A 1LoD report

Financial Crime
LEADERS' NETWORK

FORECAST 2025

When Guidance isn't enough -
Navigating the Financial Action Task Force, Fragmented Rules and the Crypto Gap

Sponsored by

AML RIGHTSOURCE
REIMAGINING COMPLIANCE

DOW JONES
RISK & COMPLIANCE

NAPIER AI

Key Takeaways

01

Real-time trigger alerts make sense in theory but are tricky in practice because of the need to balance speed with control.

02

Real-time monitoring does not imply universal application. Risk-based stratification is crucial.

03

Event-driven reviews (EDR) offer a promising evolution in compliance, contingent on the effective categorisation and design of triggers.

04

Automation is a force multiplier but should not replace human judgment, especially in nuanced client contexts.

05

Regulatory frameworks – especially Financial Action Taskforce (FATF) guidance – influence practice, but do not trump domestic regulators.

06

There are significant limitations to the control of digital assets, in particular, the monitoring of decentralised platforms and unhosted wallets.

07

Know your customer (KYC) expertise is siloed in many institutions and fails to deliver real-time value for sanctions and geopolitical risk exposure.

08

Legacy infrastructure and restrictive governance get in the way of systemic transformation, hence incremental innovation is the norm.

When Guidance isn't enough - Navigating the Financial Action Task Force, Fragmented Rules and the Crypto Gap

New cryptocurrency laws, the balance of regulatory compliance and pro-active risk management, and a move to real-time trigger alerts (T+0) topped the list of critical issues in risk management that **The Financial Crime Leaders' Network** discussed when it convened in New York on June 3rd.

T+0 Trigger Alerts: Nice to Have, Difficult in Practice

T+0 trigger alerts are a feature allowing automated actions to be taken immediately once a specific condition is met in a monitoring system. This is the future when it comes to dynamic financial crime risk management, yet participants are wary of it. There is a clear disconnect between commercial enthusiasm for real-time decisions and the compliance community's concern over whether instantaneous results can be delivered without compromising effective control.

Participants stressed that real-time monitoring cannot be universal and a risk-based framework is essential. For some institutions, basic due diligence can take place post-trade (especially for low-risk products), whereas in the case of higher-risk transactions, comprehensive onboarding and enhanced due diligence (EDD) must be done before any trading starts. This stratified model reflects the industry's recognition that regulatory compliance is not monolithic, and operational constraints must be balanced against escalating expectations for speed.

"Spikes in volume from triggers can overwhelm even well-staffed teams," one participant emphasises, underscoring the limits of flexibility. Moreover, banks lack agility because they cannot simply add or cut headcount at the drop of a hat.

Participants also questioned the timeliness and political neutrality of FATF's processes. The lag between country evaluations and published outcomes means that risk management is also subject to delays.

Event-Driven Reviews as a Pathway to Proactive Risk Management

The shift to EDR offers banks a more timely and focused response to changes in the risk profile of their clients. However, the success of this approach hinges on whether the trigger design, categorisation, and response thresholds are effective. Several institutions described categorising triggers as either 'administrative' (e.g. a contact detail changes) or 'material' (e.g. adverse media or jurisdictional shifts), which allows them to differentiate between various levels of review.

Automation is a potential force multiplier. Firms are using pilot studies or trying out specific technology which can detect adverse information and trigger reviews without requiring manual intervention. But participants cautioned against over-reliance on these tools in their current state. As one contributor put it, "automation can support, but not replace, risk-based decisioning," particularly in those instances where client relationships or contextual nuance matter. The balance between automation, technology and resources is a constant challenge for banks, faced with limited headcount and the need to work smarter, not harder.

In practice, most banks use a combination of solutions, but still rely on periodic reviews, either out of habit or because it is a regulatory requirement. Several participants said their long-term goal is to get away from periodicity. Perpetual KYC (pKYC), where real-time triggers replace scheduled recertifications, is considered promising, but conditional on having demonstrable coverage of material risk through the detection of events.

