



Financial Crime

Fall 2025

Regulatory Shifts,
Supervisory Focus,
and Emerging Risks





Executive summary

The financial crime compliance landscape in 2025 is being reshaped by technological innovation, evolving threats, and a wave of regulatory reforms. Governments and supervisory bodies are intensifying their scrutiny of data integrity, sanctions screening, and beneficial ownership transparency, while simultaneously seeking to modernize the U.S. Anti-Money Laundering (AML) regime. This white paper highlights six key themes shaping the future of financial crime compliance and outlines strategic considerations for financial institutions and compliance leaders.



Theme 1

AI and machine learning in financial crime prevention

Artificial intelligence (AI) and machine learning (ML) are transforming how financial institutions detect and prevent financial crime. While there is a clear signal from regulators encouraging innovative technologies to enhance financial institutions' compliance programs, there remains a steady emphasis on transparency, explainability, and accountability.

California's Transparency in Frontier AI Act (September 2025) set a precedent by requiring large AI developers to publicly disclose risk mitigation frameworks and report safety incidents. While the law targets frontier models, its implications for regulated industries are profound, raising expectations for model governance, testing, and auditability. Further, we need to consider that if one state has released guidance related to AI, more will likely follow.

In parallel, regulators globally are pushing back against "black box" AI. The EU AI Act and U.S. Treasury AML guidance both underscore that institutions must understand and explain model-driven decisions, particularly those that affect sanctions screening or suspicious activity report (SAR) filings. Model interpretability tools such as SHAP and LIME are becoming compliance essentials.

Recent research from the Federal Reserve Board found that large language models (LLMs) reduced sanctions screening false positives by 92% and improved detection rates by 11% compared to traditional fuzzy matching, though at slower processing speeds. These results suggest that machine learning can dramatically enhance sanctions and adverse media screening when paired with strong governance and documentation.





Theme 2

Modernizing the U.S. AML regime

Five years after the Anti-Money Laundering Act of 2020 (AMLA), several key provisions remain unimplemented, leaving financial institutions navigating uncertainty. Outstanding areas include expanded whistleblower protections, enhanced penalties for repeat BSA violators, and the full rollout of FinCEN's beneficial ownership database.

Senior Treasury officials have reinforced the administration's commitment to modernization. In recent remarks, Deputy Secretary Faulkender emphasized streamlining SAR and CTR reporting and empowering institutions to focus resources on higher-risk threats. However, tangible supervisory change will take time, as Section 6307 of the AMLA mandates examiner training and regulatory culture often evolves more slowly than policy.

FinCEN's FAQs on Suspicious Activity Reporting from October 2025 further confirm the general direction of regime change. The FAQs align in spirit with the AMLA Section 6204, which requires a formal review of SAR (and currency transaction report) requirements to reduce unnecessary burdens. While the true impact of the FAQs remains to be seen, we remain optimistic of further updates to reach FinCEN Director Gacki's vision of an AML/CFT regime that is "effective, risk-based, and focused on the greatest threats to financial institutions and national security."



The October 2025 FAQs also signal a shift toward supervisory expectations that better distinguish between truly suspicious behavior and routine regulatory filings made out of an abundance of caution. Notably, the guidance encourages institutions to leverage their existing risk assessments and focus on reporting activity with meaningful intelligence value to law enforcement. Although the FAQs do not modify regulatory obligations themselves, they provide a clearer framework for exercising judgment, prioritizing high-risk cases, and reducing "defensive filing" behaviors. Over time, this may reshape examiner-institution dialogue and incentivize investments in investigative quality over filing volume.



Theme 3

The evolving payments landscape

The payments ecosystem is undergoing rapid transformation driven by new messaging standards and real-time capabilities. The coexistence period for ISO 20022 payment instructions is ending, ushering in structured, data-rich messages that enhance sanctions filtering and reconciliation. Supervisors are closely scrutinizing how institutions configure and leverage this data.

Meanwhile, real-time payment (RTP) systems such as FedNow introduce compliance challenges. Instant settlement leaves little time for sanctions screening or fraud interdiction, raising the stakes for pre-transaction controls. Limited message data and finality of payments amplify both compliance and reputational risk.

