Secrecy Act Suspicious Activity Reporting Statistics* (Mar. 23, 2021), https://www.fincen.gov/news/news-releases/fincen-exchange-brings-together-public-and-private-stakeholders-discuss-bank; FinCEN, Innovation Honors Program: Emerging Themes and Future Role in AML Act Implementation (Mar. 2021), https://www.fincen.gov/sites/default/files/2021-03/FinCEN%20IH%20Prgm%20Public%20Report%20508C.pdf; Press Release, FinCEN, *FinCEN Launches Regulatory Process for New Beneficial Ownership Reporting Requirement* (Apr. 1, 2021), https://www.fincen.gov/news/news-releases/fincen-launches-regulatory-process-new-beneficial-ownership-reporting.

[2] More information about AML developments can be found in a related WilmerHale client alert. WilmerHale, *2021 AML Trends and Developments* (Feb. 11, 2021), https://www.wilmerhale.com/en/insights/client-alerts/20210211-2021-aml-trends-and-developments.

[3] FinCEN, A Report to Congress: Assessment of No-Action Letters in Accordance with Section 6305 of the Anti-Money Laundering Act of 2020 (June 28, 2021) [hereinafter *FinCEN No-Action Letter Assessment*], https://www.fincen.gov/sites/default/files/shared/No-Action%20Letter%20Report%20to%20Congress%20per%20AMLA%20for%20ExecSec%20Clearance%20508.pdf

- Second, FinCEN's establishment of national policy priorities within anti-money laundering ("AML") and counter-financing of terrorism ("CFT").[4]

These developments carry important implications for financial institutions. For example, a no-action letter process could pave a new avenue for obtaining clearer, potentially precedential guidance from FinCEN on a more abbreviated timeline than is available through requests for administrative rulings or exceptive or exemptive relief. Financial institutions potentially stand to gain from commenting in FinCEN's rulemaking process, whether individually, or in partnership with industry associations, by shaping the potential no-action letter process in a manner responsive to concerns of financial institutions.

Financial institutions would also be wise to begin promptly reassessing AML and CFT compliance programs in light of FinCEN's national policy priorities, as FinCEN and the federal banking and securities regulators will expect appropriate enhancements where warranted. Financial institutions should especially ensure their AML/CFT compliance programs' functions to detect and report suspicious activity are able to internalize the priorities FinCEN has highlighted.

WilmerHale regularly advises leading financial institutions on developments in the AML/CFT regulatory environment. We are available to advise clients on potential engagement with government agencies involving pending regulations such as a novel no-action letter process, and on appropriate enhancements to compliance programs in the wake of FinCEN's published priorities.

FinCEN Will Institute a No-Action Letter Program

FinCEN has determined that it may be feasible to "establish a no-action letter process through rulemaking" while noting practical caveats, especially that "sufficient resources" must be made available to render such a process practical.[5] The no-action letter process may also provide financial institutions a path to obtaining FinCEN's consent before launching the innovative approaches to financial crimes compliance that FinCEN has recently hailed.[6] All financial institutions—especially those contemplating changes to their AML compliance programs (*e.g.*, a novel approach to transaction monitoring)—may avail themselves of such a process. However, it could be especially beneficial for fintech companies seeking no-action relief, such as those wishing to understand if they are engaged in money transmission. Although the federal banking and securities regulators would likely not be bound by these determinations, FinCEN is the agency

[4] *See* FinCEN, Anti-Money Laundering and Countering the Financing of Terrorism National Priorities (June 30, 2021) [hereinafter *FinCEN Priorities*], https://www.fincen.gov/sites/default/files/shared/AML_CFT%20Priorities%20(June%2030%2C%202021).pdf.
[5] *FinCEN No-Action Letter Assessment*, *supra* note 3, at 14.
[6] *See generally 2021 AML Trends and Developments*, *supra* note 2.

charged with interpreting the Bank Secrecy Act ("BSA"), so its views are likely to carry significant weight.

On June 28, 2021, FinCEN presented to the Senate Committee on Banking, Housing, and Urban Affairs and the House Committee on Financial Services its assessment of whether to establish a no-action letter issuance process in response to AML/CFT inquiries, including concerning the application of the BSA.[7] A FinCEN no-action letter would communicate that FinCEN does not intend to bring an enforcement action against the submitting party for some specified conduct. However, FinCEN notes that such letters would generally only address the submitting party's prospective activity, which may present some limit to their precedential value.[8]

FinCEN consulted with several federal and state agencies[9] and made findings that indicate some likely characteristics of its future potential no-action letter program. The report concluded that a no-action letter process could be beneficial, though most likely effective and workable only if limited to FinCEN's exercise of its own enforcement authority, rather than also addressing other regulators' exercise of enforcement authority. FinCEN's process would likely include "consultation with other agencies as needed and appropriate" because its letters could affect agencies with similar authority, and such consultation would serve as a bulwark against significant "legal and practical challenges."[10] As a result, FinCEN no-action letters, while not binding on other agencies, may help to provide broader indicia of regulators' dispositions toward raised conduct.

