Financial Crimes Compliance: Thinking Beyond the Rulebook

The financial sector is witnessing a surge in sophisticated financial crimes, from deepfake scams and crypto-based laundering to AI-driven cybersecurity threats, further intensified by the rapid adoption of emerging technologies like AI, blockchain, and RegTech. As these threats become more complex and widespread in nature, financial institutions need to navigate a landscape of complex and evolving regulatory requirements.

This POV explores the evolving Financial Crimes Compliance (FCC) landscape and the changing requirements from regulatory bodies. It also highlights the critical role of AI in FCC operations such as enhancing onboarding due diligence, customer monitoring, automating transaction reviews for SAR narration, reducing false positives in payment and sanction screening, detecting emerging AML and fraud threats, automating compliance processes, managing risks, and strengthening operational resilience while improving customer experience. The POV also stresses the need for a proactive, adaptable, and scalable strategy to fight financial crimes.

The New Face of Financial Crimes in a Data-Driven World

As more customer interactions, transactions, and identity checks happen online, financial crimes have become more sophisticated. AI has further amplified the threats by enabling synthetic identities, deepfake impersonation, insider collusion, and regulatory evasion. Key issues include KYC, Customer Due Diligence, Ultimate Beneficiary Ownership, AML, and Fraud, with problems like poor customer identification and inadequate transaction monitoring.

What we once believed about identity, intent, and trust isn't true anymore.

In 2024, financial institutions faced penalties exceeding US $4 billion due to more than 50 consent orders, while 4 million suspicious activity reports were submitted.[1]

TD Bank appoints Compliance Officer after US $3 billion penalty post failure to KYC, EDD & AML policies.[2]

In 2023 alone, global financial institutions incurred an estimated US $500 billion in fraud losses.[3]

NatWest fined £264.8 million for anti-money laundering failures.[4]

Many financial institutions continue to depend on siloed systems and rigid compliance models that aren't built for today's dynamic, AI-driven reality. What's needed is a move away from rule-based, checkbox approaches toward an intelligence-led FCC strategy that adapts to the evolving financial crimes in real time.

Why are Traditional Defences Failing?

Legacy systems were designed for a time when risks were simpler, more predictable, and transaction based.

Today, criminals use AI to create fake identities and deceive systems, outpacing traditional controls. This has led to a widening gap between the complexity of modern financial crimes and the rigidity of traditional prevention models.

Common pitfalls include:

1. **Over-reliance on static KYC and episodic due diligence checks**
2. **Siloed fraud, compliance and cybersecurity functions**
3. **Weak orchestration between onboarding, monitoring and escalation workflows**
4. **Limited integration of regulatory mandates into day-to-day banking operations**

Fig 01: Challenges of Traditional Crime Prevention Models

The fallout is twofold: customers face delays, poor authentication, and loss of trust, while institutions deal with hidden risks, higher compliance costs, and reputation exposure.

The Rising Need for Adaptive Security in a Shifting Regulatory Climate

Financial threats are becoming faster, stealthier, and more cross-functional. In response to increasingly sophisticated financial threats, global regulatory standards are evolving to enhance accountability, transparency, and resilience. Institutions are being driven to prioritize customer privacy, strengthen internal controls, and prepare for digital disruptions, making operational stability a competitive advantage. Stricter capital and liquidity requirements promote financial resilience and trust across markets. Additionally, comprehensive anti-money laundering and terrorism financing rules focus on high-priority threats, reinforcing the security and integrity of financial systems.

The Regulation-Resilience Gap

Recent regulatory shifts, like GDPR's data responsibility and FINCEN's and AUSTRAC's AML/CFT laws and regulations, DORA's focus on operational resilience, highlight the need for compliance to be continuous, contextual, and integrated across operations. But even the best laws can't close the gap alone.

Here's the disconnect:

- Regulations offer the what, but not always the how.
- Mandates are jurisdiction-specific, while threats are borderless.
- Compliance often focuses on reporting, not risk anticipation.
- Fragmented adoption leaves institutions vulnerable at key intersections - fraud vs KYC, data vs identity, and cyber vs compliance.

To close this gap, institutions must reimagine FCC as a dynamic architecture that evolves with customer behaviour, regulatory change, and emerging threats.

Moving from Reactive to Proactive Fraud Prevention

Building a Resilient Financial Security Ecosystem: From Response to Readiness

Financial Crimes Compliance (FCC) is not a set of disconnected processes. It's an integrated approach that encompasses:

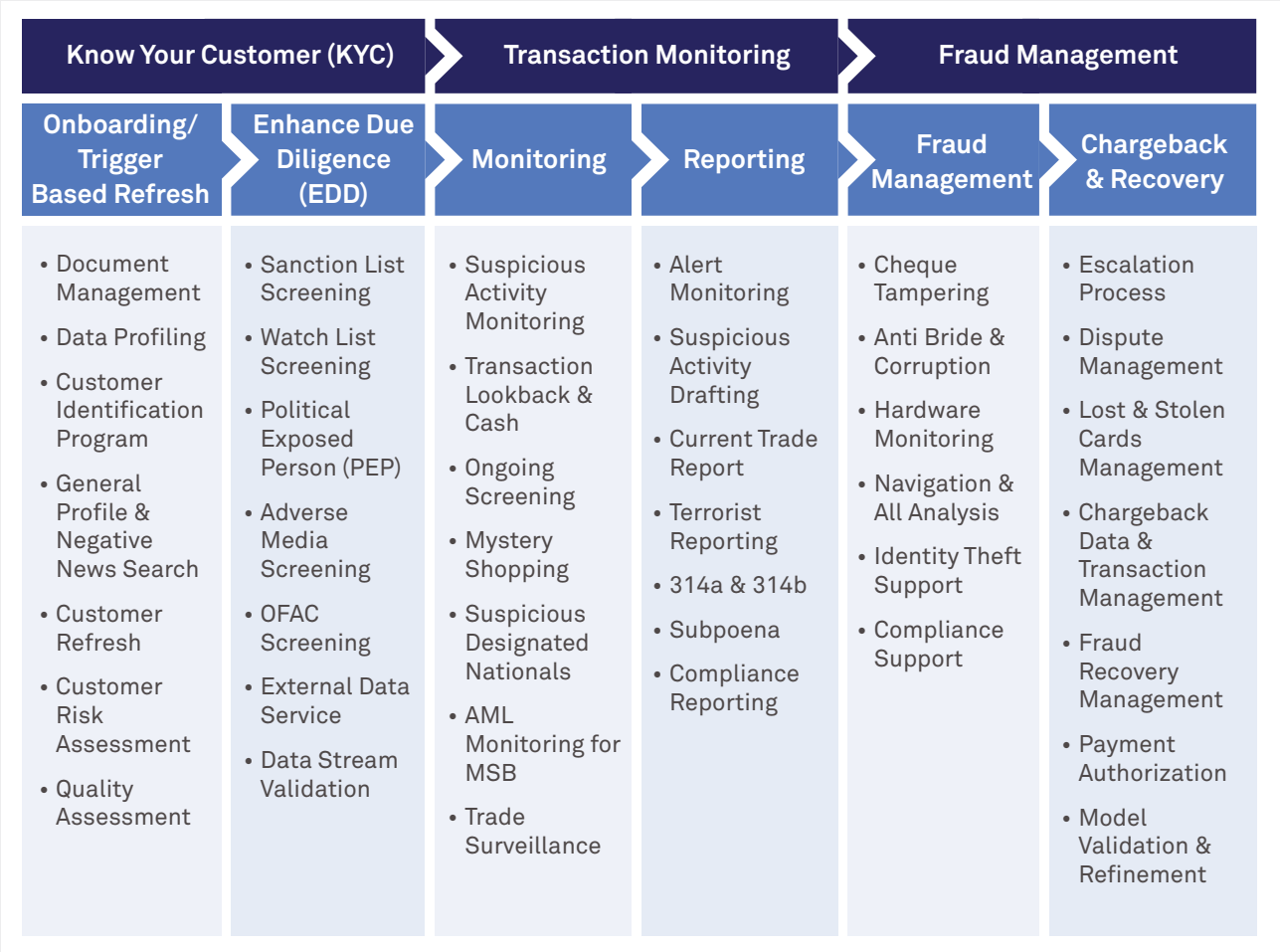

Fig 02: Pillars of an FCC Framework

To stay ahead of increasingly sophisticated threats, financial institutions must shift from static, rule-based compliance to adaptive, intelligence-led strategies. This means reimagining FCC as a dynamic ecosystem that evolves with customer behaviour, regulatory changes, and emerging threats. By building resilient, real-time defences and embracing a proactive stance, institutions can not only comply but thrive amidst the evolving landscape of financial crimes.

Sources:

[1] 4 Lessons for Firms Fighting Financial Crime in 2025

[2] Monitor Appointed in TD Bank $3 Billion Anti-Money-Laundering Settlement

[3] 2024-0208-scale-impact-3-trillion-financial-crime-webinar-slides-verafin.pdf

[4] NatWest fined £264.8 million for anti-money laundering failures

Wipro Limited
Doddakannelli
Sarjapur Road
Bengaluru – 560 035
India

Tel: +91 (80) 2844 0011
Fax: +91 (80) 2844 0256
wipro.com

Wipro Limited (NYSE: WIT, BSE: 507685, NSE: WIPRO) is a leading technology services and consulting company focused on building innovative solutions that address clients' most complex digital transformation needs.

Leveraging our holistic portfolio of capabilities in consulting, design, engineering, and operations, we help clients realize their boldest ambitions and build future-ready, sustainable businesses. With over 230,000 employees and business partners across 65 countries, we deliver on the promise of helping our clients, colleagues, and communities thrive in an ever-changing world.

For additional information, visit us at **www.wipro.com**

IND/WIPRO/JUL 2025 – JUN 2026