BSA/AML Compliance Strategies in a COVID-19 Environment

The formal study of risk management has been around since World War II and involves learning how to identify, assess and manage financial risks for an organization. It has long been associated with market insurance, protections from accidents and use of derivatives. It evolved into contingency planning, analyzing various risk prevention activities and portfolio management. Operational and liquidity risks emerged as a formalized concept in the 1990s as financial institutions intensified their market risk and credit risk management activities. Risk management has become a corporate affair—it is a major player in the decisions of an institution's management and monitoring policy. The concept of risk began to cover pure risk management, technological risk management models, and operational risk. And as the identification of new risks emerged, so did an expanded concept of operational risk.

Fraud risk is a form of operational risk. It is the risk to current or projected financial conditions and resiliency arising from inadequate or failed internal processes or systems, human error or misconduct, or adverse external events. Fraud historically has been known to increase during disaster-related events. The unprecedented COVID-19 pandemic is no exception to this increase. Fraud can be characterized as an international act, a misstatement or omission to deceive others with the sole purpose of a victim suffering a loss or a perpetrator achieving a gain. It can be internal or external but the key takeaway with fraud is that financial institutions subject to the Bank Secrecy Act are mandated to upkeep an anti-money laundering compliance program and process. Meeting BSA and AML obligations during a pandemic has proven challenging. It has forced financial institutions to adopt a new "business-as-usual process" that magnified challenges for financial crime management programs within institutions of all asset sizes.

Financial institutions, despite any differences in scale, are all facing work from home shifts, evolving customer behaviors and expectations, along with a rise in pandemic-related fraud patterns. The combination of financial and health risks opens vulnerabilities and creates more opportunities for fraudsters. The Agencies recognize that the current environment is (1) unprecedented and (2) requires flexibilities. Back on March 16, 2020, FinCEN released a state to financial institutions regarding the impact of the COVID-19 pandemic. It encouraged financial institutions to communicate their concerns related to the pandemic and to, above all things, remain alert to illicit financial activity. It encouraged financial institutions that had concerns over potential delays in filing any required BSA reports (CTRs and SARs) to contact FinCEN and their functional regulator as soon as practicable.

Second, FinCEN outlined the emerging trends connected with COVID-19: imposter scams, investment scams, product scams and insider trading. Financial institutions are reminded to review FinCEN's 2017 advisory FIN-2017-A007 for descriptions of other relevant typologies, which included benefits fraud, charities fraud and cyber-related fraud. Entering "COVID19" in Field 2 of the SAR-template when reporting suspicious transactions linked to COVID-19 was highly encouraged. But key pressure points continued to emerge in the new environment for financial institutions. Not only were financial institutions required to identify fraudulent and potentially suspicious activity outside of normal trends, they had to detect disaster-related fraud, increase their protection of elderly customers and report on COVDI-19 trends and losses. This is not to say financial institutions have not risen to the challenges.

FinCEN's April 3, 2020 notice encouraged financial institutions to "consider, evaluate, and, where appropriate, responsibly implement innovative approaches to meet their BSA/anti-money

laundering compliance obligations." Institutions have considered the health and safety of their employees and customers, and have maintained the stability of the financial system, managing, and mitigating the risks of money laundering and fraud losses. But what considerations should financial institutions continue to focus on as they navigate BSA/AML compliance?

1. Contingency Plans—Financial institutions need to be anticipating best and worse case scenarios. How will the financial institution re-establish its BSA/AML program and obligations once pivoting from remote work and a more return to normal? If the pandemic continues, what longer-term necessities and measures need to be taken to maintain or increase its BSA/AML practices?

2. Customer Due Diligence—COVID-19 has transitioned much more rapidly than an organic migration to online presences. Customers are expecting banks go even more digital via their online channels. This has not been without changed expected activity for both individuals and businesses. Has an institution increased its daily transaction limits to meet increased demands for additional cash? Has cash hoarding strained a bank's CTR filings? Did the organization experience an increase in false positives for fraud due to changing customer behaviors? Financial institutions need to continually evaluate their programs to grab control of the challenges and added workload to its BSA/AML staff.

3. Risk Assessments—No longer something for larger or more complex financial organizational structures, the need for risk assessments has increased. Customers have changed the scale of their operations. Programs like the Paycheck Protection Program under the CARES Act have flooded lending and operations divisions within the bank, which inhibits adequate oversight. Risk assessments need to continue to be reassessed on both a customer base and organizational level to re-consider the nature and purpose of customer relationships, continue that development of customer risk profiles, and reassess bank operational systems and controls. This was re-emphasized in the update to the FFIEC BSA/AML Examination Manual released April 15th.

4. Coordination and Communication—Identifying logistical challenges is one aspect; effectively communicating them to bank staff is another. Internal communication is essential. Impactful and cohesive running of compliance teams will aid financial institutions in minimizing the challenges of administering an effective BSA/AML compliance program during a pandemic. A risk-based approach with diligent adherence to a bank's BSA obligations are going to define compliance problem areas and assist financial institutions in mitigate their risks.

5. Technology—FinCEN's April guidance encouraged financial institutions to be innovative through the deployment of "novel technologies." While this encouragement has many possibilities, it does create challenges for financial institutions. Banks still must maintain prudent evaluations whenever implementing innovative approaches to current BSA/AML processes. Financial institutions need to maintain robust oversight of their vendor management relationships with third-party providers, especially as it relates to BSA/AML program implementation. Safety and soundness and consumer protection are heavily impacted by technology, increasing a bank (and regulator's) focus on monitoring.

The COVID-19 pandemic has introduced or an increased emphasis on a risk-based approach to BSA compliance. It has supported flexibilities as promulgated by FinCEN and other agencies. While regulators have highlighted the difficulties realized or otherwise by financial institutions, little reassurance or solutions have been offered. For this reason, financial institutions need to consider, evaluate, and determine what a risk-based approach means for its own institution. Criminals are luring targeted, vulnerable individuals and companies with an even stronger virtual presence—these attempts are aimed at undermining the bank's due diligence and "know your customer" processes within a remote environment. It is imperative that financial institutions review FinCEN and other Agencies' releases on advisories highlighting common typologies used in fraud, theft and money laundering activities related to the pandemic. The significant increase in online and digital transactions coupled with cyberattacks and related fraud is only going to continue to impact remote platforms and processes. Understanding the new and expanding definition of fraud risk will forces financial institutions to remain diligent with BSA/AML controls and procedures related to the pandemic.

Elizabeth K Madlem, Vice President of Compliance Operations.

Elizabeth is the Vice President of Compliance Operations and Deputy General Counsel at Compliance Alliance. In the past, she served as both the Operations Compliance Manager and Enterprise Risk Manager for Washington Federal Bank, a $16 billion dollar organization headquartered in Seattle, WA. She has industry expertise and real-world solutions surrounding bank-enterprise initiatives and knowledge of contract law and bank regulatory compliance. An attorney since 2010, Elizabeth was a Summa Cum Laude, Phi Beta Kappa, Delta Epsilon Sigma graduate of Saint Michael's College in Burlington, VT, and a Juris Doctor from Valparaiso University School of Law in Indiana.

As the Vice President of Compliance Operations, Elizabeth will be overseeing C/A's day-to-day operations of the Hotline, as well as leading our Education initiatives. Elizabeth plays an important part in all operational areas of C/A.