CEP Magazine - May 2021

Financial fraud, terrorist financing, and money laundering: Trials and trends

---

By Ambler T. Jackson, Attorney

Ambler T. Jackson (amblertjackson@gmail.com) is a governance, risk, and compliance consultant focused on data management, privacy, and security matters in Washington, DC.

- linkedin.com/in/amblertjackson
- @amblerjackson

Organizations in the financial services industry, such as banks and credit card companies, have a responsibility to protect their customers and organizations through fraud prevention, counter terrorist financing (CTF), and anti-money laundering (AML) compliance. Financial institutions are increasingly addressing risks associated with sophisticated financial fraud, terrorist financing, and money laundering due to the many digital products and automated services available to customers and new criminal opportunities for individuals and organizations. Banks are most vulnerable to crimes such as fraud and money laundering, and the solutions to their challenges, including implementing measures necessary for meeting regulatory compliance requirements, can be costly.

A holistic approach to the prevention of fraud, terrorist financing, and money laundering, complete with integration of other related functions, automation of controls, information and data sharing, and the consistent use of AML/CTF tools, will ensure greater efficiency and effectiveness of compliance programs focused on mitigating risks associated with financial crimes. This article focuses on the challenges and trends affecting financial institutions and their efforts to prevent financial fraud, terrorist financing, and money laundering.

Background, regulation, and enforcement

In general, AML addresses the detection and prevention of money laundering activities, as well as an organization's compliance with AML laws and regulations. As background, the role of the U.S. national banking system in helping the AML effort began in 1970 with the Bank Secrecy Act (BSA), the primary anti-laundering law in the US; the Office of the Comptroller of the Currency (OCC) was established soon thereafter.[1] The OCC conducts regular examinations of national banks and has supervisory, regulatory, and enforcement authority.[2]

Congress passed the USA Patriot Act (Patriot Act) after the attacks of September 11, 2001, which deters and punishes terrorist acts and strengthens US measures to prevent, detect, and prosecute international money laundering and financing of terrorism.[3] The Patriot Act requires every bank to adopt a customer identification program as part of its BSA compliance program. One of the most important requirements of the BSA is to submit a suspicious activity report (SAR). The purpose of filing a SAR is to identify violations or potential violations of law to the appropriate law enforcement authorities for criminal investigation.

In addition to being the subject of an enforcement action and sanctions, noncompliance with AML laws may result in reputational harm to financial institutions. In fact, a financial institution's image can be eroded if it becomes associated with criminals or criminal enterprises. Therefore, it is important to comply with all AML laws and regulatory requirements.

Financial fraud

Fraud is a deliberate misrepresentation of the truth or concealment of a material fact to induce another to act to their detriment. Some common forms of fraud include bank fraud, internet fraud, and check fraud.[4] Some activities lead to fraud, such as identity theft, which happens when someone steals personal information and uses it to commit fraud. Another common type of fraud is credit card fraud, which is the fraudulent use of a credit or debit card to obtain money or property.[5]

The financial services industry has been significantly affected by a spike in fraud activities due to the global pandemic.[6] Consider also that as banking transactions become more automated, the risk of financial fraud and cybercrime increases. An organization's ability to mitigate risks associated with fraud depends on its overall risk strategy, an understanding of the connection between financial fraud and cybercrimes and cybersecurity, and an awareness of internal and external threats, which requires strong identification and monitoring capabilities. Because fraud and cybercrime are interrelated—and to keep pace with the evolving risk landscape—organizations are integrating fraud and cybersecurity operations to more efficiently manage the risks associated with fraud and cybercrime. This results in enhanced information sharing and coordination across business lines.[7]

Money laundering and terrorist financing

The act of using the financial system to support terrorists or acts of terrorism is referred to as terrorist financing. The criminals are known as terrorist financiers.[8] Terrorist financiers use the formal financial system and other methods to disguise the illegal proceeds of their crimes. Strong AML/CTF tools are necessary to prevent the terrorist financiers from succeeding.[9] The financial industry plays a key role in countering the financing of terrorism by identifying and reporting suspicious activity as required under the BSA discussed above.

