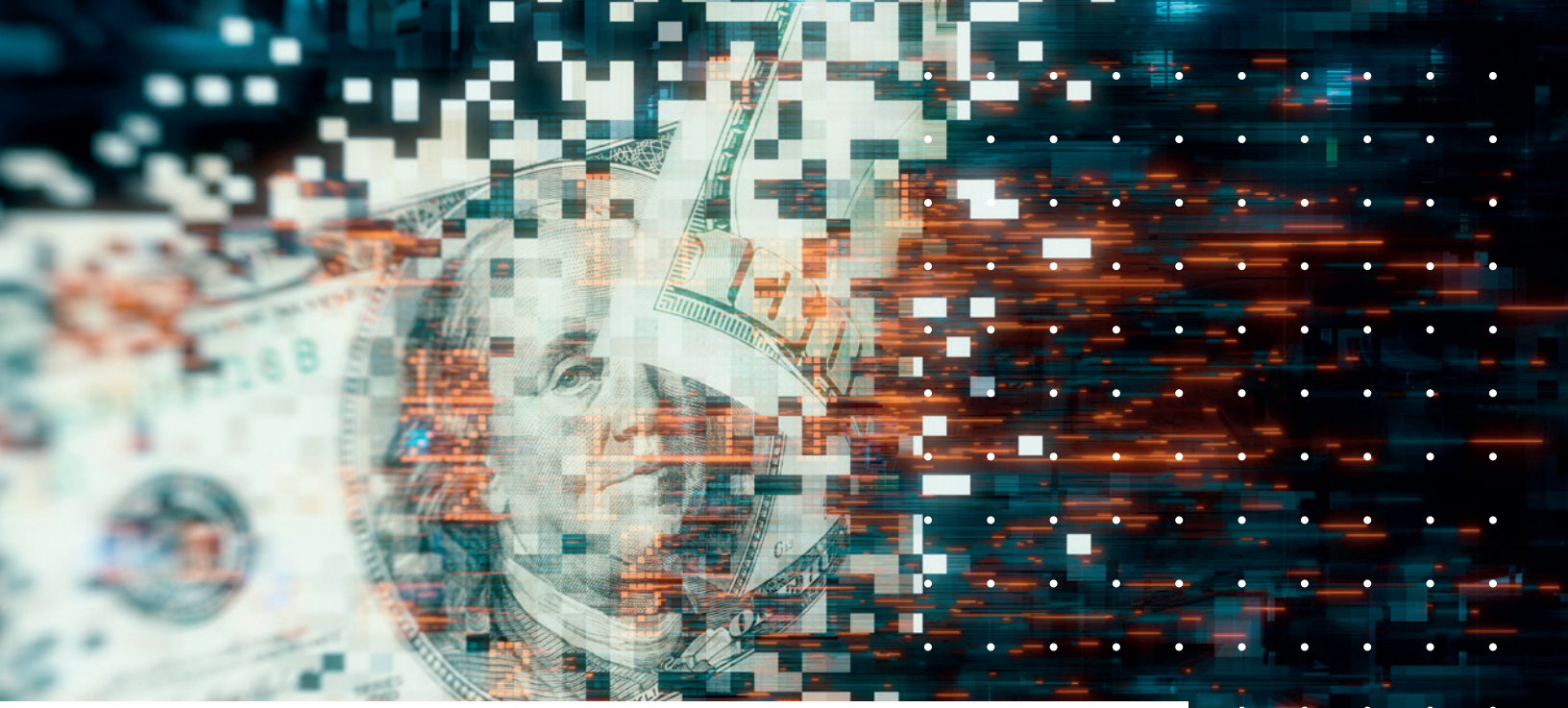

FinCEN's National AML/CFT Priorities:

Emerging Risks and Evolving Responses

JULY 2021

AUTHORS:

Christopher Sidler
Managing Director
csidler@thinkbrg.com
202.740.1307

Walter Mix
Managing Director
wmix@thinkbrg.com
213.261.7712

Conor Stanhope
Senior Associate
cstanhope@thinkbrg.com
202.480.2763

Valtteri Tamminen
Senior Associate
vtamminen@thinkbrg.com
202.480.2772

INTELLIGENCE THAT WORKS

BRG

The passage of the Anti-Money Laundering Act of 2020 greatly advanced the anti-money laundering/combating the financing of terrorism (AML/CFT) regime in the United States. On June 30, the six-month anniversary of the act's implementation, US Treasury's Financial Crimes Enforcement Network (FinCEN) released its first-ever National AML/CFT Priorities.[1] FinCEN laid out eight categories that signal its priorities for the next four years:

- Corruption
- Cybercrime and virtual currencies
- Foreign and domestic terrorist financing
- Fraud
- Transnational criminal organization activity
- Drug trafficking organization activity
- Human trafficking and human smuggling
- Proliferation financing

Key Takeaways

- **E pluribus unum.** FinCEN developed its priorities in close collaboration with US government agencies, including offices within the Treasury Department, the federal bank regulators, the Attorney General, and state regulators. This effort shows an increased priority for alignment and cooperation in addressing these threats.
- **Enemies foreign *and* domestic**. Much of the discourse on corruption has focused on foreign bribery and corrupt practices. Similarly, discussions of terrorist financing have long been limited to international and foreign terrorism, both those operating on a global scale and those focusing on regional matters. In a notable evolution in the discourse, the priorities acknowledge domestic threats associated with public corruption and terrorism within the United States, including domestic violent extremism.
- **Efficiency and effectiveness**. In his comments supporting the priorities, FinCEN Acting Director Michael Mosier acknowledged FinCEN's ongoing efforts at enhancing both the effectiveness and the efficiency of the AML/CFT regime.[2] He underscored the need for covered institutions to "assess their risks, tailor their AML programs, and prioritize their resources." The fundamental risk-based approach inherent in the AML/CFT regime depends on continual enhancement and review of practices to drive both effectiveness and efficiency in allocating finite financial crime compliance resources.

What Firms Should Do

The interagency statement on the issuance of the priorities made clear that there is no requirement that regulated institutions immediately incorporate the priorities into their compliance programs.[3] Rather, FinCEN and the federal agencies recognized the need for revised regulations and guidance before firms will have to implement changes to their risk-based BSA/AML programs. Nonetheless, the priorities provide helpful input to firms and should be considered in the following ways:

- **Risk assessment**. Firms should start preparing to review and incorporate each of the priorities into their risk-based program for when new guidance or regulations appear. This means considering, for example, customer, product, and geography factors related to the firm's exposure to these risks.
- **Risk appetite**. The board of directors should consider the impact of the risk assessment on the firm's risk appetite, and management should address those changes in relevant policies.
- **Risk typology and coverage.** Identifying typologies and red flags of potentially suspicious behavior will be key to complying with upcoming regulations, particularly where those behaviors indicate activity related to the priorities.
- **Expertise and capabilities**. Similarly, having the knowledge and capability to investigate these priority risk areas will be important to prevent financial crime and demonstrate the firm's commitment to maintaining an effective program.

1 FinCEN, *Anti-Money Laundering and Countering the Financing of Terrorism National Priorities* (June 30, 2021), available at: https://www.fincen.gov/sites/default/files/shared/AML_CFT%20Priorities%20(June%2030%2C%202021).pdf

2 FinCEN, *FinCEN Issues First National AML/CFT Priorities and Accompanying Statements* (June 30, 2021), available at: https://www.fincen.gov/news/news-releases/fincen-issues-first-national-amlcft-priorities-and-accompanying-statements

3 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), available at: https://www.fincen.gov/sites/default/files/shared/Statement%20for%20Banks%20(June%2030%2C%202021).pdf

Combatting Domestic Terrorism

Given the events of January 6, 2021, the increased prevalence of extremism and radicalization domestically, and FinCEN's reference to domestic terrorism in the publication of its AML/CFT priorities, firms should take reasonable steps to identify and report suspicious activity potentially attributed to involvement in domestic extremism and/or terrorism. In June, the Biden administration released the *National Strategy for Countering Domestic Terrorism*, stating that:

> ...the Department of the Treasury, in coordination with law enforcement and other interagency partners, is exploring ways to enhance the identification and analysis of financial activity associated with domestic terrorists and their foreign counterparts, as well as enhancing engagement with financial institutions on domestic terrorist financing, including through existing provisions of the Bank Secrecy Act.[4]

Covered institutions should identify and address risks pertaining specifically to domestic terrorism in their know your customer (KYC) and customer due diligence (CDD) programs, as well as suspicious activity investigations. KYC/CDD functions that serve to minimize the financing of domestic terrorism should:

- Identify, to the extent feasible, individuals known to be affiliated with extremist groups in screening processes
- Incorporate "keywords" in adverse media searches aimed at identifying individuals that may be publicly implicated in extremist organizations or ideologies
- Maintain robust enhanced due diligence programs applied to relationships with customers displaying higher risk characteristics, such as certain nongovernmental organizations and charities