Given the need for feedback from other agencies, FinCEN anticipates that its timeline for no-action letters could still be relatively long, ranging from 90 or 120 days for simpler cases to several months or even over a year for more complex cases. Delays may arise due to disagreement among regulators, insufficient facts from submitting parties, and/or insufficient resources at the agency.

Financial institutions intending to take advantage of FinCEN's no-action letter program will need to understand its abilities and limitations, once determined, and create a strategy to use the process to maximum effect based on such considerations. Despite the caveats, however, a FinCEN no-action letter could be an important clue in assessing whether planned actions and developments will likely be consistent with future interpretations of the BSA and other AML and CFT regulations. While FinCEN's report signals its current thinking on the contours of such a program, FinCEN has also indicated that it may alter the program after considering input during its rulemaking process.

---

[7] *FinCEN No-Action Letter Assessment*, *supra* note 3.
[8] *Id*. at 2.
[9] FinCEN consulted with the Board of Governors of the Federal Reserve System (FRB), the Office of the Comptroller of the Currency (OCC), the Federal Deposit Insurance Corporation (FDIC), the National Credit Union Administration (NCUA), the Securities and Exchange Commission (SEC), the Commodity Futures Trading Commission (CFTC), the Internal Revenue Service (IRS), the Attorney General (DOJ); the Consumer Financial Protection Bureau (CFPB), state bank supervisors, and state credit union Supervisors. *Id*. at 3.
[10] *Id*. at 6-7.

Financial institutions will likely benefit from engaging in the rulemaking process—including through a trade association—to suggest optimal characteristics for the program.

Anti-Money Laundering and Countering the Financing of Terrorism National Priorities

On June 30, 2021, FinCEN established national priorities for AML/CFT policy as required under the AML Act (the "Priorities").[11] This is the first time that FinCEN has published priorities, which are intended to reflect the most significant money laundering and national security threats facing the U.S. and permit financial institutions to prioritize compliance resources in light of the Priorities. The Priorities reflect key policy judgments from the U.S. government about the most significant money laundering threats to the U.S. and, as such, serve as a roadmap for financial institutions to ensure they have adequately developed controls to account for these threats and the risks they pose to AML/CFT compliance. FinCEN will revise the Priorities, at minimum, every four years to account for changing threats.

FinCEN, federal banking agencies, and state bank and credit union regulators issued a statement to clarify how the Priorities will affect banks.[12] FinCEN also issued a parallel statement to clarify how the Priorities affect non-bank financial institutions ("NBFIs").[13] The Priorities have not yet changed financial institutions' BSA obligations, but FinCEN will promulgate regulations within 180 days of issuing the Priorities and federal banking agencies will revise their regulations to incorporate the Priorities into financial institutions' respective BSA requirements. When the final revised regulations become effective, financial institutions will be required to incorporate the Priorities into their compliance programs and will be supervised and examined on this measure.

While more prescriptive regulations should be forthcoming, the statements to financial institutions put them on notice that they will be supervised and examined on the core basis of the Priorities[14] and that they should begin considering how the Priorities will be incorporated into their risk-based AML programs.[15]

---

[11] *FinCEN Priorities*, *supra* note 4.
[12] Board of Governors of the Federal Reserve System et al., Interagency Statement on the Issuance of the Anti-Money Laundering/Countering the Financing of Terrorism National Priorities (June 30, 2021) [hereinafter *Statement for Banks*], https://www.fincen.gov/sites/default/files/shared/Statement%20for%20Banks%20(June%2030%2C%202021).pdf.
[13] FinCEN, Statement on the Issuance of the Anti-Money Laundering/Countering the Financing of Terrorism (AML/CFT) National Priorities (June 30, 2021) [hereinafter *Statement for NBFIs*], https://www.fincen.gov/sites/default/files/shared/Statement%20for%20Non-Bank%20Financial%20Institutions%20(June%2030%2C%202021).pdf.
[14] *See Statement for Banks*, *supra* note 12, at 2 ("Finally, the AML Act requires that the review by a bank of the AML/CFT Priorities and the incorporation of those priorities, as appropriate, into its risk-based BSA compliance program, be included as a measure on which a bank is supervised and examined."); *Statement for NBFIs*, *supra* note 13, at 2.
[15] *See Statement for Banks*, *supra* note 12, at 2 ("Nevertheless, in preparation for any new requirements when those final rules are published, banks 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