The United States Department of the Treasury (Treasury) has oversight over AML and CTF. The Financial Crimes Enforcement Network (FinCEN), one of Treasury's bureaus, supports law enforcement investigative efforts and fosters interagency and global cooperation against domestic and international financial crimes. Banks must establish an effective BSA compliance program to support CTF. They must also establish effective customer due diligence systems and monitoring programs; screen against the Office of Foreign Assets Control (OFAC), another Treasury bureau, and other government lists; establish an effective suspicious activity monitoring and reporting process; and develop risk-based anti-money laundering programs.[10]

Money laundering, which the financial services industry is especially vulnerable to, generally refers to financial transactions in which criminals attempt to disguise the proceeds, sources, or nature of criminal activities. Crimes such as money laundering facilitate a broad range of serious underlying criminal offenses and ultimately threaten the integrity of the financial system.[11] Organizations must do their part to support AML efforts. This requires an awareness of the shifting profile of financial crimes, cybercrime, and the pathways to these crimes.

The Patriot Act requires financial institutions to establish money laundering programs. At a minimum, the program must include the development of internal policies, procedures, and controls; the designation of a compliance officer; an ongoing training program; and an independent audit function to test the program.[12] Organizations can ensure that their compliance and ethics team members are BSA compliant by:

- Providing opportunities to gain AML and CTF knowledge, awareness, and training

- Providing opportunities and tools that highlight the risks for AML activities in each jurisdiction
- Monitoring changing financial behaviors and transactions
- Performing due diligence to review transactions that raise red flags
- Using innovative approaches such as artificial intelligence (AI)

Trends to meet an evolving landscape

Trends related to preventing financial CTF and AML reveal new opportunities for criminals due to the impact of the COVID-19 pandemic and related financial relief programs; increased global regulation and enforcement; the adoption of technology to enhance and improve the identity and verification requirements, including the use of AI-based solutions; and increased data collaboration and data sharing internally and between regulators and law enforcement agencies.

Trends also show an uptick in enforcement actions. Globally, enforcement actions and penalties for noncompliance with AML regulations have been increasing.[13] US regulators have historically been the toughest enforcers of AML rules, but their European counterparts have been closing the gap.

Information sharing is key to mitigating risks associated with fraud, terrorist financing, and money laundering. The risk landscape requires increased collaboration now more than ever. Data collaboration and sharing between regulators and law enforcement continues to be necessary yet challenging—and, in some regard, significantly lacking. The evolving risk landscape also means risk indicators need to be regularly updated and adjusted, and effective ongoing communication between the public and private sectors is needed to share information as the risks change over time.

Global pandemic

After the World Health Organization declared the COVID-19 outbreak an international pandemic and countries began providing stimulus funds to citizens, criminals saw new opportunities to commit crimes and launder the money from those crimes,[14] including virtual assets used for criminal activity, because they offer multiple possibilities for hiding the origins of acquired assets. Changes in customer financial behavior have also presented criminals with opportunities to commit crimes and launder the proceeds.[15] Other types of criminal activities that are giving rise to money laundering include several types of fraud, including investment fraud, charity fraud, and abuse of economic stimulus programs.[16]

Technology

Prevention of criminal activities such as fraud, terrorist financing, and money laundering depends on the ability to identify, monitor, and respond to these activities. Today's financial institutions have more effective tools at their disposal to confront these activities than in years past. For example, banks are turning to digital, AI-based solutions with identity and verification capabilities to mitigate risks and tackle compliance with greater efficiency. These solutions help financial institutions ensure that customers are who they say they are through features like facial comparison ID verification. Know Your Customer (KYC) presents areas of opportunities for technology vendors, as well as challenges for organizations that want to ensure that they invest in the very best KYC technology. AI, which comprises many branches such as machine learning and natural language processing, is the bedrock of many new technologies for KYC and AML compliance.

As organizations strategize and invest in technology to mitigate risks associated with fraud and maintain compliance with AML/CTF laws, they are considering technology that is capable of identifying and monitoring activities that suggest the existence of financial crimes; identifying and monitoring virtual assets have been a challenge for some organizations.[17] False positives continue to present challenges to organizations when monitoring for suspicious activity as they result in significant resources focused on investigating low-risk accounts and transactions. Organizations are, therefore, considering options that improve AML/CTF compliance efforts, such as complex monitoring of virtual assets, to help lessen the frequency of false positives.