While some transactional typologies traditionally attributed to terrorist financing also may be applicable to domestic terrorism, others may be needed to address the unique factors of certain domestic threats. These may include:

- Multiple purchases on or transactions with known right-wing extremist sites
- Transactions associated with dark web hosting services
- Roughly reciprocating cash withdrawals following:
  - High-dollar credits from cryptocurrency exchanges
  - Settlement from crowdfunding sites
  - Multiple incoming peer to peer (P2P) transfers from individuals with no discernable connection to each other or the customer
- Roughly reciprocating purchases at sporting goods stores or known gun/ammunition dealers, following the above occurrences
- Association to ideologically driven crowdfunding sites
- Several outgoing P2P transfers to individuals with no discernable connection, funded by cash deposits, crowdfunding settlements, wire/automated clearing house (ACH) credits from charity/nongovernmental organizations or cryptocurrency exchange withdrawals
- Keywords in wire/P2P memos referencing extremist groups or ideologies

4 Executive Office of the President, National Strategy for Countering Domestic Terrorism, National Security Council (June 2021), p. 18 available at: https://www.whitehouse.gov/wp-content/uploads/2021/06/National-Strategy-for-Countering-Domestic-Terrorism.pdf

Cybersecurity and Virtual Currencies

There has been a marked increase in cyberattacks as economic activity has shifted during the COVID-19 pandemic.[5] Ransomware attacks have been particularly damaging to businesses and consumers. In mid-2021, ransomware attacks hit Colonial Pipeline,[6] causing major disruptions in gasoline and fuel deliveries on the US east coast; and JBS,[7] the largest beef supplier in the world, which led to a complete halt at several meat plants. Both instances led to the companies paying hackers millions of dollars in ransom using virtual currencies.

Financial institutions should consider the AML/CFT[8] and sanctions[9] risks associated with facilitating ransomware payments. FinCEN's decision to group convertible virtual currencies (CVCs) with cybersecurity indicates just how seriously the agency takes the linkage between them. Financial institutions should be aware of red flags that include:

- A customer's virtual currency address, or an address with which a customer is transacting, that may be linked to ransomware strains or payments
- A transaction that occurs between an organization and a digital forensics and incident response (DFIR) company or cyber insurance company (CIC)
- A DFIR or CIC that receives funds from its customer and shortly thereafter sends equivalent amounts to a CVC exchange
- A company with no, or limited, history of CVC transactions that makes a large CVC transaction
- A customer that indicates that a payment is being made in response to a ransomware attack

Conclusion

While the National AML/CFT Priorities do not impose any immediate requirements on covered institutions, now is the time to think about the risks that they pose and to take steps to incorporate them into a risk-based BSA/AML compliance program.

5 INTERPOL, "INTERPOL report shows alarming rate of cyberattacks during COVID-19" (August 4, 2020), available at: https://www.interpol.int/en/News-and-Events/News/2020/INTERPOL-report-shows-alarming-rate-of-cyberattacks-during-COVID-19

6 Collin Eaton and Dustin Volz, "Colonial Pipeline CEO Tells Why He Paid Hackers a $4.4 Million Ransom," *The Wall Street Journal* (May 19, 2021), available at: https://www.wsj.com/articles/colonial-pipeline-ceo-tells-why-he-paid-hackers-a-4-4-million-ransom-11621435636

7 Kevin Collier, "Meat supplier JBS paid ransomware hackers $11 million," CNBC (June 9, 2021), available at: https://www.cnbc.com/2021/06/09/jbs-paid-11-million-in-response-to-ransomware-attack-.html

8 FinCEN, "Advisory on Ransomware and the Use of the Financial System to Facilitate Ransom Payments," FIN-2020-A006 (October 1, 2020), available at: https://www.fincen.gov/sites/default/files/advisory/2020-10-01/Advisory%20Ransomware%20FINAL%20508.pdf

9 US Office of Foreign Assets Control, "Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments," US Department of the Treasury (October 1, 2020), available at: https://home.treasury.gov/system/files/126/ofac_ransomware_advisory_10012020_1.pdf

About BRG

Berkeley Research Group, LLC (BRG) is a global consulting firm that helps leading organizations advance in three key areas: disputes and investigations, corporate finance, and performance improvement and advisory. Headquartered in California with offices around the world, we are an integrated group of experts, industry leaders, academics, data scientists, and professionals working beyond borders and disciplines. We harness our collective expertise to deliver the inspired insights and practical strategies our clients need to stay ahead of what's next. Visit thinkbrg.com for more information.

THINKBRG.COM