A 1LoD report

Financial Crime

LEADERS' NETWORK

SINGAPORE

FORECAST 2026

Managing Financial Crime Risk Across Divergent Regulation and Emerging Asset Classes

Sponsor

fenergo

Future-Proofing Client Lifecycle Management

Key Takeaways

01

Financial crime frameworks are increasingly built around a global "gold standard", with jurisdiction-specific adaptation reflecting sustained regulatory divergence

02

Data fragmentation and unclear ownership continue to constrain both artificial intelligence (AI) adoption and the effectiveness of financial crime controls

03

AI is deployed selectively across defined use cases, with explainability, governance and human oversight prioritised over speed and scale

04

Sanctions and cross-border financial crime decision-making are increasingly shaped by conflicting regulatory obligations rather than internal policy alone

05

Digital assets expose structural gaps in existing anti-money laundering (AML) and know-your-customer (KYC) frameworks, particularly around proportionality and responsibility boundaries

06

Effective management of emerging financial crime risks depend on sustained collaboration between banks, payment service providers (PSPs) and regulators

Reshaping financial crime risk management under regulatory fragmentation

The **Singapore Financial Crime Leaders' Network** started of discussing that financial crime risk management frameworks continued to be reshaped by regulatory divergence, geopolitical volatility and the limits of data-driven oversight. Rather than pursuing large-scale transformation, institutions adapted incrementally, constrained by jurisdictional complexity, evolving threat patterns and internal capacity. The emphasis shifted decisively from architectural redesign to pragmatic execution.

Regulatory expectations across key markets were increasingly fragmented, particularly in sanctions enforcement and threat interpretation. Identical activity prompted materially different supervisory responses depending on jurisdiction, eroding the effectiveness of static global rules. As one participant noted, "the static rules are no longer valid." In response, institutions moved away from uniform execution models towards frameworks combining global minimum standards with locally calibrated controls.

This shift materially changed how governance operated in practice. While global frameworks continued to define risk appetite and baseline policy, local execution ultimately determined whether controls were defensible. Conflicts between regulatory regimes moved from exception to norm. The need to document, justify and formally accept outcomes that diverged from global policy became a recurring requirement, particularly where licensing or regulatory access was at risk.

AI and advanced analytics remained important enablers, but adoption was disciplined and controlled. Deployment accelerated in targeted areas such as alert triage, narrative generation and comparative analysis, but its impact remained bounded by governance, explainability and data maturity constraints. Investigative judgement remained central. As one participant observed, "you have to have a human into the loop." Nowhere was this more evident than in sanctions decision-making, where contextual judgement and regulatory nuance continued to drive outcomes. Accountability remained firmly with individuals, not systems.

Return-on-investment pressure reinforced this caution. Boards increasingly demanded tangible, defensible value from AI investments. Short-term gains were consistently deprioritised in favour of longer-term capability building. As one participant noted, "there is not a use case which will give you a return on investment of 6 to 12 months." As a result, AI programmes were justified primarily on resilience, defensibility and control enhancement, rather than cost reduction.

Data, participants agreed, remained the most persistent structural constraint. Fragmented systems, inconsistent identifiers and unclear ownership continued to undermine even the most sophisticated analytical models. Financial crime functions increasingly absorbed responsibilities traditionally owned by technology or operations teams, as poor data quality directly impacted regulatory defensibility. Without reliable inputs, advanced analytics did not translate into meaningful insight.

Operating model discussions reflected similar pragmatism. The structural positioning of financial crime across the 1st and 2nd lines of defence was seen as secondary to clarity of accountability, escalation authority and effective challenge. Outcomes depended less on organisational design and more on whether functions could act, challenge and escalate without friction.

Overall, the discussion concluded that next-generation financial crime risk management was defined less by automation and more by disciplined, data-anchored governance. Regulatory scrutiny on explainability and accountability was expected to intensify, reinforcing the need for operating models that absorb ongoing divergence rather than assume convergence.

