AML program effectiveness:
A new focus on outcomes for law enforcement and national security

There is a growing consensus among regulators, legislators, law enforcement, and industry that compliance with Anti-Money Laundering (AML) requirements has evolved into a layered and inefficient system that does not optimally serve the needs of law enforcement.[1] In many instances, this has resulted in regulated financial institutions (FIs) spending time on activities that may do little to mitigate the risks associated with financial crime. The AML Act of 2020 (AML Act)[2] reinforces and codifies in law a risk-based approach to AML and Countering the Financing of Terrorism (CFT), expanding on the Financial Crimes Enforcement Network's (FinCEN) Advance Notice of Proposed Rulemaking (ANPRM) on AML program effectiveness[3]. The AML Act requires FinCEN to establish national AML/CFT Priorities (Priorities) for FIs to incorporate into AML/CFT programs (AML programs), and regulators and examiners to incorporate in rules, guidance and examinations. This signals a welcome and fundamental change, shifting the primary focus for 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. For example, the AML Act states that AML programs should be "reasonably designed" and "risk-based, including that more FI attention and resources should be directed toward higher-risk customers and activities, consistent with the risk profile of an FI, rather than toward lower-risk customers and activities." Similarly, the ANPRM had previously acknowledged that FIs "may reallocate resources from other lower-priority risks or practices to manage and mitigate higher-priority risks, including any identified as Strategic AML Priorities." To facilitate technical innovation to further this aim, the AML Act reinforces the overall goal of facilitating the ability of FIs to leverage new technologies and techniques, and discard inefficient practices.

There are numerous challenges associated with making this pivot a reality for FIs including addressing the question of how examiners and auditors will evaluate programs against these new expectations. These challenges will need to be addressed as the rulemaking process continues over the coming years. With the enactment

> The AML Act lays the foundation for a more risk-based, innovative and outcomes-oriented approach to combat financial crime and safeguard national security in the US

of the AML Act, FIs are presented with an immediate opportunity to rethink how they will drive AML program effectiveness in line with the concept of Priorities and direction outlined in the AML Act.[4] This will be a long-term journey that can also deliver significant benefits in terms of efficiency and return on compliance spend.

Toward a more risk-based, Priorities-focused AML regime

The AML Act states that AML programs should be reasonably designed and risk-based, focusing on national Priorities as well as the unique risk profile of the FI in question. Both the AML Act and ANPRM emphasize that AML programs should provide information with a high degree of usefulness to government authorities, consistent with both the institution's risk assessment and the Priorities identified by FinCEN.

In the future, FIs will be required to: integrate Priorities into their risk assessments and operations; enhance their AML programs (including Know Your Customer (KYC) and monitoring controls); and demonstrate how the results of these changes provide useful information to law enforcement. In the new regime, examiners and auditors will need to change the focus of their reviews to address the new focus on risk-based AML programs that align to published Priorities including the associated impact to governance, compliance culture, training, and operational controls.

As FinCEN and other financial regulators begin to issue new guidance and regulations, FIs should be prepared to focus their attention on the following challenges:

- Aligning AML programs to Priorities and enhancing outcomes for law enforcement

- Refocusing resources on higher-value AML activities

- Rethinking AML monitoring, investigations, and information sharing

Aligning AML programs to Priorities and enhancing outcomes for law enforcement

It is reasonable to expect that forthcoming Priorities will likely include highly dynamic threats such as cybercrime, human trafficking, proliferation financing, terrorist financing, as well as emerging risks such as coronavirus related frauds. For identified Priorities, FIs should think through how each area of their AML program contributes to the production of highly useful information for law enforcement. The AML Act also amends the purpose of the Bank Secrecy Act (BSA) to formally require appropriate frameworks for enhanced information sharing. Given this, FIs should also expect that law enforcement, through existing and new channels, will share more specific information on risks, threats, and typologies related to these Priorities.

FIs could orient their AML programs toward the Priorities through several avenues. FIs can adapt their risk assessment processes and capabilities to dive deeper into the Priorities that apply to their business, leveraging additional information and input from a variety of public and private sector sources to increase knowledge of typologies and red flags. FIs could review their own history of suspicious activity reporting and law enforcement interaction to gain insight into what was provided and could be expanded. From there, FIs could embed those Priority insights in control enhancements, which could range from:

- Realigning customer due diligence (CDD) questions in certain situations,

- Enhancing AML monitoring to address new red flags, and

- Developing additional investigation procedures to provide information law enforcement has identified as useful.

An FI's understanding of its ability to provide highly useful information to law enforcement can be improved through interaction and dialogue with law enforcement through traditional channels (314(a) requests, subpoenas, and demand letters) as well as new channels cited in the AML Act, such as the FinCEN Exchange.

Perhaps most importantly, each FI will likely need to develop metrics and examples to demonstrate alignment with the Priorities and the associated value of reporting to law enforcement. FinCEN is also seeking input on potential changes to independent testing needed in order to meet the objectives outlined in the ANPRM and AML Act. This is a critical topic as ultimately if reform is to be successful, examiners, auditors, and other program evaluators will need to be on the same page in terms of how to measure and evaluate AML program effectiveness.

Specific challenges and questions for FIs include:

- How can you **pivot your AML program to focus on the Priorities**?
  - How and at what frequency would you adapt your current risk assessment?

- How will the **effectiveness of your FI's AML program be evaluated in the future** by the board, examiners, and auditors?

  - What are the possible metrics and examples that could be used to demonstrate effectiveness?
  - How might independent testing of AML programs change, and how would examiners and auditors determine if FIs have done "enough" to demonstrate focus on the Priorities and assess the value of the information the AML program produces?
  - What law enforcement feedback could be used to focus and refine your AML program?

