



A 1LoD report



Financial Crime

LEADERS' NETWORK

LONDON

FORECAST 2026

From False Positives to Risk Intelligence:

Enhancing Financial Crime
Effectiveness Through Data, AI and
Operating Model Transformation

SPONSOR*

KYC360
A part of  experian

*Bespoke version created for KYC360

Key Takeaways

False positives remain the single largest source of inefficiency across financial crime functions

Improving alert quality offers the greatest near-term opportunity for operational efficiency gains

Technology alone will not solve financial crime efficiency challenges

Artificial intelligence (AI) is already delivering measurable benefits across several financial crime use cases

Data quality is recognised as a foundational requirement for effective financial crime controls

Legacy systems and fragmented data architectures continue to restrict financial crime effectiveness

The industry is moving towards intelligence-led and proactive risk management

Perpetual KYC (pKYC) and event-driven monitoring are emerging as the future direction of travel

Future success would depend as much on people and governance as technology



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

Enhancing Efficiencies in the Financial Crime Function

This debate focused on how financial crime functions could improve efficiency whilst maintaining effective risk management and regulatory compliance. Participants consistently highlighted the significant operational burden created by high volumes of false positive alerts, the transformative potential of AI, the need to redesign legacy processes before automating them, and the importance of governance, skills, and risk appetite in shaping future operating models.

A clear consensus emerged that alert volumes and false positives remained one of the greatest sources of friction across financial crime operations. In sanctions screening, firms reported that substantial resources were being consumed adjudicating alerts that ultimately posed no genuine risk. One participant described how they were generating "an awful lot of false positives", which was diverting significant investigative capacity away from higher-value activity. Similar concerns were raised in transaction monitoring (TM) where participants observed that operating models had changed little over the past two decades despite large investments in technology. It was noted that many institutions continued to experience false positive rates of between 85% and 95%, with investigators spending much of their time on rapid case closure rather than performing meaningful investigations.



Against this backdrop, participants agreed that improving alert quality represented one of the most important opportunities for efficiency gains. Several organisations were already investing in enhanced screening systems, machine learning capabilities, and AI-driven models designed to reduce noise and improve risk identification. One contributor noted that "85% of what I send to investigations to look at is still rubbish", arguing that this level of inefficiency was no longer acceptable. Firms described using AI and analytical models to better prioritise alerts, identify plausible risk scenarios, and support investigators with richer contextual information. There was broad agreement that technology should enable investigators to focus on genuinely suspicious activity rather than processing large volumes of low-value alerts.

Participants also explored how AI was beginning to improve customer onboarding and Know-Your-Customer (KYC) processes. Examples were shared of plausibility models being used to assess whether customer information made commercial sense, allowing firms to reduce manual reviews and accelerate onboarding decisions. One organisation reported that onboarding turnaround times had fallen from several days to less than a day following the introduction of AI-supported reviews. Others discussed ambitions to move towards perpetual KYC models, where customer reviews would be triggered by risk events rather than fixed one-, three-, or five-year cycles. While participants acknowledged regulatory considerations and jurisdictional variations, many believed that continuous monitoring represented a more effective and efficient future state.

However, the discussion repeatedly returned to the idea that technology alone would not solve the industry's efficiency challenges. Many participants

Risk appetite emerged as another critical theme. Although technology offered opportunities to significantly reduce false positives, firms remained cautious about accepting any reduction in detection performance



argued that organisations first needed to address inefficient and overly complex processes. Several described legacy operating models that had accumulated multiple approval layers, hand-offs, and control points over many years in response to regulatory findings, audits, and accountability concerns. One participant reflected that "the processes are horrible" once examined in detail beneath the surface. Another explained that weeks of process analysis had revealed numerous activities for which nobody could convincingly explain the rationale. As a result, participants advocated process simplification, rationalisation, and clearer accountability before attempting large-scale automation.