Meet the challenges

Successful organizations that strategically invest in capabilities to prevent fraud, terrorist financing, and money laundering focus on strengthening governance and risk management practices with automation and identity and verification technology, tools that improve the quality of data, transaction monitoring, real-time detection and prevention, and reporting of suspicious activity. Organizations should also consider evaluating their entire KYC and AML process from start to finish.[18] Setting up a holistic center of excellence to enable end-to-end decision-making across fraud and cybersecurity operations will also help organizations reach their fraud prevention, CTF, and AML goals.[19]

As financial institutions continue to meet the challenges associated with increased fraudulent activity due to the financial impact of the pandemic, compliance teams can increase the effectiveness and efficiency of their programs by applying a holistic approach to the prevention of fraud, terrorist financing, and money laundering. This includes assessing the program to identify inefficiencies and evaluating new technologies that will improve key elements such as KYC, transactions monitoring, investigations and reporting, integration of other functions, data collection, and information sharing.

Takeaways

- Approach preventing fraud, terrorist financing, and money laundering holistically to mitigate risks within the financial services industry.
- Invest in compliance program training and awareness for leadership and team members to keep pace with challenges and trends unique to the financial services industry.
- Invest in technology capabilities that support detection and identification of customer financial behavior, monitoring, and Know-Your-Customer requirements.
- Understand the relationship between fraud and cybercrime, and integrate fraud and cybersecurity operations accordingly to achieve success in mitigating related risks.
- Position risk management departments and compliance programs to successfully address challenges such as pandemic-related fraud and virtual assets used for criminal activity.

[1] “Bank Secrecy Act (BSA) & Regulated Regulations,” Office of the Comptroller of the Currency, accessed March 16, 2021, http://bit.ly/3rTXgGh.
[2] “What We Do,” Office of the Comptroller of the Currency, accessed March 16, 2021,http://bit.ly/3vvc0xk.
[3] “USA Patriot Act,” Financial Crimes Enforcement Network, accessed March 16, 2021, http://bit.ly/3bWJs8x.
[4] “Financial Fraud Crimes,” Department of Justice, United States Attorney’s Office for the District of Alaska, updated February 5, 2020, http://bit.ly/3czVZ0I.
[5] “Scams and Safety,” Credit Card Fraud, FBI, accessed March 16, 2021, http://bit.ly/3s64hE9.
[6] “Fraud continues to grow for financial services and lending firms, both before and during the pandemic,”

Security, October 14, 2020, http://bit.ly/3qQdui7.

[7] Salim Hasham, Shoan Joshi, and Daniel Mikkelsen, "Financial crime and fraud in the age of cybersecurity," McKinsey & Company, October 1, 2019, http://mck.co/3eKoUBV.

[8] Bureau of International Narcotics and Law Enforcement Affairs, "Anti-Money Laundering and Countering the Financing of Terrorism," U.S. Department of State, accessed March 16, 2020, https://bit.ly/3tveXwj.

[9] Bureau of International Narcotics and Law Enforcement Affairs, "Anti-Money Laundering."

[10] "Bank Secrecy Act (BSA)," Office of the Comptroller of the Currency, accessed March 16, 2021, http://bit.ly/30LmieG.

[11] "Money Laundering," U.S. Department of the Treasury, accessed March 16, 2021, http://bit.ly/3bSoLdO.

[12] "USA Patriot Act," Financial Crimes Enforcement Network.

[13] Deborah Luskin, Anant Modi, Selma Della Santina, and Sarah Wrigley, "Anti-Money Laundering Trends and Challenges," *Europe, Middle East and Africa Investigations Review 2020*, Law Business Research, June 2020, https://bit.ly/2PZO98L.

[14] "Home," Financial Action Task Force, accessed March 16, 2021, http://bit.ly/3vEvKir.

[15] Financial Action Task Force, *Update: COVID-19-related Money Laundering and Terrorist Financing*, December 2020, https://bit.ly/3rS8rz6.

[16] Financial Action Task Force, *Update.*

[17] "Home," Financial Action Task Force.

[18] Susan Hackett, "FinTech: Reinforcement for Banks' AML (Anti-Money Laundering) Efforts," Thomson Reuters, accessed March 16, 2021, http://tmsnrt.rs/2No3zCR.

[19] Salim Hasham, Shoan Joshi, and Daniel Mikkelsen, "Financial crime."