



Insights

Regtech Whitepaper | March 2024

Regulatory Technology and Modern Banking: A 2024 Outlook

Navigating Compliance, Fraud, and Risk in a Digitally Driven Financial Landscape

Key Takeaways



Financial institutions (FIs) continue to face record levels of fraud and financial loss, escalating compliance costs, and a challenging regulatory environment.



To effectively combat these growing risk and regulatory burdens, FIs have access to an array of Regulatory Technology solutions to streamline compliance efforts and enhance risk management.



The Regulatory Technology sector is still in the early stages of maturity and adoption, but demand is growing as historically risk averse FIs face the reality that, to stay ahead of bad actors and evolving regulatory requirements, they need innovative solutions that keep them apace of threats and regulatory requirements.

In today's digitally driven financial landscape, banks and other financial institutions face increasing regulatory burdens and commercial risk. Fraud and financial crimes are more rampant and sophisticated than ever, leading to increased regulatory scrutiny on top of the already complex compliance and reporting requirements that FIs face.

01

Globally, an estimated \$3.1 trillion in illicit funds flowed through the financial system and FIs lost a collective \$485.6 billion in 2023.¹

02

Federal Trade Commission data reports that U.S. adults lost a record \$10 billion to fraud in 2023, compared to \$8.9 billion in 2022.²

03

98% of FIs have experienced increased financial crime compliance costs, which totaled \$61 billion annually in the U.S. and Canada in 2023.³

04

Federal regulators including the Securities and Exchange Commission (SEC), Financial Crimes Enforcement Network (FinCEN), Consumer Financial Protection Bureau (CFPB), Office of the Comptroller of the Currency (OCC), Federal Reserve Board (FRB), and Financial Stability Oversight Council (FSOC) "are taking actions to close gaps in regulatory coverage as well as expand coverage within their supervisory authorities to address market changes."⁴

Losses, fraud, and regulatory burdens are at an all-time high. Compliance and anti-financial crime measures are essential for banks to uphold regulatory standards, mitigate risks, and maintain trust and integrity in the financial system. It's increasingly clear that they need innovative solutions to get there.



"As regulatory requirements continue to evolve and financial crime threats become more advanced, the demand for new solutions only continues to grow," said Ganesh Rao, Managing Director and Head of Financial Technology & Services, THL.

"While still in the early innings of maturity, the Regulatory Technology market holds immense promise for its potential to revolutionize how banks streamline their compliance efforts and enhance risk management."

Compliance and Reporting Requirements

The US banking industry is governed by regulatory bodies (e.g. Federal Reserve, SEC, FinCen, etc.) that enforce a complex network of laws and regulations aimed at promoting stability and consumer protection. Internationally, organizations like the Basel Committee on Banking Supervision set global standards for banking regulation, requiring compliance from banks operating across borders.

FIs are required to report on their anti-money laundering (AML) and know your customer (KYC) procedures, capital reserves, derivatives trading, executive compensation, financial metrics, practices in risk management, consumer protection, data privacy, and cybersecurity – to name a few.

Meeting compliance and reporting requirements present numerous cross-functional challenges for banks. For example, the need for extensive documentation, data collection, and regulatory filings often involves manual processes, siloed systems, and data fragmentation. What's more, the sheer volume of regulations and the dynamic nature of the regulatory landscape make it difficult for banks to stay abreast of new requirements and ensure ongoing compliance.

Thomson Reuters Regulatory Intelligence's 2023 Cost of Compliance Report⁵ found that, in 2022, there were 61,228 regulatory events – meaning, actions or outcomes that result from the implementation or change of laws, regulations, or guidelines by a governing body. This number represented the third-highest annual total since 2008. These events included 1,374 regulators in 190 countries, or the equivalent of 234 daily regulatory alerts. The report also found that the volume of regulatory change, a key compliance challenge for banks, was expected to increase over the next 12 months, with more than half of respondents anticipating more time spent liaising and communicating with regulators and exchanges. As a result, compliance teams and costs are growing, as are the number of firms outsourcing compliance efforts to third parties.





“Banks need a more efficient way to stay compliant and mitigate risk,” said **Brian Radic**, Managing Director, THL. “Regulatory Technology solutions that automate compliance reporting and cover real-time monitoring, visibility, and surveillance to prevent fraud can help cover both sides of the regulatory-risk burden banks face.”

Anti-Financial Crime Measures

The financial crimes landscape is fast-evolving. Bad actors are getting better at exploiting vulnerabilities in the financial system and avoiding detection. As such, banks are at greater risk of direct financial losses, reputational damage, and legal liabilities.

AML & Anti-Fraud regulations mandate strict compliance measures that include robust customer due diligence processes, ongoing transaction monitoring, suspicious activity reporting, employee training, and regular audits. Still, detecting and preventing financial crimes is difficult for banks because fraudsters are continuously adapting and refining their tactics to avoid getting caught. They exploit weaknesses in systems and processes and use AI and machine learning to perfect their schemes, which adds another layer of complexity for fraud management teams. The emergence of generative AI-based scams has further exacerbated the problem because fraudsters are able to create convincing impersonations and manipulate data in their favor. For instance, generative AI can mimic a person’s voice, which fraudsters leverage to make phony calls to FIs to request fund transfers or gain access to sensitive data.

