WHITE PAPER

SymphonyAI

Transforming Financial Crime Compliance in Insurance

Building a scalable, intelligence-led compliance for a more complex risk landscape

Executive summary

Insurance is no longer a secondary target for financial crime. Criminal networks are increasingly exploiting the complexity of insurance products, distribution channels, and claims processes while regulators raise expectations for effectiveness, transparency, and accountability.

At the same time, many insurers remain reliant on legacy AML frameworks built on static rules, manual reviews, and fragmented systems. These approaches are no longer sufficient. They drive high operational costs, generate excessive false positives, and fail to detect the sophisticated, evolving patterns of financial crime. The result is a widening gap between regulatory expectations and operational reality, exposing insurers to financial, reputational, and strategic risk.

A fundamental shift is required from reactive, periodic compliance to **Always-on Compliance**. This means moving toward continuous, risk-based monitoring across the entire customer and policy lifecycle, enabling insurers to identify and respond to threats in real time.

AI and agentic AI are central to this transformation. While AI enhances detection and insight, agentic AI enables execution, automating workflows, orchestrating investigations, and delivering end-to-end compliance processes. Together, they allow organizations to move from manual, siloed operations to integrated, intelligence-led financial crime prevention. This evolution redefines the role of compliance. No longer a cost center, it becomes a driver of agility, intelligence, and resilience supporting faster onboarding, better risk decisions, stronger regulatory outcomes, and improved customer trust.

What must leaders do now?

- **Assess the operating model:** Identify gaps in legacy systems, data, and workflows
- **Adopt a risk-based, lifecycle approach:** Embed controls across onboarding, servicing, and claims
- **Invest in AI and agentic capabilities:** Start with high-impact use cases and scale
- **Break down silos:** Move toward unified, intelligence-led platforms
- **Enable transformation:** Align people, processes, and governance to support continuous compliance

The direction is clear. Financial crime is evolving rapidly and so must the insurance compliance function. Insurance leaders must act now to mitigate growing FinCrime risk, stay compliant with regulatory expectations to gain a strategic advantage in a more complex, risk-driven market.

The changing financial crime landscape in insurance

Despite being an industry built on risk management, insurance has historically been perceived as lower risk compared to banking. That assumption is now outdated. Financial crime is increasing in scale, sophistication, and reach, and insurers are becoming an attractive target due to the very characteristics that define the industry.

From underestimated risk to active target

Criminal networks are actively exploiting structural features of insurance, including:

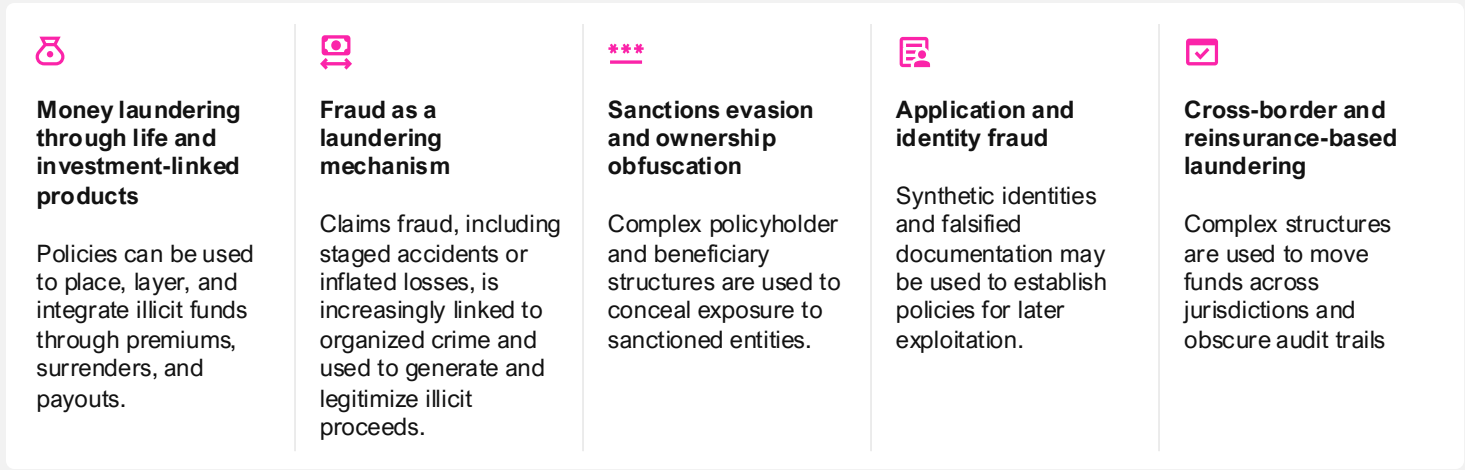
- Long-duration products that enable the layering and integration of illicit funds over time
- Complex ownership and beneficiary structures
- Intermediary-driven distribution models (brokers, agents)
- High-value, low-frequency events such as claims and policy surrenders

These characteristics make insurance uniquely vulnerable because of how and when risk materializes.

