



Financial Compliance 2025: AML & Sanctions Gaps

*AML compliance costs have surged
significantly since 2016.*

*Yet false positive rates remain high. Here's why the investment isn't
solving the problem - and what will.*

FINANCIAL SERVICES

Financial Compliance 2025: AML & Sanctions Gaps

By Sayari Analyst Team · Published April 2025

AML compliance costs have surged significantly since 2016. Yet false positive rates remain high. Here's why the investment isn't solving the problem – and what will.

Between 2016 and 2023, compliance-related employee hours at financial institutions increased significantly. Bank IT budgets dedicated to compliance grew substantially. Yet AML false positive rates remain high, sanctions screening generates overwhelming false alerts, and customer onboarding that should take days stretches into weeks because beneficial ownership verification happens manually.

This is not a story about institutions failing to try. It's about architecture. Compliance programs built on disconnected databases, manual verification workflows, and name-matching logic cannot scale to meet modern financial crime complexity. The problem is not effort—it is design.

The AML Investment Paradox: More Spending, Same False Positive Rates

The false positive problem is structural, not accidental. Traditional AML systems rely on name-matching algorithms—a person named "Michael Smith" triggers an alert because a sanctions list contains "Mike Smith." The system cannot distinguish between genuine threats and coincidental name matches.

When a bank processes millions of transactions daily, a 90 percent false positive rate means compliance staff spend time on tickets they know are false positives. The system documents that screening happened but does not prevent financial crime detection.

More sophisticated transaction monitoring systems generate more alerts. More sophisticated name-matching engines generate more false positives faster. Institutions added headcount to

manage the volume, creating jobs processing false positives-jobs that do not prevent a single dollar of illicit financing.

Why Manual Beneficial Ownership Verification Slows Onboarding and Creates Gaps

Customer due diligence requires identifying beneficial owners-the natural persons who ultimately own or control a legal entity. For simple cases-a small business with one owner-this happens quickly. For complex structures-holding companies, trusts, layered ownership-it requires investigation.

Many institutions conduct this investigation manually. Compliance staff query public databases, cross-reference company registries, place phone calls to corporate agents, and assemble documents. A straightforward customer might onboard in three to five business days. A customer with complex ownership structure might wait three to five weeks.

This timeline creates two critical problems. First, it slows revenue-delays in customer onboarding mean delayed account opening, delayed funding, delayed business engagement. Second, and more serious, it creates gaps. When beneficial ownership verification is expensive and slow, programs may under-investigate edge cases or accept incomplete documentation rather than extend the investigation. The result is accounts opening with unverified beneficial owners-a direct violation of regulatory requirements and a direct vector for financial crime.

Adding more compliance staff does not fundamentally change the cost or timeline of beneficial ownership verification.

Sanctions Alert Fatigue: When Volume Erodes True Threat Detection

Sanctions screening is necessary. When name-based matching generates false positives at high rates, analysts face backlogs of alerts. An analyst might spend an hour on fifteen false positives and miss the genuine match buried at ticket twenty.

When the majority of alerts are false positives, the signal-to-noise ratio collapses. Analysts cannot trust their screening system. Institutions report that false positives have directly contributed to missed sanctions targets-genuine matches that went undetected in a flood of false alerts.

Threshold tuning is a zero-sum game. Lower the threshold, more genuine matches are missed. Raise it, more false positives are allowed through.

What an Efficient, Evidence-Based Compliance Program Requires

Institutions solving this problem are abandoning pure name-matching in favor of network-aware, evidence-based screening. Instead of asking "does this name match a sanctions list name?", they ask "is this customer connected to a known financial crime actor through corporate relationships, common beneficial owners, or transaction patterns?"

This requires three elements. First, a comprehensive database of corporate relationships and beneficial ownership-not from government registries alone, but from integrated public records across hundreds of jurisdictions, court filings, import-export data, and corporate disclosures. Second, pre-computed networks showing how entities connect through ownership, management, and transactional relationships. Third, automated screening that evaluates whether a customer sits on a known financial crime network rather than whether a name happens to match.

The difference is profound. A name-match system flags 100 transactions, 90 are false positives. A network-aware system flags 20 transactions, 18 are true matches and 2 are ambiguous-a case management problem, not a detection problem. Alert fatigue disappears. Analysts spend time on cases that matter. Beneficial ownership is already integrated into the screening function, so onboarding accelerates because verification happens automatically against verified data rather than manual queries.

The compliance investment of the past decade has been real. It has also been insufficient, because it targeted the wrong problem. Institutions added labor to manual processes. The compliance challenge in 2025 is not capacity-it is fundamentally different architecture.

Financial institutions managing AML, KYB, and sanctions screening can assess their current program by asking a simple question: what percentage of their compliance team's time goes to investigating cases they already know are false positives? If the answer is higher than twenty percent, the program is broken not from lack of effort, but from reliance on manual, name-based processes.

Sayari serves financial institutions navigating this transition. The Sayari platform integrates corporate and individual data from over 250 jurisdictions, including import-export records for more than 70 countries. The system computes beneficial ownership and counterparty

networks automatically, pre-flagging customers connected to known financial crime actors with court-admissible evidence. The result is sanctions screening identifying true matches with minimal false positives, beneficial ownership verification accelerating onboarding, and AML investigations starting with verified network data.

Request a demo to see how network-aware screening eliminates alert fatigue and delivers evidence-based compliance at scale. For more on how Sayari helps manage financial crime risk, explore our financial crime solution.

Please visit sayari.com to learn more.

This blog is for informational purposes and isn't intended to be legal advice.