Risk appetite emerged as another critical theme. Although technology offered opportunities to significantly reduce false positives, firms remained cautious about accepting any reduction in detection performance. Participants highlighted a tension between operational efficiency and regulatory accountability, particularly for Money Laundering Reporting Officers (MLROs), who remained personally accountable for reporting decisions. While firms were often comfortable retraining models that improved overall risk detection, there was noticeably greater resistance to optimisation initiatives that reduced false positives but could potentially miss a small number of suspicious cases. This distinction reflected both regulatory pressures and long-standing cultural attitudes towards financial crime risk management.

The debate further highlighted the growing importance of governance and data quality. Participants repeatedly emphasised that successful AI deployment depended on strong foundations, including high-quality data, robust model governance, and appropriate oversight. Several organisations described developing central governance frameworks to validate models and monitor performance, whilst allowing execution and development to remain partially

decentralised. There was also discussion around proving that AI could outperform human decision-making through back-testing and quality assurance exercises. One participant argued that organisations needed evidence demonstrating that AI performed better than human reviewers before widespread adoption would gain internal and regulatory support.

Participants also identified significant implications for workforce strategy and future operating models. There was broad agreement that many traditional alert handling roles would evolve as automation became more sophisticated. Rather than focusing on repetitive processing, future roles were expected to concentrate on critical thinking, exception management, governance, and oversight of AI-enabled processes. As one speaker observed, organisations needed to train employees to understand the "why of what we're doing" rather than simply following established procedures. Several firms reported investments in AI skills, engineering capability, and workforce development programmes designed to prepare teams for this transition.

Looking ahead, participants anticipated increasing regulatory expectations around speed, efficiency, and real-time intervention. Many observed that regulators were becoming less tolerant of lengthy investigation and reporting timelines, particularly as digital payments, blockchain technologies, and faster settlement cycles reduced the window for effective intervention. While most participants believed real-time transaction monitoring remained some distance away, there was widespread agreement that AI, process redesign, and enhanced data capabilities would fundamentally reshape financial crime operating models over the next three to five years. The debate concluded that the most successful organisations would be those capable of balancing technological innovation, governance, workforce transformation, and risk management within a coherent operating model framework.



Quality, governance and architecture as pre-requisite for effective data management

The debate examined the extent to which data quality, governance, and architecture were enabling or constraining the effectiveness of financial crime controls. Participants agreed that whilst artificial intelligence (AI) and advanced analytics were creating new opportunities across financial crime functions, the underlying quality, structure, and ownership of data remained fundamental determinants of success. Much of the discussion focused on the challenges created by poor-quality data, fragmented systems, and legacy infrastructure, alongside the need to move towards more proactive, intelligence-led approaches to risk management. As one participant noted, "my role is to make sure that I screen in the best way and the most effectively", showcasing the move towards a more risk management approach to data, and a more effective financial crime function.

A recurring theme throughout the discussion was the importance of data quality as the foundation for effective financial crime controls. Participants acknowledged that poor-quality data continued to undermine sanctions screening, TM, customer due diligence (CDD), and onboarding processes. Several contributors argued that organisations often focused on new technologies without first addressing the data issues that limited their effectiveness. One participant observed that firms would never achieve meaningful reductions in false positives because "you have to have that foundation" before technology could deliver sustainable improvements. Another described how large institutions had accumulated years of temporary

fixes and workarounds, resulting in what was characterised as "millions of sticking plasters" being applied to longstanding data quality problems.

The relationship between data quality and operational performance was discussed in practical terms. Participants highlighted how incomplete, inaccurate, or poorly structured data directly contributed to excessive alert volumes and reduced confidence in screening and monitoring outcomes. Several firms reported active programmes focused on improving data models, enhancing data capture processes, and reviewing the logic supporting existing controls. The consensus was that effective data management was not simply a technical exercise but a prerequisite for improving risk detection and reducing inefficiencies across financial crime operations.

Participants also explored the impact of fragmented systems and legacy infrastructure on financial crime effectiveness. Many organisations described operating environments where data remained dispersed across multiple systems, creating barriers to efficient investigations and limiting the ability to build comprehensive customer and transaction risk views. Historical technology estates, often developed over many years through acquisitions, regulatory change, and operational growth, had resulted in significant data silos and duplicative processes.