FATF Guidance: Influential but Not Determinative

In a discussion about the role of FATF as a standard-setting body, participants agreed that it can shape global norms and influence country risk ratings, but recognised that the real power lies with national regulators, not the FATF. "You can't say 'but FATF said' to the OCC [Office of the Comptroller of the Currency]," said one participant: In practice, domestic requirements override global guidance.

Participants also questioned the timeliness and political neutrality of FATF's processes. The lag between country evaluations and published outcomes means that risk management is also subject to delays, while the subjectivity of the grey-listings makes them less valuable as indicators of risk.

Despite these shortcomings, several banks incorporate FATF outcomes into their broader jurisdictional scoring models – often as one of multiple factors. Overrides are permitted based on local intelligence or internal market presence, again reflecting the necessary use of discretion in global banking risk frameworks.

Digital Assets and the Risk-Management Paradox

The subject of digital assets sparked the most animated debate, reflecting the banks' growing discomfort with the regulatory vacuum surrounding crypto and digital assets, particularly the challenge of applying traditional KYC and transaction monitoring (TM) expectations to a system that is designed to avoid them.

A clear distinction was drawn between custody-backed stablecoins, which offer visibility and regulatory engagement, and unhosted wallets or decentralised platforms, which allow users full control of their cryptocurrency without a third-party service provider and thus operate outside the reach of institutions. Banks which are based and operate in Asia (e.g. in Singapore or Hong Kong) appear to be more advanced in engaging with regulated digital asset service providers, while institutions which are regulated in the US remain more cautious, citing regulatory and political uncertainty and toolset limitations.

Participants are worried that current monitoring tools are not fit for purpose. "Vendors can translate blockchain data into readable form, but they cannot conduct meaningful monitoring in a regulatory sense," explained one practitioner. This gap highlights an industry-wide vulnerability: The illusion of control in a space where real surveillance remains elusive.

The industry also lacks a coherent taxonomy for assessing FinTechs. Banks often group disparate entities – lending platforms, exchanges, infrastructure providers – under a single, high-risk umbrella, which can lead to inconsistent and sometimes counterproductive risk decisions. So, institutions need a more granular classification framework. Banks are talking to each other about the critical challenges of offering crypto products to clients. However, they operate within a fragmented regulatory framework and are ill-equipped to police crypto entities. The inherent question also arises: should banks be playing the police when it comes to crypto and digital assets?

Incrementalism over Transformation

The main tension lies between strategic intent and operational reality. Event-driven KYC is seen as a step in the evolution of compliance and a business enabler. Yet few institutions have achieved meaningful end-state transformation. Instead, progress is incremental, fragmented, and dependent on the context.

While automation, risk-based design, and perpetual KYC are all advancing, participants acknowledged that most firms are tied to legacy systems, manual reviews, and regulatory mandates that prevent them from being more agile in their implementation. Digital assets challenge the traditional paradigms, pushing banks to define what they can control – and where they must simply mitigate.

Ultimately, the discussion reinforced a central truth: Event-driven reviews are not only about triggers but also about control architecture, governance, and the confidence to shift away from legacy models without compromising integrity or assurance. Until those foundations are secured, the vision of fully dynamic, risk-responsive KYC remains out of reach.

Frameworks Under Pressure

In an increasingly fractured global order, the role of financial institutions in navigating sanctions and geopolitical risk has become more precarious and complex, exposing both the resilience and limitations of current compliance practices and revealing an industry in transition – an industry which is reactive in some areas and cautiously proactive in others.

Despite mounting geopolitical tensions, most firms have resisted full-scale revisions of their financial crime compliance frameworks. Instead, they have made tactical enhancements, adding controls such as extra due diligence checks, attestation layers, and onboarding adjustments.