Priorities

- **Corruption.** Corrupt actors and their "financial facilitators"[16] seek to leverage vulnerabilities in the U.S. financial system to launder their assets or hide crime proceeds. FinCEN recommends that financial institutions use FinCEN's jurisdiction-based advisories on human rights abuses to help comply with BSA requirements, though it notes that the "jurisdictions noted in those advisories are not the only ones at risk of corruption."[17] Corruption has clearly developed as an area of focus across government agencies. As referenced in the Priorities, the Biden Administration established in early June that countering corruption is "a core United States national security interest," suggesting that there has been a government-wide harmonization of this compliance and enforcement priority.[18] This development underscores the convergence of compliance across the key areas of AML, sanctions, and anti-corruption risk.

- **Cybercrime.** FinCEN defines cybercrime "as any illegal activity that involves a computer, another digital device, or a computer network," including social engineering, network attacks, and ransomware attacks.[19] Cybercriminals target U.S. financial institutions to gain access to proprietary information, defraud institutions and their customers, and harm ongoing business functions. During the COVID-19 pandemic, criminals have taken advantage of pandemic-fueled increases in online traffic to increasingly target covered institutions with phishing attacks and to compromise remote applications to execute fraudulent schemes. FinCEN has placed greater emphasis on its earlier recommendation for covered institutions that observe suspicious activity—such as laundering the proceeds of cybercrime—to share the information with each other via Section 314(b).[20] Covered financial institutions should note that FinCEN views them as "uniquely positioned" to observe cyber-enabled financial crime and related suspicious activity.[21]

---

associated with the products and services they offer, the customers they serve, and the geographic areas in which they operate."); *Statement for NBFIs*, *supra* note 13, at 2.

[16] *FinCEN Priorities*, *supra* note 4, at 3.

[17] *Id.*; *See also* FinCEN, FIN-2018-A005, Advisory to Financial Institutions on the Risk of Proceeds of Corruption from Nicaragua (Oct. 4, 2018), https://www.fincen.gov/sites/default/files/advisory/2018-10-04/Nicaragua_Advisory_FINAL_508_0.pdf; FinCEN, FIN-2017-A004, Advisory on Political Corruption Risks in South Sudan (Sept. 6, 2017), https://www.fincen.gov/sites/default/files/advisory/2017-09-06/South%20Sudan%20Advisory_09-06-2017_0.pdf; FinCEN, FIN-2017-A006, Advisory on Widespread Public Corruption in Venezuela (Sept. 20, 2017), https://www.fincen.gov/sites/default/files/advisory/2017-09-20/FinCEN%20Advisory%20FIN-2017-A006-508%20Compliant.pdf.

[18] The White House, Memorandum on Establishing the Fight Against Corruption as a Core United States National Security Interest (June 3, 2021), https://www.whitehouse.gov/briefing-room/presidential-actions/2021/06/03/memorandum-on-establishing-the-fight-against-corruption-as-a-core-united-states-national-security-interest.

[19] *FinCEN Priorities*, *supra* note 4, at 4.

[20] *See* Press Release, FinCEN, *FinCEN Director Emphasizes Importance of Information Sharing Among Financial Institutions* (Dec. 10, 2020), https://www.fincen.gov/news/news-releases/fincen-director-emphasizes-importance-information-sharing-among-financial.

[21] *FinCEN Priorities*, *supra* note 4, at 4.

Ransomware is identified as an "acute concern," as attacks have "increased dramatically in 2020 and 2021 in both scale and sophistication."[22] FinCEN and the U.S. Treasury Department's Office of Foreign Assets Control issued twin advisories in 2020 highlighting risks around ransomware payments, including potential sanctions risks.[23] In thinking through whether to make such payments—or process such payments made by others—covered financial institutions should carefully consider all dimensions and risks, including by reviewing our client alert, *2021 AML Trends and Developments,* available here.