The discussion suggested that a more integrated data architecture would allow firms to connect information more effectively across onboarding, screening, monitoring, fraud prevention, and investigations. Several participants explained that they were undertaking substantial transformation programmes designed to improve data accessibility and integration. One contributor explained that transaction monitoring challenges were driven in part by "not the right quality of data" and limited capability to monitor information in a suitable

way. This reinforced the view that enhancing data architecture was essential to improving both operational efficiency and risk outcomes.

Another prominent theme concerned the increasing use of data to generate deeper risk insights and support more proactive decision-making. Participants described a growing shift away from viewing alerts or transactions in isolation and towards analysing broader patterns of customer behaviour and interconnected risk indicators. The traditional focus on individual transaction events was viewed by many as increasingly inadequate for modern financial crime detection.

Several speakers outlined how richer datasets and AI-enabled models could be used to identify customer risk, emerging typologies, and suspicious patterns more effectively. Examples included plausibility models used in onboarding, enhanced transaction monitoring models, and approaches that combined sanctions, fraud, and money laundering indicators into a more holistic view of risk. One participant argued that organisations needed to move beyond historical approaches and create models capable of "telling a story", by bringing together multiple risk factors. This reflected a broader ambition to shift from reactive reporting models towards intelligence-led decision-making and earlier intervention.

The debate also highlighted a growing movement towards real-time and event-driven data management approaches. Participants discussed the limitations of fixed review schedules and explored how ongoing monitoring could provide a more accurate representation of customer risk. There was considerable interest in moving away from traditional one-, three-, and five-year Know Your Customer (KYC) review cycles and towards trigger-based models supported by continuous data assessment.



Some organisations reported significant progress towards this objective. One contributor explained that their organisation had already implemented trigger-based reviews for most of its customer base and expected to extend this approach further. However, participants also noted practical challenges, particularly where information still needed to be obtained directly from customers and was not available through public data sources. Despite these limitations, the overall direction of travel was clear, with many participants viewing perpetual KYC and event-driven monitoring as more effective and efficient approaches to managing financial crime risk.

Governance, ownership, and accountability featured heavily in discussions about future data strategies. Participants emphasised that better data outcomes required clear responsibility for data quality, model performance, and control effectiveness. There was broad agreement that business and process owners should retain accountability for outcomes rather than relying solely on technology teams. Several organisations described governance structures that combined central oversight with decentralised implementation, allowing innovation to progress whilst maintaining appropriate standards and controls.

The importance of model validation, auditability, and evidence-based decision-making was also repeatedly reinforced. Participants discussed the need to demonstrate that AI-driven approaches could outperform existing manual processes through rigorous testing and back-testing.

One participant highlighted that organisations needed to prove that AI decisions were reliable and transparent, noting that "the power of this is the science" because improvements could be demonstrated using historical data and measurable outcomes. Others argued that clear audit trails and explainable decision-making would be critical in gaining regulatory confidence and enabling wider adoption of advanced technologies.

Overall, the debate concluded that improving financial crime effectiveness would require firms to treat data as a strategic asset rather than a supporting function. Whilst AI, automation, and advanced analytics offered significant opportunities, participants consistently emphasised that sustainable improvements depended on high-quality data, integrated architectures, strong governance, and a greater ability to transform information into actionable risk intelligence.

In conclusion, the debates highlighted that the future effectiveness of financial crime functions will depend on four interconnected priorities: reducing false positives, improving data quality, modernising legacy processes, and deploying AI within robust governance frameworks. Participants broadly agreed that organisations that successfully integrate high-quality data, intelligent automation, simplified operating models, and skilled workforces will be best positioned to improve detection outcomes, meet growing regulatory expectations, and deliver a more efficient financial crime function over the next three to five years.

This information was taken from
The Financial Crime Leaders' Network
event in London, 25 June 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