In addition, the Financial Action Task Force (FATF) issued updated guidance to the Travel Rule in 2025, including efforts to clarify the beginning and end points of international value transfers to address risks associated with nested MSB and similar intermediary structures. The updates also expand expected coverage to non-custodial wallets and decentralized platforms, and lower the recommended reporting threshold to USD \$250 in many jurisdictions. While FATF standards themselves do not carry the force of law, they continue to drive regulatory reform globally, particularly in regions such as the EU that closely align their legal frameworks to FATF recommendations, accelerating compliance expectations for payment service providers and virtual asset service providers.





Theme 4

Data quality and model validation

Supervisors are increasingly viewing data governance as foundational to effective financial crime risk management. Examiners now expect institutions to demonstrate robust data lineage (the ability to trace data from source to decision) and implement comprehensive data integrity programs across AML, OFAC, and transaction monitoring systems.

Recent enforcement actions, such as the Wells Fargo Consent Order, mandate the establishment of enterprise-wide data integrity programs to validate that BSA/AML and OFAC systems are “commensurate with the bank’s risk profile.” Regulators are probing false negative rates, model tuning practices, and the explainability of AI-driven detection systems, pushing compliance teams to elevate their validation frameworks.



Theme 5

Whole-of-government approach to countering fentanyl

The administration’s Executive Order 14157 (January 2025) reframed the fight against fentanyl trafficking as a national security issue. By designating certain cartels as Foreign Terrorist Organizations (FTOs) and Specially Designated Global Terrorists (SDGTs), the U.S. government expanded the use of sanctions and asset-blocking authorities traditionally reserved for counterterrorism.

The Office of Terrorism and Financial Intelligence, including OFAC and FinCEN have since issued multiple geographic targeting orders (GTOs), civil money penalties, and advisories to financial institutions. Financial institutions are responding by enhancing sanctions screening and monitoring programs, particularly for high-risk correspondent banking relationships and cross-border transfers linked to Mexico.



Theme 6

Administration actions impacting financial crimes compliance

A series of executive orders in 2025 reflect broader shifts in the regulatory philosophy governing financial services. Executive Order 14331 (August 2025) directed regulators to eliminate guidance referencing “reputational risk” and to review institutions for potentially unlawful debanking practices. The order also instructed the Small Business Administration (SBA) to require reinstatement of customers denied access based on such policies, introducing new compliance and legal complexities. In parallel, the OCC declared that it would eliminate reputational risk as a standalone category in its examinations of national banks and federal savings associations. This means that the OCC will no longer assess reputational risk as a separate scope area but

will instead evaluate any related concerns through established risk areas such as operational, compliance, or credit risk. FDIC followed suit, removing references to reputational risk from the examination and other materials.

Simultaneously, Executive Orders 14192 and 14219 launched a deregulatory push. Agencies must now identify and repeal ten existing regulations for every new one proposed and review existing rules to ensure consistency with statutory authority. The end of Chevron deference further constrains agency discretion, signaling a long-term recalibration of how financial regulations are interpreted and enforced.



Conclusion

Strategic outlook

As financial crime risks evolve, regulatory and supervisory expectations are becoming more dynamic and data-driven. Financial institutions must balance innovation with control, leveraging AI and real-time analytics within robust governance frameworks. Our team recommends that clients prioritize:

- Strengthening model governance to meet explainability and auditability requirements.
- Enhancing data integrity across AML and sanctions systems to serve as a foundation for effective future AI and automation efforts.

- Modernizing payment compliance to keep pace with instant and cross-border systems.
- Integrating policy intelligence into enterprise risk management to anticipate and adapt to regulatory change.

In a landscape defined by both technological opportunity and regulatory uncertainty, agility and collaboration will be the defining traits of resilient compliance programs.

Contact us

Michaela Soctomah
Principal
E: msoctomah@kpmg.com

Jared Ott
Director
E: jaredott@kpmg.com

Lauren Santilli
Manager
E: lsantilli@kpmg.com

Maura Holst
Senior Associate
E: mholst@kpmg.com

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

Learn about us:



[kpmg.com](https://www.kpmg.com)

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act upon such information without appropriate professional advice after a thorough examination of the particular situation.

© 2025 KPMG LLP, a Delaware limited liability partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved. The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organization. USCS036541-2A