



PERSPECTIVES

Updating AML Compliance Programs: Integrating FinCEN's AML Priorities

Our perspectives feature the viewpoints of our subject matter experts on current topics and emerging trends.

INTRODUCTION

As the landscape of financial crime continues to evolve, financial institutions must stay vigilant and prepared to address emerging risks. In this regard, aligning anti-money laundering (“AML”) programs with the Financial Crimes Enforcement Network (“FinCEN”) AML Priorities¹ becomes crucial. This article explores the significance of integrating the FinCEN AML Priorities into AML programs and provides step-by-step suggestions to ensure preparedness for regulatory examinations.

Understanding the FinCEN AML Priorities

The FinCEN AML Priorities serve as a regulatory framework for AML compliance. In its inaugural list issued on June 30, 2021, FinCEN outlined several priorities that financial institutions should consider. These priorities include corruption, cybercrime, terrorist financing, fraud, transnational criminal organization activity, drugtrafficking organization activity, human trafficking and human smuggling, and proliferation financing.

The Impact of Selected FinCEN AML Priorities

Corruption

As one of the FinCEN priorities, corruption poses significant risks to the integrity of the financial system, undermining fair competition, distorting markets, and eroding public trust. Financial institutions must combat corruption as part of their AML programs, as corrupt practices facilitate money laundering, capital flight, and illicit financial flows.

Fraud

Fraud encompasses a wide range of deceptive practices, including identity theft, money mule schemes, and Ponzi schemes. Fraud poses a significant threat to financial institutions, both in terms of financial losses and reputational damage. To mitigate the impact of fraud on financial institutions, AML compliance programs should

focus on proactive fraud prevention, early detection, and swift response.

Transnational criminal organizations (“TCOs”)

TCOs engage in various illegal activities, such as drug trafficking, human trafficking and human smuggling, and weapons smuggling. These organizations exploit the global financial system to launder their illicit proceeds. The substantial funds generated from transnational criminal activities can have a distorting effect on local and global economies. Illicit funds infiltrate legitimate sectors, undermining fair competition, market dynamics, and investment opportunities. Financial institutions may unknowingly become conduits for transnational criminal activities. Criminal organizations use sophisticated methods to move illicit funds across borders, making it challenging for financial institutions to detect and prevent their involvement. When financial institutions are unwittingly used in money laundering schemes or become victims of fraud perpetrated by transnational criminals, they can suffer financial losses, damage to their reputation, regulatory penalties, and legal consequences.

Human trafficking and Human smuggling

Human trafficking and smuggling present grave humanitarian issues with significant financial implications. Human smuggling generates substantial illicit profits that criminals seek to legitimize through money laundering. Financial institutions may inadvertently become channels for laundering these funds, allowing criminals to integrate illegal proceeds into the legitimate economy. Money laundering associated with these activities can lead to reputational damage, regulatory non-compliance, and legal repercussions for financial institutions.

Cybercrime

Cybercrime refers to criminal activities conducted through digital means, targeting computer systems, networks, or individuals for financial gain or disruption. Financial institutions and their customers are prime targets for cyberattacks, which can lead to financial losses, reputational damage, and erosion of customer trust.

¹ See: Anti-Money Laundering and Countering the Financing of Terrorism National Priorities, Financial Crimes Enforcement Network, U.S. Department of the Treasury, June 30, 2021: <https://www.fincen.gov/news/news-releases/fincen-issues-first-national-amlft-priorities-and-accompanying-statements>

Integrating FinCEN AML Priorities into AML Programs

To effectively integrate the FinCEN AML Priorities into AML programs, financial institutions should consider the five key steps outlined below:

Step 1: Gap Analysis

Performing a comprehensive gap analysis is the first step towards preparedness. This analysis evaluates the alignment of existing AML programs with the FinCEN AML Priorities, identifying areas that require improvement or adjustment.

Step 2: Aligning Components of AML Programs

Financial institutions should integrate the FinCEN priorities into various components of their AML programs, such as policies and procedures, risk assessment methodologies, customer due diligence processes, transaction monitoring, and suspicious activity reporting protocols. These updates ensure the AML program explicitly addresses the FinCEN AML Priorities and provides guidance to employees for detecting and reporting suspicious activities.

Step 3: Strengthening Governance and Risk Management

Senior management should engage actively in aligning AML programs with the FinCEN AML Priorities, providing clear direction and support for implementing necessary changes. Establishing strong governance frameworks, enhancing risk assessment methodologies, and highlighting resources and controls based on the identified AML priorities are essential steps in strengthening governance and risk management.

Step 4: Leveraging Technology and Data Analytics

Leveraging advanced technologies such as artificial intelligence, machine learning, and data analytics can optimize AML programs. These technologies enhance the detection and monitoring of suspicious activities related to the FinCEN AML Priorities, identify patterns and anomalies, and automate manual processes. Network analytics can aid in uncovering complex relationships and hidden connections, helping identify sophisticated money laundering schemes or fraud networks.

Step 5: Establishing a Continuous Improvement Culture

Continuous monitoring, internal audits, independent reviews, and promoting communication, training, and awareness among employees is critical to establishing a continuous improvement culture. These efforts ensure the consistent adherence to AML policies and procedures, reinforce the importance of detecting and reporting suspicious activities associated with the FinCEN AML Priorities, and provide valuable insights for program enhancement.

CONCLUSION

By aligning AML programs with the FinCEN AML Priorities, financial institutions demonstrate their commitment to combating financial crime and promoting a safer and more transparent financial system. Corruption, cybercrime, terrorist financing, fraud, transnational criminal organization activity, human trafficking, smuggling, and proliferation financing are all significant concerns that require dedicated attention. Financial institutions that integrate these priorities into their AML programs strengthen their governance frameworks, leverage technology and data analytics, and foster a culture of continuous improvement are better prepared to address the evolving risks posed by these priorities and maintain compliance with regulatory requirements.

Acknowledgments

We would like to thank [Adil Raza](#) for providing insight and expertise that greatly assisted this research.

[Adil Raza](#) is a Managing Director in J.S. Held's [Global Investigations Practice](#) and specializes in financial crimes risk management. He has more than 13 years of global experience assisting clients with complex anti-money laundering (AML), global sanctions, regulatory compliance, and risk management matters. He collaborates with clients to evaluate their existing AML procedures and implement new programs to ensure regulatory compliance. His areas of expertise include ensuring compliance with the Bank Secrecy Act (BSA), Know Your Customer (KYC) regulations, suspicious activity monitoring and reporting requirements and Office of Foreign Assets Control (OFAC) sanctions compliance requirements.

Prior to joining J.S. Held, he led the AML subsegment within the forensics practice of a major consulting firm. He also served as the head of the U.S. Financial Intelligence Unit for two banking institutions where he was responsible for leading a team of AML investigators.

Adil can be reached at adil.raza@jsheld.com or +1 718 750 9739.

This publication is for educational and general information purposes only. It may contain errors and is provided as is. It is not intended as specific advice, legal or otherwise. Opinions and views are not necessarily those of J.S. Held or its affiliates and it should not be presumed that J.S. Held subscribes to any particular method, interpretation or analysis merely because it appears in this publication. We disclaim any representation and/or warranty regarding the accuracy, timeliness, quality, or applicability of any of the contents. You should not act, or fail to act, in reliance on this publication and we disclaim all liability in respect to such actions or failure to act. We assume no responsibility for information contained in this publication and disclaim all liability and damages in respect to such information. This publication is not a substitute for competent legal advice. The content herein may be updated or otherwise modified without notice.