MANAGING A REMOTE BSA/AML PROGRAM

INTRODUCTION

Recent impacts of COVID-19 have accelerated a digital movement and remote working model for some elements of the bank secrecy act ('BSA')/anti-money laundering ('AML') and sanctions compliance program that were likely already in motion. Despite the global impact of COVID-19, the Financial Crimes Enforcement Network 'FinCen' expects financial institutions to continue following a risk-based approach, and diligently adhere to their BSA obligations.[1]

In the context of the current pandemic, financial institutions are expected to face significant challenges due to: (i) a convergence of (probable) increased criminal activity and fraudulent schemes seeking to capitalize on the pandemic; and (ii) the strains of a remote workforce, a decrease in staffing capacity, and level of timely communication required to run an effective BSA/AML and compliance programs (i.e., a stale AML Business Continuity Plan,'BCP')

Similar to the financial crisis of 2008, the current pandemic is likely to see additional elements of fraud in many areas of the financial services industry – desperate families, investors, and lenders demanding their money back only to find it vanished before COVID-19 appeared.

This article highlights certain components of a BSA/AML and sanctions compliance program, which have been accelerated in response to COVID-19, articulates associated risks, and suggests potential solutions to maintain program effectiveness.

BSA/AML COMPLIANCE PROGRAM IMPACTS

1. Client Onboarding

Significant challenges may arise during account opening, especially for financial institutions which do not have online/remote account opening processes. Such institutions will be forced to adapt their products to reflect the fact that customers may not wish to enter a branch to open an account.

Additional challenges concerning the customer identification program ('CIP') and associated customer due diligence ('CDD') documentation and verification process will be disrupted as document hard copies may be inaccessible remotely. There may be reliance on crucial information from third parties – namely related to beneficial ownership documentation – who are also navigating the effects of the pandemic.

1. "The Financial Crimes Enforcement Network Provides Further Information to Financial Institutions in Response to the Coronavirus Disease 2019 (COVID-19) Pandemic," April 3, 2020. Available at: https://www.fincen.gov/news/news-releases/financial-crimes-enforcement-network-provides-further-information-financial.

Finally, critical metrics, such as a customer's expected versus actual activity, may no longer be relevant as people's lives, businesses, and behaviors were altered by COVID-19. Typically, this data is updated as part of risk-based know your customer ('KYC') updates (or periodic 'refreshes'), or during routine transaction monitoring and investigation activities. However, financial institutions must weigh the effects of COVID-19 on their KYC refresh programs and determine how 'risk-based' applies in this context.

Banks lending to small businesses participating in the Paycheck Protection Program ('PPP') under the CARES Act will need to make sure that CIP and other elements of KYC and onboarding are performed quickly, but without sacrificing regulatory compliance. The loan recipient will want to receive the much-needed financial aid as quickly as possible; however, an inefficient KYC process could lead to delays in loan disbursement or restrict the application process to existing customers. Banks will need to examine their ability to perform 'expedited KYC' for SBA loans, a process that is likely already slowed by remote people and processes.

2. Currency Transaction Reports ('CTR') and Suspicious Activity Report ('SAR') Filing

Due to the remote nature of their workforce and potential drains on compliance staffing capacity, financial institutions will see significant challenges in meeting certain BSA obligations, including timing requirements for certain report filings, as their people, processes and technology become remote. Although FinCEN recently stated, "it recognizes certain regulatory timing requirements with regard to BSA filings may be challenging during the COVID-19 pandemic and that there may be some reasonable delays in compliance," they only offered a narrow form of relief in the form of CTR obligations for an even more narrow class of entities[2].

3. Transaction Monitoring Program

During this COVID-19 outbreak, financial institutions may see a surge in their transaction monitoring alerts due to: (i) a likely increase in criminal activity; and (ii) also increases to (and deviations in) transaction activities from a worried customer base. Remote BSA/AML compliance teams may be operating with fewer resources and less coordination than before. Therefore transaction monitoring rules must be reviewed (and recalibrated where possible) to reflect a bank's highest risks, and consider the efficiency of alerts that systems have previously produced. The term "risk-based approach" concerning transaction monitoring programs has never been more meaningful.

Financial institutions will not want their BSA/AML staff to become overwhelmed by alerts generated from customers deviating their transaction behavior in response to COVID-19. Instead, the focus should be on identifying true criminal activity, and to adjust monitoring protocols accordingly. Turning off certain alerts altogether without adding additional scenarios could prove risky, as regulators could subsequently question what potential illegal activities were missed when the original alerts were suppressed. Perhaps a better solution would be to generate all alerts and provide analysts with more time to review them or use a triage approach to prioritize the alerts producing actionable financial crime intelligence.