Importantly, exposure is wider than life insurance. While life products have long been associated with money laundering risk, general insurance lines are increasingly vulnerable, particularly where fraud, claims, and digital channels intersect.

Expanding and evolving financial crime typologies

Financial crime in insurance is increasingly sophisticated, organized, and interconnected:



These typologies span the full insurance lifecycle, from onboarding to claims and payouts, making isolated controls insufficient.

The convergence of fraud and anti-money laundering

A critical shift for insurers is the growing convergence of fraud and AML.

Fraud is often a gateway to money laundering, a mechanism used by organized crime networks or a signal for broader financial crime activity. This directly challenges one of the most persistent industry assumptions that fraud and AML can be managed separately. In reality, siloed approaches create blind spots, allowing risk to go undetected.

In many insurance lines, particularly property and casualty, fraud is not an isolated issue but a systemic challenge that increasingly intersects with broader financial crime.

Rising regulatory expectations

Global regulatory bodies, including the International Association of Insurance Supervisors (IAIS), the Financial Conduct Authority (FCA), European Insurance and Occupational Pensions Authority (EIOPA), and Financial Crimes Enforcement Network (FinCEN), are increasingly aligned on a clear expectation: where financial crime risks are understood, insurers must take action, applying risk-based controls that reflect their exposure, even as regulatory scope continues to evolve.

This reflects the growing emphasis on the risk-based approach (RBA), where insurers are expected to:

- Identify, assess, and understand financial crime risks across their operations
- Focus controls and resources where exposure is greatest
- Demonstrate that their programs actively mitigate risk

Regulatory focus is also expanding beyond traditionally regulated areas. Authorities across multiple jurisdictions are reassessing AML obligations in insurance, particularly in non-life segments, indicating a clear shift toward broader and more rigorous oversight. This is reflected in IAIS Insurance Core Principle 22, FCA supervisory guidance, and supporting risk analysis from EIOPA, demonstrating a clear shift toward more rigorous and more consistent oversight.

The implication for insurance leaders

Insurance is no longer low risk and treating it as such creates material exposure.

For senior leaders, this requires a fundamental shift in mindset:

- **From underestimating exposure to recognizing systemic risk**
- **From isolated controls to integrated, lifecycle-based oversight**
- **From reactive compliance to proactive, intelligence-led prevention**

If financial crime risk has fundamentally changed, the question is whether current approaches are equipped to manage it.

Why traditional AML approaches fall short

The current compliance operating model in insurance is operationally expensive and strategically insufficient.

Built on static rules, fragmented workflows, and manual processes, it was not designed for the complexity, scale, or velocity of modern financial crime. While it may meet minimum regulatory expectations, it does not deliver the effectiveness, agility, or insight required today.

Issue	What it causes	Strategic implication
Rules-based systems generate noise, not insight	• 90–95% false positives • Investigators focused on low-value alerts • Limited detection of complex risk	Compliance becomes inefficient and reactive, with resources diverted away from genuine threats
Fragmentation obscures risk	• Disconnected systems and data • Hidden relationships and patterns • Incomplete risk visibility	Inability to identify enterprise-wide financial crime risk, leading to missed threats and weaker controls
Manual processes constrain scale	• High reliance on human effort • Slow investigations and decision-making • Rising operational costs	Compliance cannot scale with growth, increasing cost pressures and operational risk
Lack of lifecycle visibility creates blind spots	• Risk assessed in isolation • Inability to track evolving behavior • Missed cross-lifecycle patterns	Institutions fail to detect how risk develops over time, exposing them to more sophisticated financial crime

Traditional AML approaches are not only inefficient, they are structurally misaligned with how financial crime risk emerges in insurance. They:

- **Consume significant resources without proportional effectiveness**
- **Limit visibility across the enterprise**
- **React to risk rather than anticipating it**
- **Struggle to scale with increasing complexity**

Incremental improvements will not address these structural limitations. A fundamentally different approach is required which is integrated, intelligence-led, and designed for the realities of insurance.