"This was a small and cosy Leaders' Network that allowed for constructive conversation/ discussion vs other events which are much more 'one-way'."

CHEE FONG LOH, MIZUHO

"As a first timer of the Leaders' Network, I found the event interactive and interesting."

DISHA NUNKOO, HEAD OF COMPLIANCE, SOUTHEAST ASIA, SCHRODERS

Integrating digital assets into financial crime compliance frameworks

The second discussion focused on digital assets, and that they continued to challenge assumptions underpinning traditional financial crime compliance frameworks. Blockchain based products it was agreed exposed structural gaps in AML and KYC models, particularly around transaction monitoring (TM), counterparty transparency, and the limits of institutional responsibility for on chain activity beyond a direct customer relationship.

A consistent view emerged that digital assets could not be treated as a single, coherent risk typology. Risk varied materially by product and service, whether institutional custody, stablecoin payments, tokenised instruments, or decentralised protocols. As one participant put it, "it's not a one size fits all model." Broad asset class classifications were therefore seen as increasingly ineffective, pushing institutions towards more granular, product and business line specific risk assessments.

Speed and transparency were identified as defining characteristics of on chain activity, creating both opportunity and unresolved challenge. Blockchain analytics enabled transaction flows to be traced with unprecedented visibility, yet questions persisted around how far institutions should be expected to pursue that information. The ability to identify multiple transaction

"hops" blurred traditional boundaries of responsibility, particularly where no customer relationship existed. Importantly, it was emphasised that data accessibility alone did not justify expanded institutional liability.

These challenges all the participants agreed, were amplified by uneven regulatory maturity across jurisdictions. Divergent approaches to travel rule implementation, treatment of hosted and unhosted wallets, and oversight of virtual asset service providers (VASPs) continued to complicate compliance design. As a result, institutions were increasingly reliant on third party controls and counterparty due diligence, heightening interdependence across the ecosystem. As one participant observed, "PSPs need banks and banks need PSPs."

Traditional customer due diligence models were widely viewed as insufficient in this context. Static KYC records captured ownership and profile at a point in time, but failed to reflect behavioural change, transaction velocity, or ecosystem exposure. There was growing interest in continuous monitoring models integrating behavioural indicators, external intelligence, and trigger based review. While conceptually compelling, these approaches introduced material complexity and cost, with many firms still working through integration challenges.

Tokenisation of real world assets generated cautious interest but little near term consensus. Potential benefits such as fractional ownership and improved liquidity were acknowledged, yet unresolved challenges around valuation, custody, cyber risk, and enforceability limited broader adoption. Most initiatives remained confined to controlled pilots rather than scalable production environments.

Regulatory engagement was viewed as necessary rather than constraining. Supervisors were generally seen as open to dialogue and learning where institutions engaged early and transparently. However, the absence of prescriptive benchmarks left firms navigating uncertainty, balancing innovation against established supervisory expectations around control design and evidencing.

Technology maturity remained uneven. While experimentation with vendor provided transaction monitoring models was underway, significant calibration was often required before practical use. Hybrid environments combining rules based and model driven controls were therefore expected to persist. As one participant remarked, "rules will continue to exist in their current form for the next two to three years."

Overall, the participants agreed that integrating digital assets into financial crime compliance frameworks was proving less a question of technology and more one of clearly defined risk boundaries. Progress depended on articulated risk appetite, defined limits of responsibility, and sustained collaboration across financial institutions, payment providers, and regulators. Until legal clarity, cyber resilience, and traceability matured further, institutions appeared committed to cautious exposure management rather than proactive expansion.

"Most informative and engaging. A good mix of people."

PRAVEEN JAIN, MANAGING DIRECTOR, MODEL RISK, FINANCIAL CRIME, BANK OF AMERICA

This information was taken from The Financial Crime Leaders' Network event in Singapore, 26 March 2026.

Upcoming Financial Crime events

1LoD

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