Deloitte.

AML/CFT Priorities:
5 areas of potential impact and 5 key questions for FIs to consider

As required by the Anti-Money Laundering (AML) Act of 2020, the Financial Crimes Enforcement Network (FinCEN) recently issued the first government-wide National AML/Countering the Financing of Terrorism (CFT) Priorities (Priorities).[1]

When implementing rules become effective, Financial Institutions (FIs) will be required to incorporate the Priorities into their risk-based AML programs.

The publication of the Priorities is a significant step forward in shifting the primary focus of regulators and FIs concerning AML programs from maintaining technical compliance to a more risk-based, innovative and outcomes-oriented approach to help combat financial crime and safeguard national security.

While the publication of the Priorities does not create any new obligations or expectations for FIs, they should start considering and planning for how they will incorporate the Priorities into their risk-based AML programs in preparation for rules that will be finalized later this year.

5 areas of potential impact

1

Greater focus on understanding threats

Incorporating Priorities into AML programs will likely involve a greater focus on understanding specific threats related to applicable Priorities and how they may intersect with the FI's business activity. FIs may need to leverage additional data and information including publicly available information (e.g., FinCEN Advisories, US National Risk Assessments) as well as internal information, including historical monitoring and investigations data.

2

Adjustments to risk assessment processes

In order to identify, evaluate, and mitigate risks associated with the Priorities, FIs will likely need to adjust their AML risk assessment processes to focus more closely on applicable Priorities and more rapidly understand and incorporate new information received from law enforcement and other sources in the future. Finally, for Priorities like cybercrime, corruption and fraud, FIs will need to assess how to leverage additional intelligence and expertise from across the organization to improve the value of their AML reporting to law enforcement.

3

Resource allocation

In order for a risk-based approach to be effective, an FI will need the flexibility to focus resources on higher-risk customers and activities, consistent with its risk profile. This will require the FI to be more willing and agile in making AML program changes. When reallocating focus and resources from lower to higher value activities, the FI will need to demonstrate how the resulting shifts are producing highly useful information for law enforcement.

4

Strengthening feedback loops to integrate additional data and intelligence into AML programs and controls

FIs should consider how they will incorporate additional data and intelligence into their AML programs and controls on an ongoing basis. As volume and quality of information sharing across the public and private sectors increases, FIs will need to identify the most effective way of incorporating new intelligence relating to the Priorities into monitoring and investigations approaches. This also includes closer integration of data and intelligence within the FI's AML, fraud, and cyber operations.

5

Demonstrating alignment to Priorities

It is likely that most FIs will also need to develop metrics and examples to demonstrate how their AML programs align to the Priorities and the associated value of reporting to law enforcement. Based on the FI's size, complexity, customer base, and products and services offered, these metrics or examples could include: participation in public-private sharing partnerships (e.g., FinCEN Exchange, Suspicious Activity Report (SAR) review teams); timeliness of responses to law enforcement and relevant government authorities (e.g., responses to grand jury subpoenas); SARs filed related to the Priorities, recognition from law enforcement related to the Priority areas, and employee participation in training in applicable Priority areas. The Wolfsberg Group recently published a paper on this topic.[2]

5 key questions for FIs to consider

1

How do we align to the Priorities?

In the future, how will our AML programs need to evolve to better align to the Priorities? Do we fully understand the applicable threats? Have we mined appropriate public, private and internal sources of information or typologies to fully understand the risk? How should we best mine our history of suspicious activity reporting and law enforcement interaction to gain insight into what was reported related to the Priorities, and how could the use of the information be expanded?

2

What is the impact to our risk assessment process?

What needs to change in terms of how we assess risk and enhance the value of the reporting and the outcomes that we produce against each applicable Priority? Have we fully thought through the cybercrime, bribery, corruption and fraud threats that may have a nexus to our operations and that we might detect and report on? How do we pivot our risk assessment processes to be more agile, forward looking and responsive to emerging threats?

3

What is the potential impact on our AML resourcing?

Are our resources focused on the right areas, customers and activities? Do we need to reallocate resources from lower value areas to focus more deliberately on the Priority areas? When pivoting away from activities that produce low risk management value, how can we document, justify, and defend this shift in AML program risk and procedural changes?

4

How will we demonstrate and evidence effectiveness?

How will the effectiveness of our AML program be evaluated in the future by the Board, examiners, and auditors (e.g., metrics, key performance indicators)? How might independent testing of AML programs change, and how would examiners and auditors determine if we have done "enough" to demonstrate focus on the Priorities, and assess the value of the information the AML program produces and its effectiveness?

5

What role can innovation and emerging technology play?

Can we appropriately leverage emerging technology, including machine learning and artificial intelligence, to better detect emerging threats and risks associated with the Priorities? Can a NextGen approach help achieve the goal of identifying more complex suspicious activity that would be highly valuable to law enforcement?

Connect with us

Clint Stinger
Anti-Money Laundering and Sanctions Services Leader
Principal | Deloitte Risk & Financial Advisory
Deloitte Transactions and Business Analytics LLP
cstinger@deloitte.com

Yamicha Stephenson
Manager | Deloitte Risk & Financial Advisory
Deloitte Transactions and Business Analytics LLP
ystephenson@deloitte.com

Thomas Hughes
Senior Consultant | Deloitte Risk & Financial Advisory
Deloitte Transactions and Business Analytics LLP
thohughes@deloitte.com

End notes

1. FinCEN, Anti-Money Laundering and Countering the Financing of Terrorism National Priorities, June 30, 2021.

2. The Wolfsberg Group, Statement on Demonstrating Effectiveness, June 30, 2021.