Financial institutions need innovative fraud detection strategies that put them a step ahead of bad actors. Leveraging Regulatory Technology has become instrumental for banks in bolstering their AML and fraud prevention efforts, and point solutions exist across key anti-financial crime categories. For example

- 01** **Threat intelligence** provides banks with valuable insights into emerging threats and vulnerabilities, enhancing their ability to proactively combat financial crime.
- 02** **Orchestration platforms** facilitate management of multiple solutions and coordinate responses across vendors, enabling an agile and holistic approach to AML and fraud detection.
- 03** **KYC and know your business (KYB) solutions** allow FIs to streamline compliance procedures, automate identity verification, and risk assessment tasks.
- 04** **Advanced data analytics and machine learning** enable banks to analyze vast amounts of data and detect suspicious patterns indicative of financial crimes.
- 05** **Transaction monitoring systems** play a crucial role in flagging suspicious transactions in real-time, allowing banks to take swift action and mitigate risk.
- 06** **Automated investigations** enhance efficiency by enabling banks to conduct thorough and timely inquiries into suspicious activities.

While FIs need to mitigate risk with these and other strategies, they also need to maintain regulatory conformity, especially as federal requirements evolve. This sets the stage for a deeper exploration of the connection between risk and compliance.



Regulatory Compliance and Anti-Financial Crime Synergy

The intersection of regulatory compliance and anti-financial crime measures is crucial for banks to effectively combat illicit activities and adhere to regulatory standards. There is a natural overlap between regulation compliance and financial crime prevention. For example, AML regulations require FIs to implement robust procedures to detect and prevent money laundering activities, which inherently align with efforts to combat financial crime. By adhering to AML requirements, banks fulfill their regulatory obligations and actively contribute to efforts to thwart illicit financial activities like money laundering and terrorism financing.

This is why a comprehensive Regulatory Technology strategy is crucial. Clear visibility into all risk-related information and activities, along with seamless integration of risk-related data and processes, provides FIs with a complete picture of their risk exposure and compliance status. Having this kind of contextual awareness can lead to more effective mitigation and adherence processes. All to say, FIs still largely run on legacy systems, the Regulatory Technology sector is fragmented, and security teams often layer multiple single point solutions together to maximize their coverage.

“An integrated approach to Regulatory Technology is crucial to avoid gaps and inefficiencies in risk management,” said Stephen Lantz, Principal, THL.

“Today, we most firms use a ‘Swiss cheese approach’ where each layer of protection is a slice of Swiss cheese – there are obvious holes, but if a bad actor gets through one, they’ll hit another layer that will hopefully stop them. Of course, this isn’t optimal long-term, and results in a patchwork of overlapping solutions. The future should bring better integration and interoperability across the Regulatory Technology landscape.”

By definition, integration and interoperability capabilities would enable Regulatory Technology solutions to seamlessly exchange data and work alongside existing systems to streamline a bank’s risk and compliance efforts.

Future Trends and Considerations

Looking ahead, the future of Regulatory Technology in banking is poised for significant evolution, driven by changing regulatory landscapes and technological advancements.

The emergence of gen AI and the continued use of artificial intelligence and machine learning pose both a threat and an opportunity. On one hand, these technologies help bad actors devise and execute intricate scams that are difficult to detect and prevent. On the other hand, they can be used as tools to enable FIs to strengthen fraud prevention strategies and help automate compliance and reporting processes.

While 98% of FIs recognize a need for gen AI as a solution to combat fraud and financial crime, only about half (52%) plan to implement solutions using AI technologies and machine learning.⁶ A majority (70%) are still in the process of learning about them and understanding their business and regulatory implications.⁶

AI aside, 27% of FIs confirmed the active implementation of new risk mitigation strategies in 2023, a substantial increase from the 10% reported in 2022.⁶ Overall, while adoption of these technologies is low, the industry's view is cautiously optimistic.

Getting Involved in Regulatory Technology

Regulatory technology has the potential to transform how banks mitigate risk and stay compliant, especially as the regulatory environment gets more complex and bad actors get more sophisticated. By leveraging technology solutions that use AI and ML, banks can meet regulatory requirements and detect and prevent financial crimes at scale.

As a starting point, we recommend banks conduct thorough assessments of their regulatory compliance and financial crime prevention needs, identify gaps and inefficiencies in their current processes, and select Regulatory Technology providers that offer comprehensive and customizable solutions tailored to their specific requirements.

“

“Despite the ongoing arms race between financial institutions and bad actors, we remain bullish on Regulatory Technology as a crucial part of a bank’s risk-compliance strategy,” said Rao.

“As banks continue getting comfortable with these technologies, we anticipate growth in spend and increased demand for innovative solutions that provide visibility, seamlessly integrate, and address regulatory concerns.”

To learn more about how THL's involved in Regulatory Technology and Bank Technology, contact our team today:



Ganesh Rao,
Managing Director and Head of Financial
Services Technology
grao@thl.com



Brian Radic,
Managing Director
bradic@thl.com



Stephen Lantz,
Principal
slantz@thl.com

dun & bradstreet

experian.

FIS

BLACK KNIGHT

optimalblue

odessa

¹ 2024 Global Financial Crime Report. Nasdaq Verafin. 2024.

² U.S. adults lost a record \$10 billion to fraud in 2023. Axios. February 2024.

³ True Cost of Financial Crime Compliance Study 2023 US and Canada. Forrester Research, Inc. study commissioned by Lexisnexis Risk Solutions. November 2023.

⁴ Regulatory Recap: February 2024 At A Glance. KPMG. February 2024.

⁵ 2023 Cost of Compliance. Thomson Reuters Regulatory Intelligence. May 2023.

⁶ The State of Fraud and Financial Crime in North America: The 2023 Annual Report. Featurespace. December 2023