The unique challenges of financial crime in insurance

Financial crime in insurance behaves fundamentally differently from banking. Yet many compliance frameworks remain adapted from banking models, creating structural gaps in detection and oversight.

Insurance risk is defined by four characteristics:

Complex products

Life, pensions, and annuities enable funds to be introduced, layered, and extracted within legitimate structures.

Lifecycle-driven risk

Risk develops over time, across onboarding, policy servicing, claims, and payouts, requiring continuous, contextual assessment.

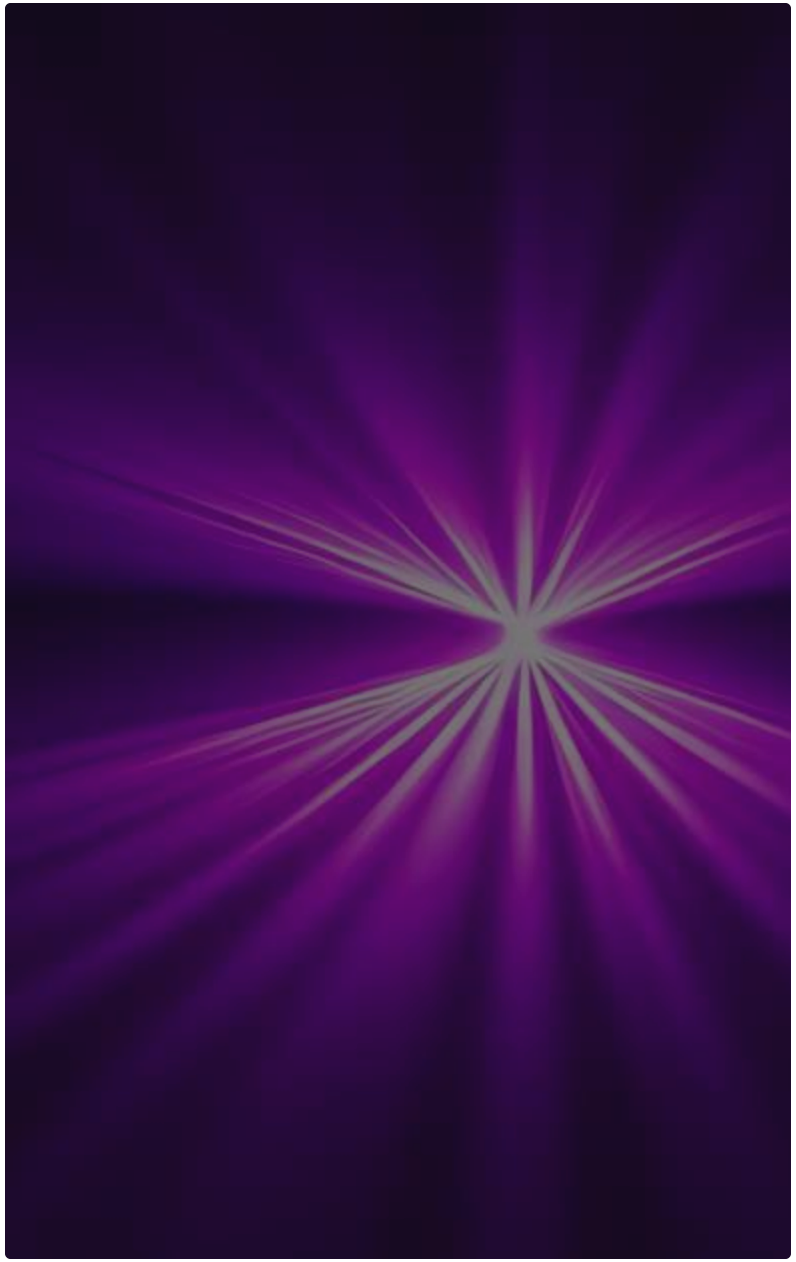
Intermediary-driven distribution

Brokers and agents reduce direct customer visibility, introducing variability in data quality, due diligence, and risk exposure.

Limited transaction signals

Unlike banks, insurers rely on irregular, event-driven interactions, reducing the effectiveness of traditional transaction monitoring models.

Risk in insurance often crystallizes at the point of claim, where fraud and money laundering converge. As a result, financial crime risk is less visible but more complex, lifecycle-driven rather than transaction-driven, and dispersed across products, intermediaries, and events. Banking approaches are insufficient, insurance requires a tailored, intelligence-led model.



A risk-driven, lifecycle-based approach to FinCrime prevention

Financial crime risk in insurance does not occur at a single point; it evolves across the customer and policy lifecycle.

