



A 1LoD report



Financial Crime

LEADERS' NETWORK

NEW YORK

FORECAST 2026

Future Proofing Financial Crime: AI Adoption, Governance Constraints and Cultural Change

SPONSORS

ORACLE

 **sigma360**

Key Takeaways

Financial crime functions remain at an early stage of artificial intelligence (AI) adoption, with most firms prioritising incremental, tightly scoped use cases over enterprise wide transformation due to data, governance, and regulatory constraints

Data quality and ownership continue to represent the most material barriers to progress, with fragmented internal systems and unclear accountability limiting confidence in advanced analytics and AI outputs

Regulatory engagement is characterised by growing openness rather than resistance, provided firms can demonstrate strong explainability, governance discipline, and clear articulation of how AI supports risk management objectives

Hybrid operating models combining established, explainable techniques with AI enabled enrichment are favoured over fully opaque approaches, reflecting both supervisory expectations and internal model risk management realities

Cultural change and capability uplift are essential enablers, with successful adoption dependent on retraining teams for oversight focused roles and addressing fears around job displacement through transparency and leadership engagement

Senior leadership plays a decisive role in enabling progress, not only by setting ambition but by actively clearing organisational barriers across governance, risk appetite, and regulatory dialogue

Reducing false positives in transaction monitoring (TM) is viewed as the clearest value opportunity, but efficiency gains must be balanced carefully against risk tolerance and the potential for heightened scrutiny following isolated failures

Meaningful progress requires iterative delivery, realistic time horizons, and alignment between business, compliance, technology, and risk functions, rather than short term mandates to automate without supporting infrastructure



Subscribe here
to receive new content
and event information
directly to your inbox

Future Proofing Financial Crime: AI Adoption, Governance Constraints and Cultural Change

Participants gathered for the morning Financial Crime Leaders' Network where they examined the accelerating pressure on financial crime functions to adopt advanced technologies, particularly AI, while operating within persistent data, governance, and regulatory constraints. Discussions consistently returned to the tension between ambition and readiness: senior leadership expectations to deliver AI enabled efficiencies contrasted with unresolved foundational issues around data quality, model risk management, and explainability. While there was a broad consensus that AI adoption was unavoidable, firms described themselves as still early in their maturity journey, focusing on incremental use cases, regulatory engagement, and cultural change rather than wholesale transformation.



From ambition to reality: AI adoption in the foothills

Participants broadly agreed that most institutions remained at an early stage of AI adoption within financial crime, despite growing pressure from boards and senior executives. One participant observed that firms were "still in the foothills" when it came to applying advanced technologies to evolving financial crime threats, reflecting both technical and organisational barriers. This sense of immaturity was not framed as resistance, but rather as realism about the scale of change required.

A recurring theme was the disconnect between external enthusiasm for generative AI and the operational risk profile of financial crime compliance. Participants contrasted relatively low risk uses of AI elsewhere in organisations with the high stakes consequences of failure in anti money laundering (AML) and sanctions. One participant captured this tension by noting that in financial crime, "the risk is too big to rush into" AI deployment where errors could lead to customer harm or regulatory breaches.

As a result, firms described favouring narrowly scoped proof of concepts over enterprise wide rollouts. Several participants emphasised the importance of identifying "somewhere small I can start to test this, and show that it can work," using contained use cases to build confidence and internal credibility. This incremental approach was seen as essential to balancing innovation with regulatory and reputational risk.

A recurring theme was the disconnect between external enthusiasm for generative AI and the operational risk profile of financial crime compliance.

Data quality and governance as binding constraints

Despite advances in analytics and tooling, data quality was repeatedly described as the most stubborn constraint on AI adoption. Participants characterised data challenges as longstanding, structural, and predominantly internal, driven by fragmented systems, legacy architectures, and unresolved ownership issues. One participant summarised the problem bluntly by referring to “data quality issues” that “are always interesting because... there have been concerns in the past about who owns what.”