Refocusing resources on higher-value AML activities

The AML Act states that an effective AML program ensures more attention and resources are directed toward higher-risk customers and activities, consistent with the risk profile of an FI. This will require FIs to be more agile in making AML program changes. To take advantage of this opportunity, FIs should adopt a consistent, repeatable, and defensible approach to procedural changes that can be applied across AML program areas and satisfy examiners and auditors. A change management process with appropriate governance, documentation, and sign off will be key to realign resources on more high value-added activities and, thereby, increasing return on investment for AML compliance spend, which is high on the agenda for many FIs. By way of example, recent Frequently Asked Questions (FAQs) and guidance released by the regulatory community clarify requirements in a number of important areas. FIs are able to reference this guidance and reexamine their procedures, change what they are doing, and reallocate resources to meet the objectives of the intended reform.[5] Examples of areas where this may be appropriate are negative news screening on all customers, frequently conducting periodic reviews for low- and medium-risk customers with no material trigger events, as well as Politically Exposed Person (PEP) screening of US domestic customers/transactions.

Specific challenges and questions for FIs
- Given the expectations outlined in the AML Act, how can you create a repeatable change management process to drive ongoing transformation and resource redeployment to high-value activity?
  – How can you determine which activities are delivering low AML risk management value?
  – How can you document, justify, and defend AML program risk and procedural changes?
  – Where should you start? What's the right strategy? How could you scale the effort and effectively reallocate resources?

Rethinking AML monitoring, investigations, and information sharing

In order to meet the objectives of providing highly useful information to law enforcement and refocusing efforts toward higher value AML activities, FIs should focus on enhancing AML monitoring and investigations. Under the current AML regime, FIs dedicate significant resources to routine activities performed by lower level staff, such as clearing of false positive AML monitoring alerts and documenting case dispositions. In line with the Act's stated objective of facilitating industry's ability to leverage new technologies, FIs should consider rethinking their approach to AML monitoring and investigations, including automating routine activity, reducing false positives through advanced analytical approaches, and experimenting with advanced next generation (NextGen) models. Models that leverage behavioral analytics, machine learning, and advanced network analysis are designed to more effectively identify complex patterns of suspicious behavior with fewer false positives.

Specific challenges and questions for FIs
- How can your FI enrich and automate current AML monitoring, investigating, and reporting approaches to deliver more useful information for law enforcement?
  – Can routine activities be automated to free up resources and utilize standardized processes?
  – Are there areas delivering low AML risk management value, which could be scaled back?
  – What strategies and analytics can be deployed to reduce false positives coming out of your FI's AML monitoring system(s)?
  – How can your FI better utilize and share information and intelligence from a broader array of internal, external, and public sources?
- How can you appropriately leverage emerging tech and NextGen AML detection models?
  – Can a NextGen approach help achieve the goal of identifying more complex suspicious activity?
  – What are the data, technology, modeling, and regulatory challenges associated with developing, testing, validating, and implementing such models?

Conclusion

The AML Act provides an immediate opportunity for FIs to rethink and influence the focus of their AML programs and start on a journey that can deliver significant benefits in terms of effectiveness, efficiency, return on compliance spend, and providing highly useful information to law enforcement. FIs can consider the following actions in the near-term:

- Evaluating how risk assessment processes can be modified to address expected Priorities, and identifying metrics and examples that could be used to demonstrate effectiveness

- Assessing areas of low added risk management value, in light of recent regulatory guidance, for potential reductions and/or reallocation of resources

- Considering ways to further enrich, automate, and innovate AML monitoring and investigations, and to deliver more valuable information to law enforcement more effectively and efficiently.

Contacts

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

Todd Raque
Senior Manager | Deloitte Risk & Financial Advisory
Deloitte Transactions and Business Analytics LLP

Yamicha Stephenson
Manager | Deloitte Risk & Financial Advisory
Deloitte Transactions and Business Analytics LLP

Kyle Cooke
Senior Consultant | Deloitte Risk & Financial Advisory
Deloitte & Touche LLP

Endnotes

1. Federal Reserve Board of Governors (FRB), Federal Deposit Insurance Corporation (FDIC), Office of the Comptroller of the Currency (OCC), National Credit Union Administration (NCUA) and Financial Crimes Enforcement Network (FinCEN), "Interagency Statement on Sharing Bank Secrecy Act Resources," accessed September 16, 2020; FRB, FDIC, OCC, NCUA and FinCEN, "Joint Statement on Innovative Efforts to Combat Money Laundering and Terrorist Financing," accessed September 16, 2020; and, FRB, FDIC, OCC, NCUA and FinCEN, "Joint Statement on Risk-Focused Bank Secrecy Act/Anti-Money Laundering Supervision," accessed September 16, 2020.

2. The Anti-Money Laundering Act of 2020 is contained in division F of the National Defense Authorization Act (NDAA) for fiscal year 2021: "H.R. 6395 - NDAA for Fiscal Year 2021," accessed December 22, 2020.

3. FinCEN, "FinCEN Seeks Comments on Enhancing the Effectiveness of Anti-Money Laundering Programs," accessed September 16, 2020.

4. Federal Financial Institutions Examination Council (FFIEC), "Federal and State Regulators Release Updates to BSA/AML Examination Manual," accessed September 16, 2020; FinCEN, "Frequently Asked Questions Regarding Customer Due Diligence (CDD) Requirements for Covered Financial Institutions," accessed September 16, 2020; and FRB, FDIC, OCC, NCUA, and FinCEN, "Joint Statement on Bank Secrecy Act Due Diligence Requirements for Customers Who May Be Considered Politically Exposed Persons," accessed September 16, 2020.

5. Ibid.