SymphonyAI

The new financial crime ecosystem

Always-on Compliance™

Contents

Executive Summary

Financial institutions are transitioning from siloed, reactive compliance models to real time, AI enabled, fully integrated financial crime ecosystems. The next generation of capability delivers agility, transparency, and continuous adaptation to meet rapidly evolving regulatory and threat landscapes.

This future state enables continuous monitoring of global regulatory change and instant ingestion of emerging threat intelligence. Institutions automatically interpret updates to AML/CFT rules, sanctions programs, data standards, cyber signals, and criminal typologies.

Next generation systems provide open APIs, full model lineage, decision traceability, and real time dashboards for supervisors. Built in explainability ensures clarity around why alerts are triggered and how decisions are made.

Future platforms capture and analyse every operational decision—alert outcomes, analyst narratives, SAR filings, case patterns—to feed automated feedback loops. Models, rules, and workflows are refined autonomously.

KYC, AML, sanctions screening, fraud analytics, and case management converge into a single unified platform. Shared data, shared intelligence, and consistent risk scoring eliminate duplication and fragmentation.

AI becomes the backbone of detection and workflow orchestration. Always on context is provided through AI ready data pipelines, feature stores, advanced ML/LLMs, and multi agent systems that perform triage, summarisation, document extraction, SAR drafting, and escalation, bring capability together that

- Controls, policies, and thresholds adjust immediately - minimising regulatory exposure and keeping pace with fast moving risks.
- A shift from periodic, manual audits to continuous, technology enabled oversight, strengthening trust with regulators.
- Self optimising operations that reduce false positives, improve accuracy, and lower manual investigation costs.
- A single customer risk view, faster onboarding, improved detection quality, and lower integration and maintenance overhead.
- Highly accurate, faster decision-making and augmented investigator productivity, with explainable and auditable outcomes.

And the strategic impact: this marks the industry’s shift from defensive compliance to proactive, intelligent, continuously adaptive financial crime defence.

Today’s Financial Crime Challenges

Financial institutions are operating in an environment of intensifying regulation, rising compliance costs, shifting technology expectations, and growing scrutiny around AI adoption. Four critical challenges define the landscape.

1 **Regulators worldwide are increasing scrutiny** of sanctions screening, beneficial ownership transparency, and data integrity as transnational crime grows more sophisticated. Risk expectations continue to rise, with FATF expanding high risk jurisdiction lists and global regulatory regimes modernising in response to emerging criminal threats. Concurrently, real time payments and ISO 20022 migrations are forcing institutions to adopt real time controls and higher data quality standards, fundamentally reshaping compliance operations.

- The FATF continues to expand high risk jurisdiction lists, adding countries like Laos and Nepal to “Jurisdictions Under Increased Monitoring” in 2025—forcing banks to strengthen due diligence processes and reassess country risk models.
- Real time payments regulations create new compliance burdens. The EU Instant Payments Regulation now requires both sending and receiving euro payments within 10 seconds, forcing institutions to run sanctions and fraud checks in real time. Traditional batch screening is no longer viable, and inadequate real time controls trigger regulatory scrutiny.
- ISO 20022 migration raises data governance pressures, with incomplete fields (e.g., LEIs) leading to payment rejections and compliance breaches—already causing operational issues for banks processing cross border transactions.

2 **Compliance teams face overwhelming alert volumes,** with false positives reaching up to 95%, driving massive operational inefficiencies. Investigations remain the largest cost driver, often requiring extensive manual work far beyond

regulatory estimates. Rising fraud, increasing sanctions complexity, and growing personnel requirements have contributed to global compliance costs exceeding $270B. Institutions are urgently seeking automation and AI-driven optimisation to contain escalating cost pressures.

- False positives remain extremely high, with up to 95% of alerts in traditional rules-based AML systems proving non-suspicious, driving enormous operational inefficiencies. And Investigations are the biggest cost driver. Our analysis of client processes show that end-to-end investigations from alert to SAR can take 2 hours and can stretch to 20 hours when including full investigation, documentation, and review cycles.

- Manual workflows still dominate. Increasing transaction volumes and outdated rule sets force compliance teams to spend time chasing false alarms, diverting resources from genuine risks and increasing costs.

- Global compliance costs are escalating. By 2022–2025, compliance costs rose significantly due to fraud growth, sanctions complexity, and rising personnel requirements, with estimates exceeding $270B globally.

3 As regulatory expectations for explainability and auditability grow, **financial institutions increasingly prefer external solutions over internal builds.** Pre configured, regulator aligned AI models and integrated KYC/AML platforms are now the preferred path due to speed to value, lower maintenance overhead, and built in explainability. Rapid digitalisation—especially real-time payments and ISO 20022—has further expanded reliance on third party platforms with proven orchestration capabilities.

