



## The Rising Bar of Suspicious Activity Reporting

- Jonathan Greenstein



# The Rising Bar of Suspicious Activity Reporting

April, 2026

Suspicious activity reporting has long sat at the core of the UK's anti-money laundering framework. What is changing is not its role, but the expectations around it. Regulators are no longer satisfied with volume or process alone. They want reporting that is timely, well-reasoned and capable of generating real intelligence value.

Supervisory focus is shifting towards how suspicion is identified, assessed and articulated. The emphasis is on clear rationale, effective upstream controls and a coherent understanding of customer behaviour and risk. Filing is no longer viewed in isolation, but as the output of a system that must withstand scrutiny.

These expectations are operational, not theoretical. They require firms to process, connect and interpret large volumes of data in near real time, placing technology at the centre of effective compliance.

From obligation to intelligence function

At a legal level, the trigger for filing a SAR remains unchanged. Under the Proceeds of Crime Act, firms must report where they know, suspect, or have reasonable grounds to suspect money laundering or financial crime.

What has changed is how effectiveness is judged.

The Financial Conduct Authority has made clear that the value of a SAR lies in its quality and usefulness, not its volume. Firms are expected to provide clear, structured narratives that support law enforcement and the National Crime Agency in understanding the underlying risk.

In parallel, UK guidance has warned against defensive reporting, where firms submit large volumes of low-quality SARs to mitigate regulatory exposure rather than highlight genuine suspicion.

The implication is straightforward. Firms must not only detect suspicious activity but articulate it with enough clarity and context to be useful. That depends on how effectively they surface signals, connect them and present them.

Timeliness becomes capability

Timeliness is no longer a best-efforts principle. It is a capability test.

Under the UK regime, SARs must be submitted promptly once suspicion is formed. Delays, particularly where they stem from weak internal processes or fragmented systems, are increasingly viewed as control failures rather than operational constraints.

This reflects a broader shift. SARs are expected to support timely intervention, not retrospective documentation.

For firms reliant on manual processes, this creates a structural constraint. Timeliness at this level is not about effort. It is about how quickly a firm can move from signal to insight, and from insight to a defensible decision.

The end of the siloed AML model

Regulators no longer treat SARs as a standalone activity. They assess them as the outcome of upstream controls, from onboarding and customer due diligence to transaction monitoring and behavioural analysis.

The FCA has consistently stressed the importance of effective systems and controls to detect and prevent financial crime. In practice, this means testing not just whether a SAR was filed, but how the firm reached that decision.

Supervisors are examining the full journey from detection signal to investigative context to documented rationale.

Where data is fragmented, patterns are missed and narratives weaken. Where firms can unify customer data, transaction activity and historical alerts, suspicion becomes clearer, decisions faster and reporting more meaningful.

Volume is exposing operational fragility

The scale of financial activity in the UK has made SAR reporting a high-volume process, with hundreds of thousands of reports submitted annually.

Regulators are increasingly highlighting the risks created when volume meets manual workflows. Cases of delayed or poor-quality SARs are often linked to overwhelmed teams, ineffective monitoring outputs and weak prioritisation of risk.

The issue is not just resourcing. It is the inability of systems to prioritise, contextualise and escalate risk effectively.

The expectation is clear. Firms must detect suspicious activity consistently, at speed and with sufficient context to support decision making. Manual processes are not built for this level of scale or complexity. The challenge is signal quality as much as volume.

Auditability and explainable compliance

Regulators now expect firms to evidence not only why a SAR was filed, but why one was not.

This requires clear records of decision making, supporting data and investigative reasoning. Weak documentation of SAR decisions has already been cited by the FCA as an indicator of poor practice.

The standard is shifting towards compliance that is explainable, repeatable and reviewable at scale. That cannot be delivered through policy alone. It requires systems that capture and structure decision making as it happens.

## Technology as the determining factor

Taken together, these developments point to a clear conclusion. The effectiveness of a financial crime framework is inseparable from the technology that underpins it.

The expectation that firms can connect customer data, transaction activity, risk profiles and historical alerts into a coherent investigative view cannot be met through fragmented systems. Nor can consistent, well-documented decision making across large volumes of cases.

At the same time, UK authorities are becoming more data-driven in how they assess firms, placing greater emphasis on consistency, traceability and evidencing outcomes.

In this environment, AML effectiveness is judged not by policy, but by how well systems surface risk, support investigation and enable defensible outcomes.

## The quiet role of better systems

Firms investing in more advanced analytical and case management platforms are better able to move from detection to decision with speed and consistency.

By unifying customer context, transaction behaviour and historical activity, these systems enable investigators to understand not just what has happened, but why it matters. They reduce reliance on fragmented alerts and support a more complete assessment of risk.

They also introduce consistency. Escalation, investigation and decisioning follow structured workflows, ensuring rationale is captured, evidence retained and outcomes aligned to regulatory expectations.

Crucially, they close the gap between detection and action. Improved signal quality reduces noise and allows teams to focus on activity that genuinely warrants escalation.

The result is not just more efficient compliance, but more effective reporting.

A higher bar that will keep rising

The direction of travel in the UK is clear. Greater emphasis on data quality, consistency of reporting and supervisory scrutiny points to a more integrated and intelligence-led system.

For MLROs and compliance leaders, the message is simple. Suspicious activity reporting is no longer a downstream obligation. It is a test of the entire financial crime framework.

Those who treat it as an administrative process will struggle to meet expectations.

Those who treat it as an intelligence function, supported by the right analytical and technological capability, will be better placed to deliver reporting that is timely, credible and genuinely useful.



*[Quantum Data Engines](#) is a reg-tech company that helps financial institutions detect, manage, and report financial crime more effectively and efficiently.*