Addressing this requires a shift from static, point-in-time controls to a **risk-driven, lifecycle-based approach** in which risk is continuously assessed, and controls adapt dynamically. This is the foundation of **'Always-on Compliance'.**

A lifecycle view of risk

Effective financial crime prevention aligns controls to where risk actually emerges.

Risk area	Key risks	Required approach	Impact
Onboarding and underwriting	• Identity fraud and sanctions exposure • Misrepresentation of customer risk • Complex ownership structures	• Real-time screening and onboarding • Dynamic risk scoring at entry • Early identification of high-risk entities and relationships	• Earlier detection of high-risk customers and entities • Reduced onboarding risk and downstream exposure • Stronger risk segmentation from the outset
Policy lifecycle monitoring	• Unusual premium patterns or policy changes • Behavioral shifts inconsistent with customer profile • Emerging links to high-risk entities or jurisdictions	• Continuous, event-driven monitoring • Dynamic risk re-scoring as new data emerges • Integration of internal and external intelligence	• Continuous visibility of evolving risk • Faster identification of suspicious behavior • Shift from periodic review to real-time risk awareness
Claims processing	• Fraudulent or inflated claims • Claims linked to organized crime • Use of claims to legitimize illicit funds	• Integration of fraud and AML signals • Contextual assessment against full customer and policy history • Detection of patterns across policies, claims, and networks	• Improved detection of complex and organized fraud schemes • Greater accuracy through contextual, lifecycle-based assessment • Reduced losses and enhanced financial crime detection at the point of risk crystallization
Payout and exit	• Early surrenders or withdrawals • Payments to third parties or complex structures • Cross-border exposure and sanctions risk	• Final-stage risk validation before disbursement • End-to-end visibility of customer activity • Controls aligned to jurisdictional and counterparty risk	• Prevention of illicit fund extraction at point of exit • Reduced regulatory and sanctions exposure • Stronger control over high-risk transactions and disbursements

Connecting the lifecycle: From fragmentation to a 360° view

A lifecycle-based model is only effective when risk signals are connected.

This requires a unified view of the customer, policyholder, and related parties, integration across onboarding, monitoring, and investigations, and the ability to link customers, intermediaries, beneficiaries, and entities. Connecting data and workflows in this way creates a 360° view of risk surfacing hidden relationships and patterns that would otherwise remain undetected.

From static controls to dynamic risk management

Traditional AML applies uniform controls regardless of context. A lifecycle-based model is adaptive by design.

It enables insurers to continuously reassess risk through dynamic, event-driven scoring, trigger alerts based on material changes rather than fixed intervals and prioritize high-risk activity with greater precision. Compliance shifts from periodic checks to continuous, intelligence-led decisioning.

The impact of a lifecycle-based approach

A lifecycle-based model enables insurers to detect risk earlier and more accurately, reduce false positives through contextual prioritization, strengthen regulatory defensibility, and align compliance with core business processes.

In an increasingly complex financial crime landscape, compliance must be continuous, connected, and adaptive. This approach aligns directly with the risk-based model, requiring institutions to identify, assess, and mitigate risk proportionate to their exposure.

Crucially, this shift is enabled not only by AI-driven insights, but by agentic AI that can act on those insights triggering workflows, coordinating responses, and ensuring controls are applied dynamically across the lifecycle.

The role of AI and agentic AI in modern financial crime prevention

AI is a practical enabler of more effective, scalable, and resilient compliance. Increasingly, agentic AI extends this capability, moving from insight to execution by automating workflows and orchestrating end-to-end compliance processes.

For insurers, the value of AI lies not in replacing existing controls, but in enhancing them, improving precision, reducing manual effort, and enabling continuous risk coverage across the lifecycle.

Enhancing detection and reducing noise

AI can significantly improve the effectiveness of core compliance capabilities.

Capability	How AI helps
Name screening	AI enhances matching accuracy by understanding context, variations, and relationships, reducing false positives while maintaining detection quality.
Transaction and behavior monitoring	Machine learning models identify patterns and anomalies that static rules cannot detect, enabling earlier and more accurate identification of risk.
Entity resolution and network detection	AI connects customers, policies, intermediaries, and beneficiaries, surfacing hidden relationships and exposing complex financial crime networks.
Investigations with generative AI	Generative and agentic AI enriches case data from multiple sources, consolidates relevant risk signals into a single view, and produces clear case summaries and narratives. This reduces manual effort and allows investigators to focus on decision-making.

The impact is immediate: higher detection accuracy with materially less noise, faster investigations, and more consistent outcomes.

