BCLP. Client Intelligent

Insights

COMPLIANCE IMPACT OF FINCEN STATEMENT OF PRIORITIES

Jul 28, 2021

At the direction of the President, FinCEN is intensifying its regulation of banks and fintechs across the spectrum of the laws that it is charged with enforcing. This past June, the White House published the Memorandum on Establishing the Fight Against Corruption as a Core United States National Security Interest (the "**Memorandum**"). In the Memorandum, President Biden sets forth a policy of "effectively preventing and countering corruption and demonstrating the advantages of transparent and accountable governance" and commits to "lead efforts to promote good governance; bring transparency to the United States and global financial systems; prevent and combat corruption at home and abroad; and make it increasingly difficult for corrupt actors to shield their activities."[1]

Following just a few weeks later, FinCEN published a Statement on the Issuance of the Anti-Money Laundering/Countering the Financing of Terrorism (AML/CFT) National Priorities (the "**Statement**") and Anti-Money Laundering and Countering the Financing of Terrorism National Priorities (the "**AML/CFT Priorities**"). The AML/CFT Priorities are applicable to all "covered entities" – financial service providers required to maintain an anti-money laundering program under the Bank Secrecy Act – which includes banks, money services businesses, credit card system operators, loan and finance companies, and broker-dealers.[2] In an earlier Client Alert, we discussed the expected impact on criminal enforcement activities.[3] Now we are turning our attention to impacts on compliance activities. While the priorities will be addressed specifically through regulations yet to be proposed,[4] FinCEN recommends that covered entities begin considering how to incorporate the AML/CFT Priorities into their compliance programs.

FinCEN's Eight AML/CFT Priorities

Echoing President Biden's earlier policy statements, the eight AML/CFT Priorities are (1) corruption; (2) cybercrime, including relevant cybersecurity and virtual currency considerations; (3) foreign and domestic terrorist financing; (4) fraud; (5) transnational criminal organization activity; (6) drug trafficking organization activity; (7) human trafficking and human smuggling; and (8) proliferation financing.[5] In the Statement, FinCEN elaborates on its concerns, as follows:

Corruption: Citing the Memorandum, FinCEN notes the grave risks of corruption and offers some practical guidance provided in prior advisories on human rights abuses enabled by corrupt senior foreign political figures in certain specific jurisdictions as a resource for the identification of red flags and other patterns.[6] *Takeaway: Apply patterns and red flags from prior incidents of corruption to root out future corruption or potential corruption.*

Cybercrime: U.S. financial institutions have proven to be popular targets for criminals, with the AML/CFT Priorities highlighting in particular "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."[7] Special attention is paid to cryptocurrencies, noting they are "often are used to layer transactions to hide the origin of money derived from illicit activity"[8] and "have been used by some of the highest-priority threat actors to advance their illegal activities and nuclear weapons ambitions."[9] FinCEN references advisories issued on ransomware, cryptocurrencies, cyber-enabled crime, and COVID-19 cybercrime in addition to a recent fact sheet and OFAC advisory on sanctions risks in connection with ransomware payments as supporting resources.[10] *Takeaway: Cybersecurity is increasingly important as more work shifts to technological solutions and bad actors increasingly target weaknesses in those technological solutions.*

Terrorist Financing: Terrorists use funds to recruit and support members, fund logistics, and conduct operations.[11] FinCEN calls out both international and domestic terrorists, noting that financial institutions are expected to comply with U.S. sanctions programs and be aware of terrorists and terrorist organizations included on U.S. sanctions lists. *Takeaway: Efforts to combat terrorist financing have long been a vital piece of a robust AML/CFT program, and AML/CFT Priorities reinforce recent focus on domestic terrorism.*

Fraud: Business and personal email account compromise are significant and growing sources of fraud affecting U.S. financial institutions.[12] FinCEN released an advisory in 2016, updated in 2019, on email compromise, and notes that COVID-19 has offered myriad opportunities for fraudsters to pursue novel schemes. *Takeaway: Provide robust controls for employee accounts and be aware of the risk that customer accounts are insecure.*

Transnational Criminal Organization Activity: Criminal organizations continue to develop strategies to launder money without detection, often leaning on professional money laundering networks.[13] *Takeaway: AML/CFT programs should address red flags and other indicia of professional money laundering networks.*

Drug Trafficking Organization Activity: Drug traffickers generate significant proceeds which may be laundered in or through the U.S.[14] Often drug traffickers rely on professional money laundering networks and complex laundering schemes, particularly through Mexico and China.[15] A FinCEN

advisory offered guidance on schemes and methods used by drug traffickers to launder money. *Takeaway: Specific red flags listed in FinCEN's guidance can help identify drug traffickers attempting to launder money and swift and detailed reporting can help authorities stop the underlying activity.*