- Regulators prefer transparent, explainable, externally validated models. Guidance from the EU AI Act and U.S. Treasury emphasizes the need for explainability in model-driven decisions (e.g., sanctions screening, SAR filing). This makes external providers with pre-built explainability tooling more attractive than in-house teams building from scratch.

- Pre-built ML risk models are in strong demand. With rapid digitalisation, FIs seek out-of-the-box models and AI systems that come with regulator-friendly documentation, explainability, and audit readiness.

- Digital transformation expands outsourcing opportunities. Rapid growth of real-time payments, ISO 20022, and digital onboarding increases reliance on third-party platforms—especially those offering integrated KYC, TM, and sanctions solutions.

4 Despite strong investment in AI, **trust and governance concerns continue to stall deployment.** Executives cite data privacy and security as their top barrier, and regulators are introducing stringent requirements for explainable and responsible AI. Regional differences in consumer trust and mounting pressure from investors for transparency reinforce the need for robust governance, clear oversight mechanisms, and responsible AI frameworks.

- Data privacy and security concerns remain the top barrier. A majority of financial services executives cite data privacy and security risk as their biggest concern when deploying GenAI, slowing adoption despite high investment intentions.

- This has brought about a shift from GenAI hype to responsible AI standards. Responsible AI is critical to ROI, when regulators and executives prioritize governance over speed.

- Consumer trust varies by region. U.S. consumers demand transparency and human oversight, while Asia-Pacific consumers focus more on outcomes, revealing structural trust challenges that firms must manage.

- Increasing regulatory pressure on AI governance. Emerging frameworks (EU AI Act, Algorithmic Accountability Act, and others) require robust governance, auditability, explainability, and oversight—further incentivizing institutions to adopt vendor systems with mature controls.

Institutions recognise that unlocking GenAI's potential requires credible, transparent, and well governed AI systems.

The Next Generation of Financial Crime Capability

Financial institutions are shifting from reactive, siloed compliance operations to real time, AI enabled, fully integrated financial crime ecosystems. The next generation of capability is defined by five major advancements, all underpinned by intelligent, trusted AI.

Real Time Regulatory and Threat Awareness

Institutions will automatically interpret global regulatory changes and ingest live threat intelligence—spanning sanctions updates, cyber signals, law enforcement data, and emerging typologies. This enables instant policy and control adjustment, dramatically reducing regulatory lag and exposure.

Transparent, Regulator Aligned Architecture

Future platforms provide full explainability, auditability, and model lineage through open APIs and real time supervisory dashboards. This transforms regulatory engagement from periodic audits to continuous, technology enabled oversight.

Self Learning, Continuously Improving Operations

Every analyst action, alert outcome, SAR, and case narrative becomes structured intelligence. Systems learn from operational behaviour to refine detection logic, reduce false positives, and standardize decisions—delivering self-optimising compliance operations that lower cost and increase accuracy.

Fully Integrated Financial Crime Platform

KYC, AML, sanctions screening, fraud, behavioural analytics, and case management converge into a unified environment. This creates a single customer risk view, accelerates onboarding, eliminates duplication, and provides end to end lifecycle management across all risk domains.