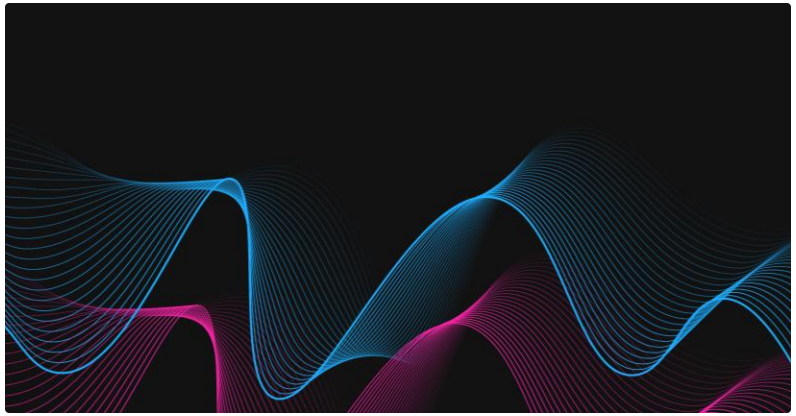
Agentic AI: automating end-to-end compliance workflows

Agentic AI represents the next step – a move from assistance to **intelligent automation of workflows.**

AI agents can:

- Automate alert triage, prioritization, and routing
- Enrich and prepare investigation cases
- Generate regulatory reports and disclosures
- Execute complex, multi-step compliance processes

This is different from a simple task automation. Agents operate across workflows, with human oversight, to deliver end-to-end process efficiency.



The real value of agentic AI is not in automating individual tasks, but in redesigning end-to-end compliance workflows.

Agents act as collaborative digital partners, coordinating activities across silos, orchestrating processes, and ensuring consistency at scale. This enables a shift to a hybrid human–AI operating model, where:

Agents manage execution, coordination, and data-driven tasks

Humans focus on judgment, strategy, and oversight

The result is faster cycle times, more consistent outcomes, and a level of operational responsiveness that manual coordination cannot match.

Two outcomes are particularly critical for insurance leaders:

Significant cost and effort reduction **01**

Agent-led automation transforms the economics of compliance:

- Alert noise is reduced before investigators engage
- Manual data gathering is eliminated

This enables:

- 50–70% faster case resolution
- Up to 80% reduction in false positives
- Substantial reductions in cost per alert and investigation
- Scalable operations without proportional FTE growth

Compliance teams shift from volume processing to value-added analysis.

Continuous risk coverage **02**

By embedding AI agents across the operating model, compliance becomes continuous rather than periodic.

Agents can:

- Monitor regulatory changes and emerging threats in real time
- Update detection models, rules, and policies dynamically
- Identify and close compliance gaps as they arise

This ensures:

- Continuous regulatory alignment
- Always-on monitoring across the lifecycle
- Audit-ready compliance at scale

Risk coverage is no longer intermittent. It is always active, always current.

AI with governance, not black boxes

Modern AI frameworks are designed with:

- **Explainability** – every decision can be understood and justified
- **Auditability** – full traceability of actions and outcomes
- **Human-in-the-loop oversight** – ensuring control and accountability

This enables insurers to adopt AI with confidence, meeting regulatory expectations while strengthening governance.

AI is not about replacing compliance functions, but **redefining their effectiveness.**

It enables insurers to:

- **Improve detection accuracy while reducing false positives**
- **Lower operational cost and increase scalability**
- **Accelerate investigations and decision-making**
- **Strengthen regulatory defensibility and audit readiness**

In a landscape defined by complexity and constant change, AI provides the foundation for intelligent, adaptive, and resilient financial crime prevention.

Breaking down silos: Toward a unified FinCrime platform

Across many insurance organizations, AML, fraud, sanctions, and KYC functions operate in disconnected environments. While individually effective, this fragmentation creates blind spots, duplication, and slower investigations.

Modern financial crime spans these domains. Managing them in isolation limits visibility and reduces effectiveness.

A unified approach that brings AML, fraud, sanctions, and KYC into a single risk framework, enables shared intelligence, coordinated decision-making, and a more complete view of risk.

Historically, integration required complex and costly large-scale platform consolidation. A more effective model is now emerging. Rather than replacing systems, organizations can orchestrate intelligence across existing environments. Agentic AI enables this by connecting data, workflows, and decisions across compliance domains creating a unified view of risk while preserving existing investments.

This shift extends to data. Instead of centralizing information, organizations can bring intelligence to the data, accessing, interpreting, and connecting it at source across structured and unstructured environments. The result is a move from data consolidation to data orchestration.