This conservative approach reflects both heightened regulatory scrutiny and a belief that existing frameworks are largely fit-for-purpose. Yet such confidence may prove misplaced. "We're not reviewing the total framework, just enhancing parts of it," one practitioner said, hinting at a risk-averse mindset. In the face of increasingly agile adversaries and evolving regulatory demands, incrementalism may be insufficient.

While enhancements can deliver marginal gains, they also risk masking structural weaknesses, particularly where outdated systems or fragmented governance models persist.

Regulatory Volatility and the Illusion of Control

Participants noted the tension between regulatory complexity and operational readiness. Jurisdictional divergence, particularly between the US, UK, and EU regarding sanctions, has become a significant point of friction, raising questions about how institutions reconcile conflicting obligations.

Weekly compliance calls are effective tools for internal alignment, yet several participants said that translation of guidance into enforceable procedure is still a weak link. "We issue guidance, but the policy change might take a year, if it happens at all," one said. The inability to move at the speed of regulation raises concerns not just about regulatory breach, but also about audit readiness and reputational risk.

There was a striking admission of retrospective rationalisation: Firms often scramble to prove control effectiveness only after an issue emerges. This reactive posture risks leaving institutions flat-footed in the event of enforcement or reputational risk exposure.

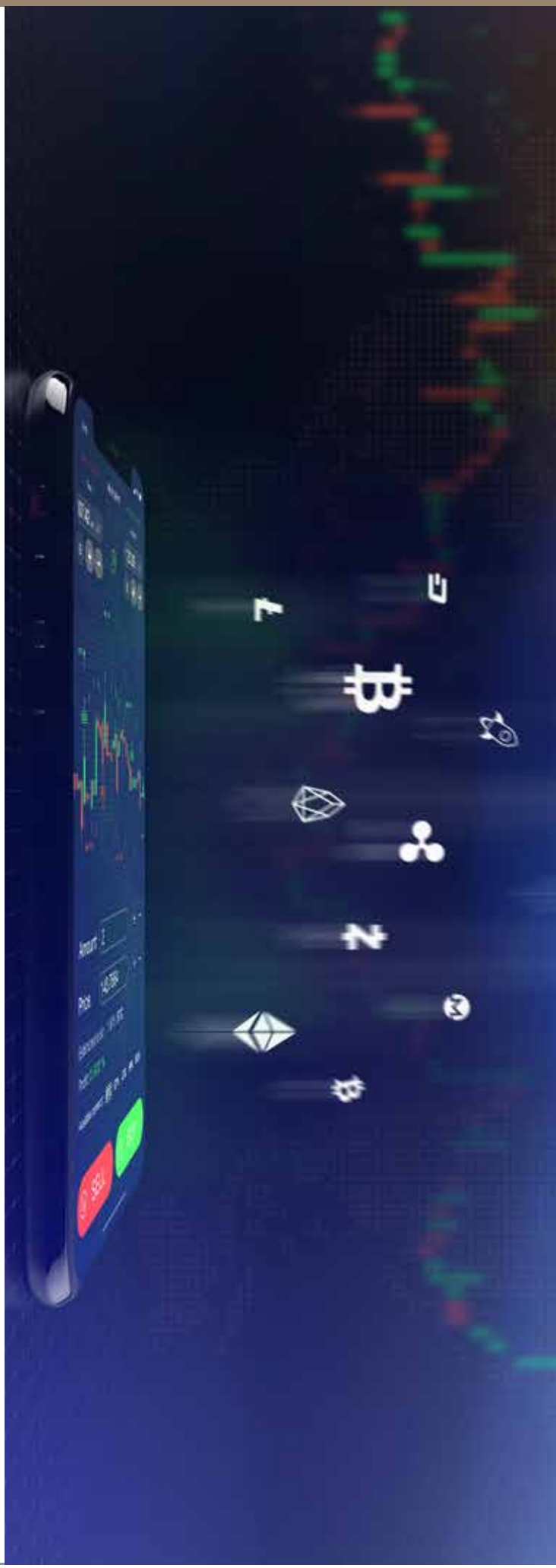
KYC: Still a Liability or an Untapped Strategic Asset?