In addition, business continuity plans ('BCPs') should provide flexibility to compliance programs in times of crisis, so that leadership can make risk-based decisions with respect to alert generation. To prevent future confusion, financial institutions should clearly document any changes made to AML and sanctions programs taken in response to COVID-19, including clear sign-off from senior leadership that the institution has evaluated and accepted the temporary risks presented by any deviation from previous rules.

2. Id.

RESPONSIBLE INNOVATION TO MEET BSA/AML COMPLIANCE REQUIREMENTS

In its most recent COVID-19 release, FinCEN encouraged "financial institutions to consider, evaluate, and, where appropriate, responsibly implement innovative approaches to meet their BSA/anti-money laundering compliance obligations, in order to further strengthen the financial system against illicit financial activity and other related fraud."[3]

Federal regulators have previously stated they welcome a bank's use of artificial intelligence and digital identity technologies, as they can "strengthen BSA/AML compliance approaches, as well as enhance transaction monitoring systems," including "maximize utilization of banks' BSA/AML compliance resources."[4]

Maximizing a bank's BSA/AML compliance resources without sacrificing regulatory obligations or customer experience is especially relevant. Areas of focus which lend themselves to a digital framework, remote operation and/or third-party outsourcing include:

1. Customer Identification Program
2. Sanctions and Politically Exposed Person ('PEP') screening
3. Customer Due Diligence and Enhanced Due Diligence
4. Related beneficial ownership and customer risk-ranking/ongoing monitoring
5. Alert clearing and case investigations

If financial institutions choose the COVID-19 pandemic to deploy responsible innovation toward its BSA/AML compliance processes, including blockchain opportunities, there are specific questions that must be answered. These include how to address the security of customer data captured during the account lifecycle, and determining whose security is threatened by possible shortcomings arising from the remote workforce and remote data access.

Customer data used during critical downstream processes of BSA/AML Compliance Programs, including ongoing transaction monitoring and related alert/case investigation and disposition and suspicious activity reports ('SARs'), must also be accessible to investigators, auditors and regulators alike. Therefore, financial institutions should, at a minimum, determine the following:

- How will KYC data be accessed remotely by critical BSA/AML compliance resources during daily monitoring and investigation activities?
- How will relevant data integrate into existing BSA/AML compliance workflows?
- Where will supporting customer information be stored (e.g., information obtained to verify customer information at account opening)?
- How will event-driven account information be updated remotely (e.g., when beneficial ownership information or expected/actual customer activity changes)?

Contact Information and Additional Resources

For further details regarding Capco AML services, please reach out to us at spencer.schulten@capco.com.

3. Id.
4. "Joint Statement on Innovative Efforts to Combat Money Laundering and Terrorist Financing," Board of Governors of the Federal Reserve System Federal Deposit Insurance Corporation Financial Crimes Enforcement Network National Credit Union Administration Office of the Comptroller of the Currency, December 2018.

AUTHORS

Spencer Schulten, Executive Director
Geoff Lash, Principal Consultant

ABOUT CAPCO

Capco is a global technology and management consultancy dedicated to the financial services industry. Our professionals combine innovative thinking with unrivalled industry knowledge to offer our clients consulting expertise, complex technology and package integration, transformation delivery, and managed services, to move their organizations forward.

Through our collaborative and efficient approach, we help our clients successfully innovate, increase revenue, manage risk and regulatory change, reduce costs, and enhance controls. We specialize primarily in banking, capital markets, wealth and asset management and insurance. We also have an energy consulting practice in the US. We serve our clients from offices in leading financial centers across the Americas, Europe, and Asia Pacific.

To learn more, visit our web site at www.capco.com, or follow us on Twitter, Facebook, YouTube, LinkedIn and Instagram.

WORLDWIDE OFFICES

APAC
Bangalore
Bangkok
Hong Kong
Kuala Lumpur
Pune
Singapore

EUROPE
Bratislava
Brussels
Dusseldorf
Edinburgh
Frankfurt
Geneva
London
Paris
Vienna
Warsaw
Zurich

NORTH AMERICA
Charlotte
Chicago
Dallas
Houston
New York
Orlando
Toronto
Tysons Corner
Washington, DC

SOUTH AMERICA
São Paulo

WWW.CAPCO.COM

CAPCO
THE FUTURE. NOW.

JN_1973