In the Priorities, FinCEN also identified convertible virtual currencies ("CVCs") as "the currency of preference in a wide variety of online illicit activity."[24] CVCs can be used to obscure the origin of illicitly obtained funds. Such currencies enjoyed a spectacular (albeit volatile) increase in value and popularity last year, fueling increased demand and commensurately larger opportunities for bad actors to use them as vehicles for malfeasance. FinCEN recommends that covered institutions review its advisory on how to identify and report suspicious use of CVCs, including by increasing attention to analysis of blockchain history and metadata associated with wallets used for cryptocurrency transactions.[25]

- **Terrorist financing.** International and domestic terrorism "has evolved significantly" since the September 11 terrorist attacks.[26] FinCEN has highlighted both international terrorism and domestic terrorism (including white-supremacist and anti-government activities) within this priority. Covered institutions have an existing obligation to help prevent terrorist financing by identifying and filing Suspicious Activity Reports on potential terrorist financing activity; however, as terrorism has evolved, its definition has expanded. Covered financial institutions should consider ways to address necessary changes to AML compliance programs given this expanded definition, particularly to the extent that their services may be used by perpetrators of domestic terrorism, as evidenced by the events of the past year. Regarding international terrorism, FinCEN again emphasized the connectivity with sanctions compliance, noting covered financial institutions' continued responsibilities.
- **Fraud.** Fraud—which has increasingly become internet-enabled—is believed to "generate the largest share of illicit proceeds in the United States," and its proceeds may be

---

[22] *Id*. at 5. For more information about ransomware developments, *see* WilmerHale, *Ransomware Attacks—Financial Crimes Compliance Requirements* (Oct. 8, 2020), https://www.wilmerhale.com/en/insights/client-alerts/20201008-ransomware-attacks-financial-crimes-compliance-requirements.
[23] *See* U.S. Dep't of Treasury, Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments (Oct. 1, 2020), https://home.treasury.gov/system/files/126/ofac_ransomware_advisory_10012020_1.pdf; FinCEN, FIN-2020-A006, Advisory on Ransomware and the Use of the Financial System to Facilitate Ransom Payments (Oct. 1, 2020), https://www.fincen.gov/sites/default/files/advisory/2020-10-01/Advisory%20Ransomware%20FINAL%20508.pdf.
[24] *FinCEN Priorities*, *supra* note 4, at 5.
[25] *Id.*, Press Release, U.S. Dep't of Treasury, *Treasury Sanctions Individuals Laundering Cryptocurrency for Lazarus Group* (Mar. 2, 2020), https://home.treasury.gov/news/press-releases/sm924.
[26] *FinCEN Priorities*, *supra* note 4, at 6.

laundered through offshore accounts, accounts controlled by cyber actors, or money mules.[27] Covered institutions should review FinCEN's fraud-related advisories.[28] NBFIs should be especially careful in this area because gift cards and other forms of electronic money transmission have increased opportunities for fraud, given the speed and relative anonymity of their transactions.

- **Transnational criminal organization activity.** Transnational criminal organizations engage in a variety of illegal activities, including cybercrime, human trafficking, and corruption. These organizations frequently use professional money laundering networks that receive a commission for their services.[29] Covered financial institutions should ensure that their AML compliance programs are adequate to address this issue, particularly because organizations are using increasingly professional and sophisticated means to launder proceeds of illicit activities.

- **Drug trafficking organization ("DTO") activity.** There is significant drug trafficking activity from Mexican and Chinese organizations. DTOs also use professional money laundering networks in Asia, including complex schemes that involve transferring funds from Mexican DTOs to Chinese citizens living in the U.S.[30] Covered financial institutions should review FinCEN's advisory about drug trafficking, which include case studies and discussions of red flags.[31]

- **Human trafficking and human smuggling.** Human trafficking and smuggling networks can use cash smuggling and professional money laundering networks to move their illicit proceeds. Particularly given the increased migration at the U.S.-Mexico border in the past year and subsequent overwork of border enforcement personnel, opportunities for human smuggling have greatly increased. Furthermore, these cartels are increasingly interacting with the formal financial system by using ever-more sophisticated shell companies and funnel accounts.[32] Covered institutions should consult FinCEN's advisories, which contain red flags associated with human trafficking and human smuggling.[33]