Client risk profiles need to be clear if they are to be of any use in sanctions risk management. While most firms acknowledge the value of detailed KYC data, especially regarding Ultimate Beneficial Owners (UBOs) and geopolitical exposure, few have fully integrated this intelligence into live transaction monitoring or decision-making systems.

One participant described how their firm collected China nexus data "two years before it became important", showing what's possible when compliance teams think ahead. But this was the exception rather than the norm. Three years on from Russia's invasion of Ukraine, banks have managed in increasingly complex sanctions environments with no signs of sanctions enforcement slowing.

In many cases, KYC operates in a silo within the institution, treated as a static onboarding hurdle rather than a dynamic tool for determining risk. Without clear mechanisms to link client data to transactional behaviour, firms risk missing indicators of sanctions evasion or reputational exposure.

Perhaps the most alarming finding was the lack of readiness regarding crypto-related sanctions evasion. A handful of participants have begun using blockchain analytics tools, but most described their efforts as basic or experimental.



The Operational Bottleneck: Automation Without Oversimplification

Operational efficiency is especially important in that it can free up skilled investigators to focus on complex risk reviews; with artificial intelligence (AI) and automation being viewed with cautious optimism. Tools that help triage alerts or summarise large datasets are seen as alleviating investigative pressure, but participants warned against a false sense of progress.

Automation is not a panacea. Several participants noted that many so-called efficiency tools failed to support nuanced decision-making or contextual understanding, which is essential when dealing with Politically Exposed Persons (PEPs) or multi-layered corporate structures. The risk is that by going for efficiency, institutions might inadvertently dilute judgement-based controls or overlook soft signals of risk.

Firms that can digitise their control environments by linking KYC, TM, and sanctions data demonstrate a clear advantage. These institutions are better placed to identify contradictions, spot escalation triggers, and adjust exposure assessments in real time.

The Crypto Gap: Acknowledged but Undercooked

Perhaps the most alarming finding was the lack of readiness regarding crypto-related sanctions evasion. A handful of participants have begun using blockchain analytics tools, but most described their efforts as basic or experimental. This is surprising, given the clear use of cryptocurrency channels by those individuals who want to circumvent formal financial systems. Several participants acknowledged they had no dedicated resource or to trace such activity. "We're only running a high-risk exchange list through TM – it's not embedded yet," one participant said.

The implication is clear: the financial system's capacity to detect crypto-enabled evasion is still immature. Without more structured investment in blockchain forensics, firms remain exposed – not only to regulatory action, but to reputational fallout if they unwittingly facilitate illicit flows.

Proactivity or Complacency?

The Financial Crime Leaders' Network asked a fundamental question – are institutions prepared to shift from defensive compliance to strategic risk intelligence? Current approaches show signs of sophistication – enhanced onboarding controls, cross-functional response teams, and nascent AI adoption – but these are patchy and often reactive.

In an era where sanctions can be imposed overnight and circumvented within hours, compliance frameworks built for slower cycles are reaching their limit. To move beyond compliance-by-box-ticking, banks must treat geopolitical risk as a live, interconnected threat, not a compliance sub-function. This will require better tools, stronger data integration, and a cultural shift from documenting compliance after the fact to proving readiness in real time.

This information was taken from The Financial Crime Leaders' Network event in New York, 3rd June 2025.

Upcoming Financial Crime events

1LoD®

2025

Responding to threats, redefining risk, rebuilding frameworks

IN-PERSON CONFERENCE

A 1LoD event

The Financial Crime Summit

LONDON

11 | Sep | 2025

VIRTUAL EVENTS

01&02 July	Onboarding & KYC Deep Dive
21&22 Oct	AML Deep Dive
02&03 Dec	Fraud Risk Deep Dive

www.1lod.com