AI Driven Reasoning and Multi Agent Orchestration

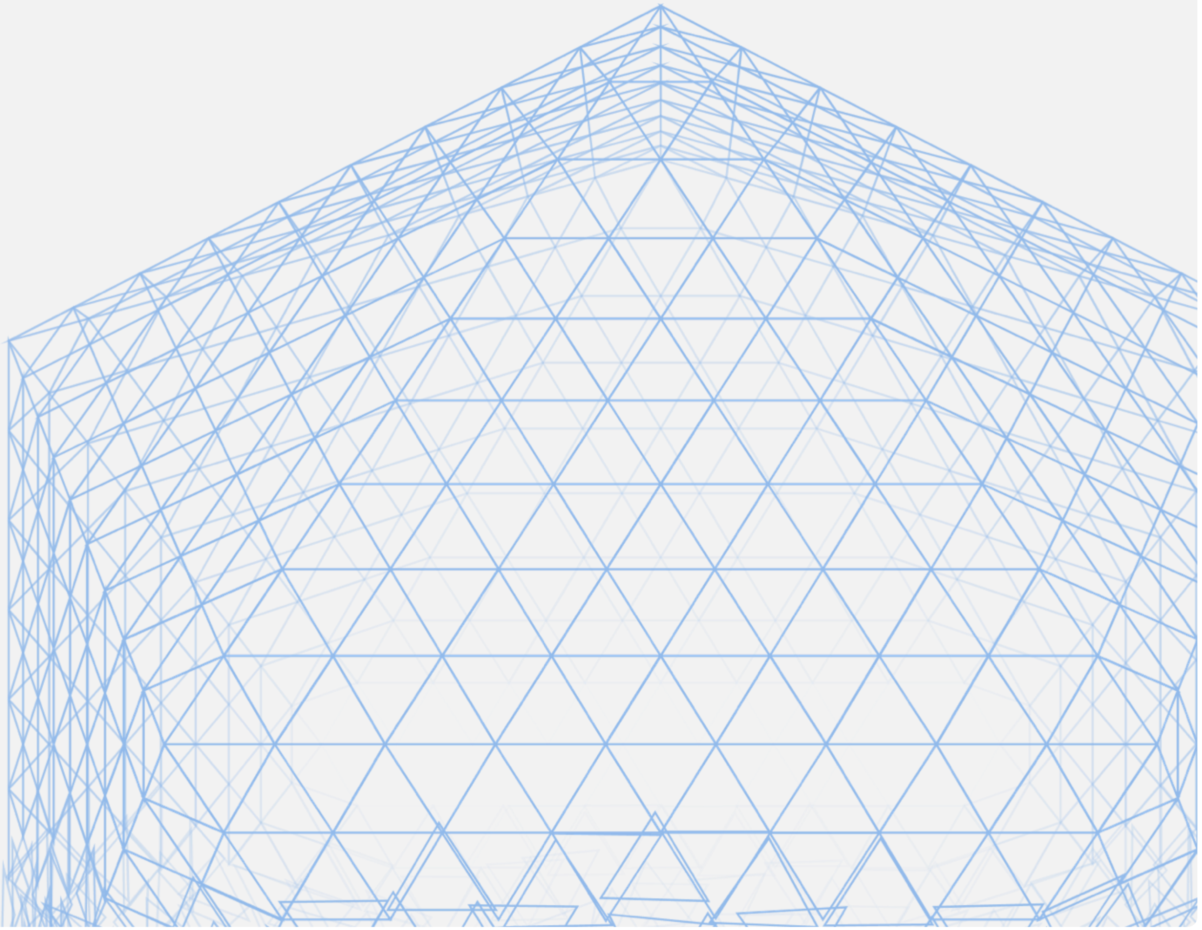
Modern financial crime defence is powered by AI-ready data, feature stores, advanced ML/LLMs, and multi agent systems that handle triage, summarisation, evidence gathering, SAR drafting, and escalation. This augments investigators and delivers faster, more consistent, and more explainable decisions.

The Bottom Line

The next generation of financial crime capability delivers:

- Real time alignment with fast moving regulation and threats
- Transparent, auditor ready governance
- Self-improving operations driven by continuous learning
- Integrated risk disciplines across the entire lifecycle
- AI orchestrated workflows delivering scale, speed, and precision

Together, these advances shift institutions from defensive compliance to proactive, intelligent, continuously adaptive financial crime prevention.



About Symphony Risk Intelligence

Symphony Risk Intelligence (SRI) is an AI-native FinCrime platform that's designed to help financial institutions move from reactive to proactive risk management. It centralises and optimizes every aspect of compliance operations, from data ingestion and model management to investigation and reporting.

Every layer of the cloud-native platform has been built to leverage the latest predictive, generative, and agentic AI technology to enable greater automation, improved detection effectiveness, and significant operational efficiency savings. SRI represents a reimagining of the compliance operating model, built to eliminate legacy inefficiencies, unify fragmented systems, and turn compliance into a driver of business growth. With the ability to automate a wide range of processes and operational tasks, SRI halves the compliance workload while equipping teams with powerful AI-driven tools to accelerate workflows and maximise performance.

SRI allows financial institutions to begin their transformational journey to a next generation, evergreen infrastructure that futureproofs payment ecosystems and prepares businesses to scale with speed, efficiency, and regulatory resilience.

Find out more:
symphonyai.com/financial services

SymphonyAI

www.symphonyai.com

About SymphonyAI

SymphonyAI, 2024 Microsoft Partner of the Year for Business Transformation– AI Innovation, is building the leading enterprise AI SaaS company for digital transformation across the most critical and resilient growth verticals, including retail, consumer packaged goods, finance, manufacturing, media, and IT/enterprise service management. SymphonyAI verticals have many leading enterprises as clients. Since its founding in 2017, SymphonyAI has grown rapidly to 3,000 talented leaders, data scientists, and other professionals. SymphonyAI is an SAI Group company, backed by a $1 billion commitment from Dr. Romesh Wadhwani, a successful entrepreneur and philanthropist.

SymphonyAI provides AI-focused SaaS solutions developed from the ground up for fighting financial crime. An end-to-end offering compiled from more than 25 years of knowledge in tackling money laundering and fraud, our award-winning product ecosystem comprises an innovative and modern approach to financial crime investigation using world-leading agentic, predictive, and gen AI. From KYC/CDD and transaction monitoring through to payments fraud, entity resolution, and sanctions, PEP, and adverse media screening, SymphonyAI is a trusted name in finance technology with more than a third of the world's top 100 banks enjoying the power, efficiency, effectiveness and productivity that our solutions provide.

Author

Craig Robertson

Financial Crime & Compliance SME, APAC

craig.robertson@symphonyai.com

Get started:
symphonyai.com/get-started