---

[27] *Id*. at 8.
[28] *See* FinCEN, FIN-2016-A003, Advisory to Financial Institutions on E-Mail Compromise Fraud Schemes (Sept. 6, 2016), https://www.fincen.gov/sites/default/files/advisory/2016-09-09/FIN-2016-A003.pdf; FinCEN, FIN-2019-A005, Updated Advisory on Email Compromise Fraud Schemes Targeting Vulnerable Business Processes (July 16, 2019), https://www.fincen.gov/sites/default/files/advisory/2019-07-16/Updated%20BEC%20Advisory%20FINAL%20508.pdf.
[29] *FinCEN Priorities*, *supra* note 4, at 10.
[30] *Id.*
[31] *See* FinCEN, FIN-2019-A006, Advisory to Financial Institutions on Illicit Financial Schemes and Methods Related to the Trafficking of Fentanyl and Other Synthetic Opioids (Aug. 21, 2019), https://www.fincen.gov/sites/default/files/advisory/2019-08-21/Fentanyl%20Advisory%20FINAL%20508.pdf
[32] *FinCEN Priorities*, *supra* note 4, at 11.
[33] *See* FinCEN, FIN-2014-A008, Advisory: Guidance on Recognizing Activity that May be Associated with Human Smuggling and Human Trafficking – Financial Red Flags (Sept. 11, 2014), https://www.fincen.gov/sites/default/files/advisory/FIN-2014-A008.pdf; FinCEN, FIN-2020-A008, Supplemental Advisory on Identifying and Reporting Human Trafficking and Related Activity (Oct. 15, 2020), https://www.fincen.gov/sites/default/files/advisory/2020-10-15/Advisory%20Human%20Trafficking%20508%20FINAL_0.pdf.

- **Proliferation Financing.** Proliferation support networks use the U.S. financial system to move funds that will be used to acquire weapons of mass destruction or to develop state-sponsored weapons programs. Given the increased globalization of financial intermediators and the increasing disintermediation presented by, for instance, cryptocurrency funding vehicles, bad actors are increasingly able to obfuscate the source of funds using, e.g., sophisticated gatekeepers, front or shell companies, or exchange houses, to generate and transfer funds through covered institutions.[34] Covered institutions should review FinCEN and U.S. Treasury Department advisories on proliferation financing, comply with sanctions programs, and remain aware of federal economic and trade sanctions.[35]

Certain of these Priorities, including corruption and cybercrime, warrant even greater focus for financial institutions, given their link to strict-liability sanctions compliance regimes. In addition to incorporating these Priorities into their AML programs, covered financial institutions will need to ensure their diligence—typically an AML function—sanctions screening, and alert disposition processes take into account the Priorities and their sanctions compliance implications. Finally, financial institutions should also regularly review enforcement actions and U.S. Department of Justice filings to stay current on the latest typologies.

As financial institutions navigate these complex challenges, WilmerHale is ready to assist.

[34] *FinCEN Priorities*, *supra* note 4, at 11-12.
[35] *See* U.S. Dep't of Treasury et al., Guidance to Address Illicit Shipping and Sanctions Evasion Practices (May 14, 2020), https://home.treasury.gov/system/files/126/05142020_global_advisory_v1.pdf; U.S. Dep't of Treasury, Sanctions Risks Related to Petroleum Shipments involving Iran and Syria (Mar. 25, 2019), https://home.treasury.gov/system/files/126/syria_shipping_advisory_03252019.pdf; U.S. Dep't of Treasury, Sanctions Risks Related to North Korea's Shipping Practices (Feb. 23, 2018), https://home.treasury.gov/system/files/126/dprk_vessel_advisory_02232018.pdf; FinCEN, FIN-2021-A003, Advisory on the Financial Action Task Force-Identified Jurisdictions with Anti-Money Laundering and Combating the Financing of Terrorism and Counter-Proliferation Deficiencies (Mar. 11, 2021), https://www.fincen.gov/sites/default/files/advisory/2021-03-11/FATF%20February%202021%20Advisory%20FINAL%20508.pdf.

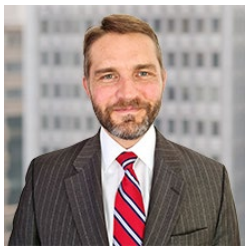
Contributors

Franca Harris Gutierrez
PARTNER

franca.gutierrez@wilmerhale.com
+1 202 663 6557

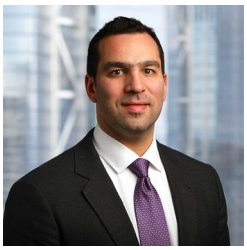
Michael Dawson
PARTNER

michael.dawson@wilmerhale.com
+1 202 663 6638



David M. Cook
SPECIAL COUNSEL

david.cook@wilmerhale.com
+1 202 663 6109



Zachary Goldman
COUNSEL

zachary.goldman@wilmerhale.com
+1 212 295 6309

Michael Romais
SENIOR ASSOCIATE

michael.romais@wilmerhale.com
+1 202 663 6233

Andrew Miller
ASSOCIATE

andrew.miller@wilmerhale.com
+1 202 663 6691