Human Trafficking and Human Smuggling: Human traffickers and smugglers use a variety of mechanisms to move illicit proceeds. FinCEN issued an advisory in 2014, which was supplemented in 2020, highlighting certain red flags that may indicate human trafficking or smuggling.[16] *Takeaway: Guidance identifying typologies and behavioral and financial indicators should be compared against customer profiles by covered institutions to identify potential human trafficking or smuggling.*

Proliferation Financing: Trade brokers and front companies seek to acquire weapons and tools of mass destruction or further state-sponsored weapons programs.[17] FinCEN highlights global correspondent banking as a particular vulnerability and encourages covered institutions to consult several advisories addressing counter-proliferation strategies in specific countries, and a more general advisory released earlier this year.[18] *Takeaway: Risk-based AML/CFT programs should have more robust processes in place for those jurisdictions that have been identified by the Financial Action Task Force identifications as having strategic deficiencies.*

Next Steps and Practical Guidance

A robust existing AML/CFT program likely includes elements of the AML/CFT Priorities, but the FinCEN guidance provides helpful information that covered entities should take into consideration – and that covered entities can use to appropriately direct internal resources to specific areas of concern. The AML/CFT Priorities also highlight increased national focus on domestic terrorism and cybersecurity; the latter is already front-page news from a recent spate of high-profile and critical infrastructure ransomware and hacking attacks.

Additionally, recent criminal enforcement actions shed light on some of the conduct that will likely be specifically addressed in forthcoming regulations addressing controls, monitoring and reporting obligations. Prosecutions have hit large banks as well as fintechs and industrial companies, collecting large settlements ranging into the billions of dollars. The actions have targeted many activities already clearly illegal, such as money laundering schemes and passive complicity in bribery and corruption schemes. As expected, cryptocurrency dealings have drawn increased scrutiny and action and this scrutiny has been intensified by the use of cryptocurrency in facilitating ransomware attacks. We expect this prosecutorial activity to intensify and new regulations to require more robust measures to identify and verify parties and beneficiaries of transactions, monitor, identify and report suspicious activity, as well as maintain controls to prevent fraudulent and abusive practices. It remains to be seen how specifically prescriptive the proposed regulations will be.

Of particular interest are the prosecutions that were effectively rejected by courts because, for example, existing regulations were not sufficiently specific to describe the allegedly violative conduct or because prosecutors were attacking conduct that was considered common practice. As commented in the earlier Client Alert mentioned above, we expect regulations to sharpen the descriptions of conduct that is considered violative to support prosecution of criminal cases, and this heightened specificity will also be reflected in new regulatory obligations and civil sanction authority.

While compliance with the above AML/CFT Priorities is not yet required, covered entities are encouraged to begin investigating workable solutions for implementation without overburdening compliance and regulatory teams. Starting early to consider feasible policy, procedure, and systems updates can reduce disruption and unanticipated budget impacts when regulations are finalized and implemented. This advance planning could also better position covered entities to analyze the impacts and perhaps comment to regulators on the practical implications of the proposed regulations when they are published.

1. Joseph Biden, Jr., "Memorandum on Establishing the Fight Against Corruption as a Core United States National Security Interest," White House Briefing Room (June 3, 2021), available at 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/.

2. Separate statements were published for non-bank financial institutions by FinCEN, and jointly for banks and credit unions by the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, the National Credit Union Administration, and the Office of the Comptroller of the Currency. See 31 CFR Chapter X; see also summary of covered entities provided in AML/CFT Priorities, FN 6.

3. "Sharper Lines Mean Tighter Nets: How the FinCEN's Latest Priorities are Another Step to Increased Enforcement," Bank BCLP (July 9, 2021), available at https://bankbclp.com/2021/07/sharper-lines-mean-tighter-nets-how-the-fincens-latest-priorities-are-another-step-to-increased-enforcement/.

4. Regulations must be promulgated within 180 days after the establishment of the priorities. 31 U.S.C. § 5318(h)(4)(D) (as amended by the Anti-Money Laundering Act of 2020 § 6101(b)(2)(C)).

5. AML/CFT Priorities.

6. AML/CFT Priorities, II(A).

7. AML/CFT Priorities, II(B).

8. See U.S. Treasury Department, National Money Laundering Risk Assessment, December 20, 2018, at 3.

9. AML/CFT Priorities, II(B).

10. Id.

11. AML/CFT Priorities, II(C).

12. AML/CFT Priorities, II(D).

13. AML/CFT Priorities, II(E).

14. AML/CFT Priorities, II(F).

15. Id.

16. AML/CFT Priorities, II(G).

17. AML/CFT Priorities, II(H).

18. Id.

RELATED CAPABILITIES

- Finance
- Fintech

MEET THE TEAM

Stanton R. Koppel

San Francisco

stanton.koppel@bclplaw.com
+1 415 675 3437