The discussion highlighted how poor data foundations undermined confidence in more sophisticated models. Participants questioned how firms could be expected to rely on AI outputs when underlying datasets remained unreliable or incomplete. In this context, attempts to layer AI on top of weak data infrastructures were criticised as superficial fixes, with one participant warning against “putting band aids on solutions” rather than addressing root causes.

Accountability for data was therefore seen as both a governance and cultural issue. Several participants argued that unless ownership was clearly anchored in the business, financial crime teams would remain trapped in costly downstream remediation. One participant stressed that without this shift, organisations would continue “cleaning up instead of fixing things at the front end,” inflating AML and sanctions costs over time.

Regulatory engagement and the primacy of explainability

Regulatory expectations featured prominently, with participants reporting increasing interest, rather than outright resistance, from supervisors. Several described regulators as actively seeking to understand firms’ AI strategies, provided models could be clearly articulated and justified. One participant stated that regulators’ “favourite word is explainable,” emphasising that transparency was a prerequisite for supervisory comfort.

Explainability was discussed not only as a regulatory requirement but as a practical discipline shaping model design choices. Participants highlighted a preference for hybrid approaches that combined established, explainable techniques with AI driven enhancements, rather than fully opaque models. This was seen as a pragmatic response to both regulatory scrutiny and internal model risk management processes.

Model risk management itself emerged as a significant bottleneck. Participants expressed concern that traditional validation timelines were incompatible with the pace of technological change, creating a risk of firms “being left in the dust.” In response, some described evolving internal frameworks that reassessed what explainability meant in the context of generative AI, acknowledging that existing standards would need to adapt.



Culture, capability, and the human dimension

Beyond technology and governance, participants devoted significant attention to people and culture. AI adoption was framed as a shift from manual execution to oversight, requiring new skills and mindsets across financial crime teams. One participant described this transition as moving staff towards "being an overseer, not a doer," supported by extensive training and real world use cases.

Concerns about job displacement were openly acknowledged, particularly among junior staff, but many participants argued that AI offered an opportunity to redirect effort towards higher value work. The discussion emphasised that fear and resistance could only be addressed through transparency, education, and visible leadership commitment. As one participant noted, "it is a cultural shift big time, but it is also training people."

Senior leadership was repeatedly identified as critical to success, not only in setting ambition but in removing institutional barriers. Participants argued that leaders needed to "clear the path forward" by aligning governance, risk appetite, and regulatory engagement, rather than issuing abstract mandates to "automate." Without this alignment, cultural change risked stalling at the middle management level.

Redefining effectiveness in financial crime operations

The scale of inefficiency in current operating models provided a powerful impetus for change. Participants cited industry benchmarks of 80 to 90% false positives in TM as both a cost and morale challenge. One participant asked rhetorically, "what business would survive if 80% of the stuff you do is bad?" underscoring the urgency of reform.

Rather than attempting to perfect detection upfront, some participants advocated widening detection thresholds and using AI to enrich, prioritise, and rationalise alerts downstream. This reframing challenged long standing assumptions about precision versus coverage, suggesting that digital capacity could offset the historical trade off between risk sensitivity and operational cost.

However, participants were clear that such shifts required explicit agreement on risk tolerance and regulatory comfort. The possibility that "one thing gets blown up" despite overall improvements was seen as an unavoidable reality, reinforcing the need for robust testing, escalation, and governance alongside technological change.

The discussion concluded with cautious optimism. Participants agreed that the prize was significant, particularly if AI could materially reduce false positives and redirect scarce expertise towards genuine risk. At the same time, there was a shared recognition that progress would be uneven, iterative, and dependent on sustained leadership engagement. As one participant summarised, if firms could align mutual benefit, governance flexibility, and regulatory dialogue, "there is the opportunity of a big prize."

This information was taken from The Financial Crime Leaders' Network event in New York, 11 March 2026.

Upcoming Financial Crime events



2026

A 1LoD event



The Financial Crime Summit

IN-PERSON CONFERENCES



NEW YORK

11
March



SINGAPORE

22
October



LONDON

12
November

VIRTUAL EVENTS

21
April

Onboarding & KYC Deep Dive

02
June

AML Deep Dive

16
June

Fraud Risk Deep Dive

www.1lod.com