



A 1LoD report



Financial Crime

LEADERS' NETWORK

FORECAST 2026

One Financial Crime Risk with Many Channels

Key Takeaways

01

Firms have entered the crypto and digital asset space cautiously, using phased, partner-led models to manage regulatory uncertainty rather than launching full-scale propositions

02

Anticipated regulatory shifts, including a more permissive US posture, act as a catalyst for experimentation but not a relaxation of anti-money laundering (AML) standards

03

Governance models evolve by extending existing AML, sanctions, and fraud frameworks to digital assets, rather than creating entirely new paradigms.

04

The most significant structural risk remains the identity gap between on-chain activity and real-world actors, particularly in decentralised finance (DeFi) and off-platform environments

05

Operational effectiveness depends less on acquiring blockchain analytics tools and more on integrating, enriching, and operationalising data for investigators.

06

Risk ownership and accountability across the 1st and 2nd lines remain a point of tension as digital asset activity expands

07

Crypto-native firms demonstrate materially greater speed in deploying models and controls, but that agility requires compensating governance, QA, and explainability

08

Regulatory fragmentation and uneven supervisory capacity continue to enable arbitrage and constrain the scalability of global financial crime programmes.



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

One Financial Crime Risk with Many Channels

The Financial Crime Leaders' Network brought together senior leaders in financial crime in New York on 09 October. Firstly, participants focused on the extent to which financial institutions had begun to de-silo financial crime functions and the practical realities of delivering a more holistic approach to financial crime risk management. While there was broad agreement that integration across anti-money laundering (AML), know your customer (KYC), fraud and sanctions was both desirable and inevitable, participants consistently emphasised that progress had been incremental, uneven and far more advanced at the data layer than at the organisational level. Many firms had moved towards integrated investigative teams across AML and sanctions, often supported by shared case management tools, but fraud typically remained anchored in the 1st line with its own investment priorities and technology stack. As one participant observed, "you can work cases together regardless of the organisational structure, but if the data doesn't flow, you're still operating in silos."



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

Examining the Limits of De-Siloing Financial Crime Functions

A recurring theme was that de-siloing was less about collapsing reporting lines and more about enabling a common view of risk through shared data and analytics. Several participants described efforts to build single data domains or global data lakes to bring together transaction, customer and behavioural data across business lines. However, this was widely characterised as a multi-stage journey, beginning with basic data harmonisation, followed by the development of cross-functional investigative processes, and only later by the removal of redundant systems and duplicated monitoring. Participants stressed that without getting the foundational data layer right, firms would “never get to the point where you can actually turn systems off or stop investigating the same transaction three times in three different teams,” as one participant explained.

Data integration challenges dominated the discussion. Banks reported persistent fragmentation between KYC repositories, transaction monitoring (TM) platforms, fraud systems and sanctions screening tools, often built for different purposes, at different times and under different regulatory pressures. Investigators frequently lacked access to core KYC information, while contextual intelligence generated by financial intelligence units (FIUs) was not systematically fed back into onboarding or ongoing due diligence processes. One participant noted that “the infrastructure itself has become

“the infrastructure itself has become an active impediment – everyone agrees we should work end to end, but the databases simply don’t talk to each other.”

an active impediment – everyone agrees we should work end to end, but the databases simply don't talk to each other." These issues were compounded by legacy architectures, jurisdictional variation, and the sheer cost of re-engineering data at scale.

Funding and prioritisation emerged as critical constraints and participants were candid that, in many institutions, large-scale integration only became feasible when driven by regulatory enforcement. Several cited consent orders as the trigger that unlocked investment in enterprise data platforms and enabled consistent data feeds across 1st and 2nd line functions. Without such pressure, integration initiatives were frequently deprioritised in favour of mandatory remediation work. As one participant put it, "unless there's regulatory pressure, moving data around just doesn't make it into the top three priorities." Even firms that had recently exited consent orders described how non-mandatory integration work quickly slipped down IT delivery lists once formal regulatory deadlines were removed.

The role of financial crime compliance leadership was a central point of debate. Participants generally agreed that compliance leaders were expected to champion integration, articulate the long-term risk management case and challenge siloed thinking. However, there was also recognition that compliance had, in some cases, taken on too much responsibility for decisions that should have sat with the business. Several participants warned that when technology and financial crime teams defined authoritative data sources and system hierarchies without sustained business ownership, accountability became blurred. "We're happy to drive the decision," one participant remarked, "but the risk ultimately sits with the business, and they're often too far removed from what's being built."

This led into a broader discussion on governance and ownership. Participants highlighted

widespread discomfort around data ownership, with the 1st line often reluctant to accept accountability for customer data beyond what was strictly required to transact. Some attributed this to incentives, with one participant noting that "they don't make money off data quality, so it never becomes a priority," while others framed it as a cultural issue shaped by past enforcement patterns. There was consensus that future governance models would need to place clearer accountability on the 1st line for data quality and outcomes, with compliance setting standards, oversight and challenge rather than acting as de facto data owner.

Governance risks were seen as intensifying as firms adopted more advanced technologies, particularly AI and machine learning (ML). While participants were cautious about vendor claims and stressed that much of what was currently deployed was rules-based automation rather than true AI, they acknowledged that new tools were increasing the distance between customer-facing teams and underlying decision-making logic. Several warned that without clear governance over data lineage, decision rights and change control, firms risked future client friction and regulatory scrutiny. "The minute a customer experiences friction," one participant noted, "the business will say, 'you built this system, you didn't consult us.'"