With integrated data and workflows, compliance becomes real-time and intelligence-led. Risk is assessed continuously, alerts are prioritized based on true risk, and investigations are faster, more consistent, and more defensible.

The result is a fundamental shift in the operating model – from fragmented controls to an integrated, intelligence-led ecosystem.

Operational excellence: Reducing cost while increasing effectiveness

Amid rising costs, increasing regulatory expectations, and limited access to skilled talent, many insurers are finding their current compliance model increasingly unsustainable. Alert volumes continue to grow, false positives consume the majority of investigative effort, while skilled compliance resources remain scarce and expensive.

Agentic AI can help insurers reverse these outcomes by automating end-to-end workflows, reducing manual intervention, and enabling more efficient, scalable compliance operations.

Area	Current challenge	AI-enabled transformation	Business impact
Alert management	• High alert volumes driven by false positives • Investigators overwhelmed by low-value alerts	• AI-led prioritisation and triage • Noise reduction before investigator review	• Up to **80–95% reduction in false positives** • Focus on high-risk activity • Faster, more efficient alert handling
Investigations	• Manual data gathering and fragmented case preparation • Inconsistent case quality	• Automated data enrichment and case assembly • Investigation-ready case delivery	• **50–70% faster case resolution** • Improved consistency and quality • Reduced investigator effort
Workflow efficiency	• Fragmented systems and manual handoffs • Repetitive, non-value tasks	• End-to-end workflow orchestration • Integrated case management across functions	• **Significant reduction in manual effort** • Faster decision-making • More consistent execution
Operating model scalability	• Linear headcount growth required to manage volume • Talent constraints and rising cost of skilled resources	• AI-driven automation and augmentation • Workload absorbed without proportional hiring	• **6x increase in investigator productivity** • Scalability without headcount growth • Lower cost per alert and investigation
Overall compliance effectiveness	• High cost with limited effectiveness • Reactive, volume-driven operating model	• Intelligence-led prioritisation and continuous monitoring • Adaptive, risk-based decisioning	• Lower cost of compliance • Improved detection accuracy • **Alert-to-SAR timelines reduced from days to hours**

Operational excellence in financial crime prevention is about **cost-to-effectiveness optimization.**

Agentic AI, combined with workflow redesign enables insurers to:

- **Lower the cost of compliance through automation**
- **Improve effectiveness through better detection and prioritization**
- **Address talent constraints through intelligent augmentation**
- **Scale sustainably without linear increases in resources**

In a more complex and regulated environment doing more with greater accuracy and lower cost is a key advantage.

Regulatory expectations and explainability

As insurers face increasing exposure to financial crime across onboarding, policy servicing, and especially claims, supervisors expect institutions to demonstrate measurable effectiveness in reducing financial crime risk, supported by clear, defensible audit trails.

For insurers, this raises the bar across three critical dimensions:

Transparency **Explainability** **Auditability**

From controls to demonstrable effectiveness

Traditional compliance models focused on process ensuring the right checks were in place. Today, regulators are asking a different question: Are those controls effective across the full insurance lifecycle?

Insurers must evidence how risks are identified and mitigated across onboarding, servicing, and claims, demonstrate effectiveness at key risk moments, and provide clear, defensible justification for decisions. This marks a shift from process compliance to performance-driven compliance.

Auditability and continuous oversight

Auditability must be embedded into the operating model, not added retrospectively.

This requires full traceability of data, decisions, and actions, end-to-end visibility across the lifecycle, and consistent, regulator-aligned documentation. As compliance becomes increasingly AI-enabled, audit readiness must be built in from the outset ensuring institutions remain continuously audit-ready.

AI governance as a core capability

Effective AI adoption depends on strong governance. This includes model validation and monitoring, ongoing testing and recalibration, controls for fairness and consistency, and clearly defined human oversight.

A robust governance framework ensures AI operates within defined boundaries which are aligned with both internal policies and regulatory expectations.

Working with regulators, not around them

AI does not replace compliance controls. It enhances how they are delivered. Leading institutions engage regulators early, demonstrate how AI improves detection and reduces risk, and provide clear evidence of explainability and control. This collaborative approach builds confidence and supports smoother adoption.

AI and compliance are not in conflict.

When implemented correctly, AI enables insurers to:

- **Improve transparency** through explainable decisioning
- **Strengthen auditability** across the full policy lifecycle
- **Enhance effectiveness** in detecting and managing financial crime risk
- **Maintain continuous alignment** with evolving regulatory expectations

The result is more defensible compliance.

The priority for insurance leaders, then, is straightforward: adopt AI in a transparent, governed, and regulator-ready way to strengthen compliance and build trust.

A practical roadmap for insurance leaders

Transforming financial crime compliance does not require a big bang approach.

Leading insurers are taking a **phased, pragmatic path** focusing on high-impact areas first, building confidence in new capabilities, and scaling over time.

Phase	Focus	Key actions	Outcome
1. Assess the current state	Establish baseline	• Identify fragmentation across systems, data, and workflows • Assess reliance on manual processes and rules-based detection • Evaluate gaps in lifecycle visibility and risk coverage	Clear understanding of current limitations and highest-value transformation opportunities
2. Prioritize high-impact use cases	Deliver quick wins	• Focus on name screening and false positive reduction • Address claims-related risk and fraud/AML convergence • Improve investigation efficiency and case management	Early, measurable impact with minimal disruption to operations
3. Introduce AI to augment existing capabilities	Enhance, not replace	• Apply AI overlays to improve detection • Automate alert triage and case enrichment • Introduce dynamic risk scoring	Improved detection accuracy and reduced manual effort, building confidence in AI adoption
4. Redesign workflows, not just technology	Transform operations	• Integrate AML, fraud, and sanctions processes • Eliminate manual handoffs and duplication • Embed AI into end-to-end workflows	Greater efficiency, consistency, and operational effectiveness
5. Build toward a unified, lifecycle-based model	Enable Always-on Compliance	• Connect data across onboarding, monitoring, and claims • Establish a unified customer and policyholder risk view • Enable continuous, event-driven risk assessment	End-to-end visibility and continuous, intelligence-led risk management
6. Strengthen governance and regulatory alignment	Ensure sustainability	• Implement robust AI governance frameworks • Maintain explainability and auditability • Engage regulators proactively	Regulator-ready, trusted, and scalable compliance transformation

The path forward is clear:

- **Start small, think big**
- **Deliver value early, then scale**
- **Evolve from fragmented controls to integrated, intelligence-led compliance**

This will enable organizations to position compliance as a strategic capability that supports growth, resilience, and trust.

Case study

Scaling real-time financial crime prevention at a leading US insurer

A leading US insurance and financial services provider, with more than 15 million customers and a network of over 400,000 agents and employees, sought to strengthen its ability to detect and prevent financial crime at scale.

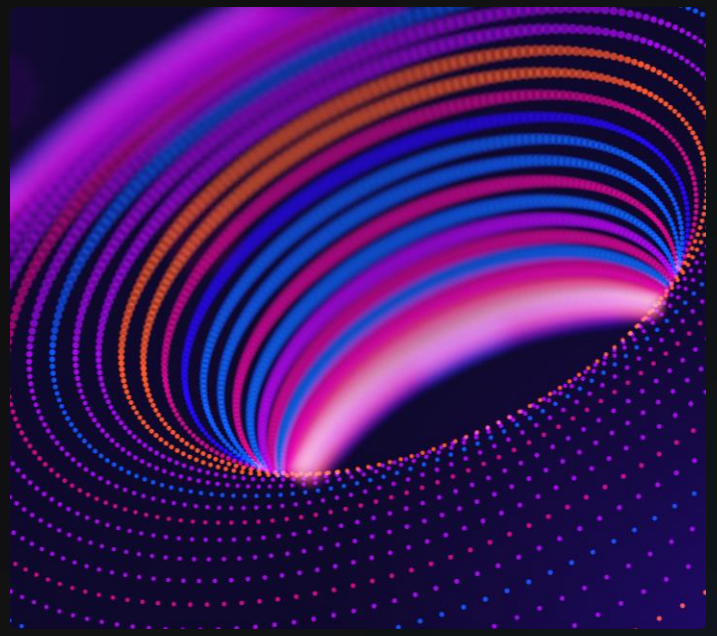
The challenge

Operating at significant scale, the organization was required to monitor and secure more than 500,000 transactions daily across a complex and distributed environment.

Key challenges included:

- Managing high transaction volumes while maintaining real-time risk visibility
- Responding to evolving regulatory expectations and increasingly sophisticated fraud and financial crime typologies
- Scaling compliance and fraud prevention capabilities in line with business growth
- Ensuring consistent, efficient operations across a large and diverse customer and distribution base

The existing approach needed to evolve from traditional controls to a more scalable, real-time, and intelligence-led model.



The approach

The insurer implemented an AI-enabled financial crime and fraud prevention platform to unify monitoring, enhance detection, and support real-time decisioning.