Overall, the debate painted a picture of an industry aligned on the direction of travel but constrained by legacy, incentives and governance complexity. De-siloing was progressing, but primarily through data-sharing initiatives rather than wholesale structural change. Participants agreed that achieving a genuinely holistic financial crime risk framework would require sustained leadership, clearer ownership models and governance structures capable of supporting shared platforms over the long term, rather than relying on regulatory pressure alone to force integration.

Balancing Speed, Innovation and Accountability as Digital Assets enter Regulated Financial Institutions

The second debate explored how financial institutions and crypto-native firms had been preparing for a shifting regulatory landscape and what that had meant for crypto-related AML governance. The moderator set the tone by noting that many banks had been considering crypto offerings, stablecoins, or integrations with exchanges, and then linked the conversation to regulatory momentum by describing a “wind of deregulation from Washington”. Participants generally treated the regulatory direction as an accelerant rather than a free pass: it encouraged entry, but it did not remove the need for robust AML controls, careful programme ownership, and defensible governance.

Several firms described adopting deliberately constrained business models as a form of regulatory and operational risk management. Rather than launching broad wallet functionality, some banks had partnered with exchanges so that customers routed orders externally while funding accounts through existing brokerage relationships. This structure had allowed firms to retain strong knowledge of fiat finance and customer KYC while limiting exposure to the full breadth of crypto transaction types. One participant stressed that the offering had been “purposely somewhat tailored” because the organisation had not been “fully prepared to offer the breadth of what you could do in a typical crypto wallet.” The gradual approach had also reflected concerns about supervisory perception: even if a bank was “not technically delivering crypto services”, as one participant put it, it still needed to consider how regulators interpreted the risk posture and the brand association with crypto markets.

The discussion then turned to how governance models had evolved traditional AML and fraud frameworks to address blockchain-based risks and DeFi-adjacent activity. One participant argued that they had built a compliance programme that “looked and felt like what you have at banks”, combining transaction monitoring, sanctions controls and KYC, albeit delivered differently for competitive and operational reasons. They explained that crypto controls still needed to be auditable and defensible, stating that “everything is auditable, everything’s explainable, and everything’s subject to oversight.” Yet they also acknowledged that the industry’s risk appetite was culturally different and that some firms could operate “a bit more wrong sometimes” because they could pivot quickly.

That ability to move quickly was presented as a defining contrast with traditional banking governance. The exchange representative said banks could take “14–15 months” to roll out a new model, while their organisation could do it “in weeks”. However, speed had not been



portrayed as inherently safe; the exchange described having to persuade the business that rapid delivery still required governance and controls embedded into the development process. Quality assurance and quality control functions had been strengthened to test both what machine learning surfaced and what it suppressed, including reviews of activity placed into "continuous monitoring" or holding patterns to assess potential misses. This approach had been framed as a way to scale innovation without losing control integrity.

On risk ownership and expertise, participants repeatedly implied that digital asset capability had been spreading across both 1st and 2nd lines, but the practical challenge had been timing, resourcing, and clarity of accountability. Asset managers and banks described outsourced or partner-led operating models (custody arrangements, onboarding through third parties, offshore structures) that reduced operational burden but increased the need for strong oversight. Some practitioners had felt structurally disadvantaged when product teams moved too quickly: they were sometimes brought in "too close to the launch of a product to really make an impact," and they were "fighting for some resources." The underlying message was that governance models had needed to hardwire

The underlying message was that governance models had needed to hardwire digital asset expertise early into product approval and change governance, rather than treating compliance as an end-stage checkpoint.



digital asset expertise early into product approval and change governance, rather than treating compliance as an end-stage checkpoint.

When the debate addressed detection and investigation challenges, the group converged on a consistent operational reality: the blockchain provided excellent transactional visibility, but attribution remained difficult without identity data and information-sharing. Participants described the duality of "good data" on-chain that was immutable and traceable, versus limited certainty about "who the hell they are" behind certain transactions, especially when activity moved off-platform into DeFi-style environments that were "scary stuff." Firms described using a common set of blockchain analytics vendors alongside homegrown attribution capabilities to link addresses to individuals or entities. The exchange perspective was that maturing attribution had enabled stronger law enforcement referrals—cases were described as effectively "bow-tied", combining on-chain flows with whatever KYC could be assembled.

Yet the discussion highlighted a major ecosystem weakness: competitive dynamics had inhibited cross-exchange cooperation, meaning there was no consistently effective analogue to established

information-sharing norms in banking. Requests for information were "not typically well received" unless a crisis such as a major hack forced collective action. This lack of sharing, combined with fragmented regulation across jurisdictions, was seen as a key reason why illicit actors could exploit gaps and pursue the "path of least resistance."

Finally, participants emphasised that the biggest operational challenge was not simply acquiring blockchain data but making it usable at scale. Several speakers suggested differentiation came from "what you do with that" information—analytics, contextual enrichment, and investigator workflow design. The work was described as "not exactly rocket science, it's just very tedious," largely because building and maintaining the necessary APIs and integrations was complex. Without strong user experience, even rich datasets could produce slow investigations, creating a programme that had data "but you can't actually drive" effectively.

This information was taken from The Financial Crime Leaders' Network event in New York, 9 October 2025.

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