This enabled:

- Integrated AML, sanctions, KYC, and fraud capabilities, providing a unified view of financial crime risk
- Real-time monitoring and screening, including customer due diligence, sanctions, and adverse media checks
- Event- and transaction-level fraud detection, supporting both payment and policy-related risk scenarios
- End-to-end case management and regulatory reporting, improving investigation consistency and auditability

This approach supported a shift toward a more connected and responsive compliance model, capable of operating at scale without compromising speed or accuracy.

The impact

The transformation delivered significant operational and risk management benefits:

Real-time decisioning capabilities, with response times measured in milliseconds

High-volume scalability, supporting over 500,000 daily transactions with efficient batch processing completed in approximately two hours

Improved detection and response, enabling faster identification and mitigation of suspicious activity

Enhanced operational efficiency, reducing friction across compliance and fraud workflows

Greater agility, allowing the organization to adapt quickly to regulatory and threat changes

The outcome

By modernizing its financial crime and fraud capabilities, the insurer established a scalable, real-time compliance operating model aligned to the demands of a complex and evolving risk environment.

The transformation strengthened the organization's ability to protect customers, support business growth, and maintain regulatory confidence, while reinforcing trust across its extensive customer and partner ecosystem.

Conclusion: The future of FinCrime in insurance

Financial crime in insurance has fundamentally changed and so must the response.

What was once considered a lower-risk domain is now a growing target for sophisticated criminal networks. At the same time, regulatory expectations have intensified, demanding not only compliance, but demonstrable effectiveness, transparency, and resilience.

Yet many insurers remain constrained by legacy models – fragmented systems, manual processes, and static controls that are no longer fit for purpose.

A defining shift in compliance

Across the industry, a clear shift is underway, from:

Periodic reviews	**Continuous, Always-on Compliance**
Rules-based detection	**Intelligence-led risk identification**
Siloed functions	**Unified financial crime ecosystems**
Manual operations	**AI-enabled, scalable workflows**

This is not incremental change. **It is redefining the compliance operating model.**

From cost center to strategic capability

Compliance is no longer just a regulatory requirement. it is becoming a source of strategic advantage.

When modernized, it enables insurers to improve detection precision, reduce operational costs, strengthen regulatory confidence, and build trust across customers, partners, and regulators. By following this model, compliance evolves from a **cost center into a driver of agility, intelligence, and resilience.**

AI as the enabler of transformation

AI and increasingly, agentic AI provides the foundation for this shift.

By enhancing detection, automating workflows, and enabling continuous risk coverage, AI allows insurers to move from reactive to proactive risk management, scale operations without proportional cost increases, and maintain alignment with evolving threats and regulations. When implemented with strong governance and human oversight, **AI strengthens regulatory compliance.**

The imperative for insurance leaders

Financial crime is becoming more complex, more connected, and more difficult to detect using traditional approaches. At the same time, expectations from regulators, boards, and stakeholders continue to rise.

Insurance leaders must act now to rethink outdated assumptions, move beyond fragmented and manual operating models, embrace lifecycle-based, intelligence-led approaches, and invest in AI as a core capability.

The imperative is clear: modernize now and embed intelligence, integration, and continuous risk awareness at the core of the operating model.

Top five priorities for insurance leaders

Shift to Always-on Compliance

Move from periodic reviews to continuous, lifecycle-based risk monitoring across onboarding, servicing, and claims.

Adopt AI to improve detection and reduce cost

Use AI to enhance screening, monitoring, and investigations – reducing false positives while increasing detection accuracy.

Break down silos across AML, fraud, and sanctions

Integrate functions, data, and workflows to create a unified view of financial crime risk.

Redesign compliance operating models for scale

Automate manual processes, augment investigators, and enable growth without proportional increases in headcount.

Embed governance, explainability, and regulatory alignment

Ensure AI-driven compliance is transparent, auditable, and aligned with evolving regulatory expectations.

About SymphonyAI

SymphonyAI, 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 2000 leading enterprises as clients globally. 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 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.

SymphonyAI

Learn more at www.symphonyai.com

Authors

Charmian Simmons

Financial Crime and Compliance Advisor
Strategy and Innovation
SymphonyAI

Lala Huseynli

Financial Services Marketing
and Growth Lead, EMEA
SymphonyAI

Get in touch to discuss how your organization can redesign financial crime compliance operating model, reduce operational costs, improve effectiveness, and enable Always-on Compliance across the insurance lifecycle, powered by AI and agentic AI.

Email us directly at connect.fs@symphonyai.com
Visit www.symphonyai.com