Managing Fraudulent Life & Health Claims: Challenges, Emerging Risks & The Role of AI

Shari Or

Head L&H Underwriting & Claims SE Asia
Swiss Re

Sharad Mahamia

Head L&H Underwriting & Claims India
Swiss Re

01

WHY FRAUD IS A PORTFOLIO RISK

Managing fraudulent Life & Health claims

Fraud as Strategic Risk

Fraud in Life & Health insurance is a portfolio-level risk impacting pricing, underwriting, and trust in APAC markets.

Evolving Fraud Patterns

Fraud schemes have evolved from opportunistic to organised, exploiting identity gaps and cross-border complexities.

Broader Costs of Fraud

Fraud increases costs beyond claims, including investigations, operational inefficiencies, and adverse market effects.

Role of AI and Governance

AI enhances fraud detection but requires strong governance and human oversight for effective intervention.

Why fraud matters more than ever: Systemic, scalable, and upstream

Upstream Fraud Shift

Fraud now starts early in the lifecycle, impacting underwriting and portfolio outcomes beyond claims.

Cross-Border and Organized Fraud

Fraud schemes are increasingly organized, crossing borders and exploiting fragmented identity systems.

Professional Facilitation and Collusion

Modern fraud involves complex networks, including insiders, making detection more difficult.

Strategic Risk Management

Insurers must adopt unified lifecycle views to prevent fraud and protect reputation and fairness.

The true cost of fraud: Beyond claims leakage to portfolio drag

COST CATEGORY	WHAT IT INCLUDES	WHY IT MATTERS STRATEGICALLY
Direct claims leakage	Fraudulent payouts; partial exaggeration	Immediate profit impact; can mask systemic schemes
Investigation & recovery cost	SIU time, vendors, legal, field checks	Consumes scarce expertise; affects operational capacity
Operational friction	Manual reviews, escalations, rework	Slower cycle times; higher expense ratio
Customer impact	Delays and repeated requests for evidence	Erodes trust; increases complaints and churn
Portfolio drag	Pricing distortion; adverse selection; persistency effects	Long-term sustainability and competitiveness

Fraud landscape in Asia: Growth, digitisation, and ecosystem complexity

Growth and Digital Expansion

Rapid digital adoption in health insurance increases convenience but expands fraud attack surfaces.

Fragmented Health Ecosystems

Diverse data standards hinder consistent fraud detection across providers and administrators.

Complex Identity Verification

Variable identity systems create gaps exploitable through synthetic and manipulated identities.

Organised and Cross-Border Fraud

Coordinated fraud schemes and cross-border document manipulation complicate fraud detection.

02

FRAUD TYPOLOGIES AND CHALLENGES

Life insurance fraud in a new era: Synthetic identities, collusion, and escalation tactics

Synthetic Identities Threat

Fraudsters create synthetic digital personas from stolen data, passing checks and enabling false claims.

Collusion and Document Forgery

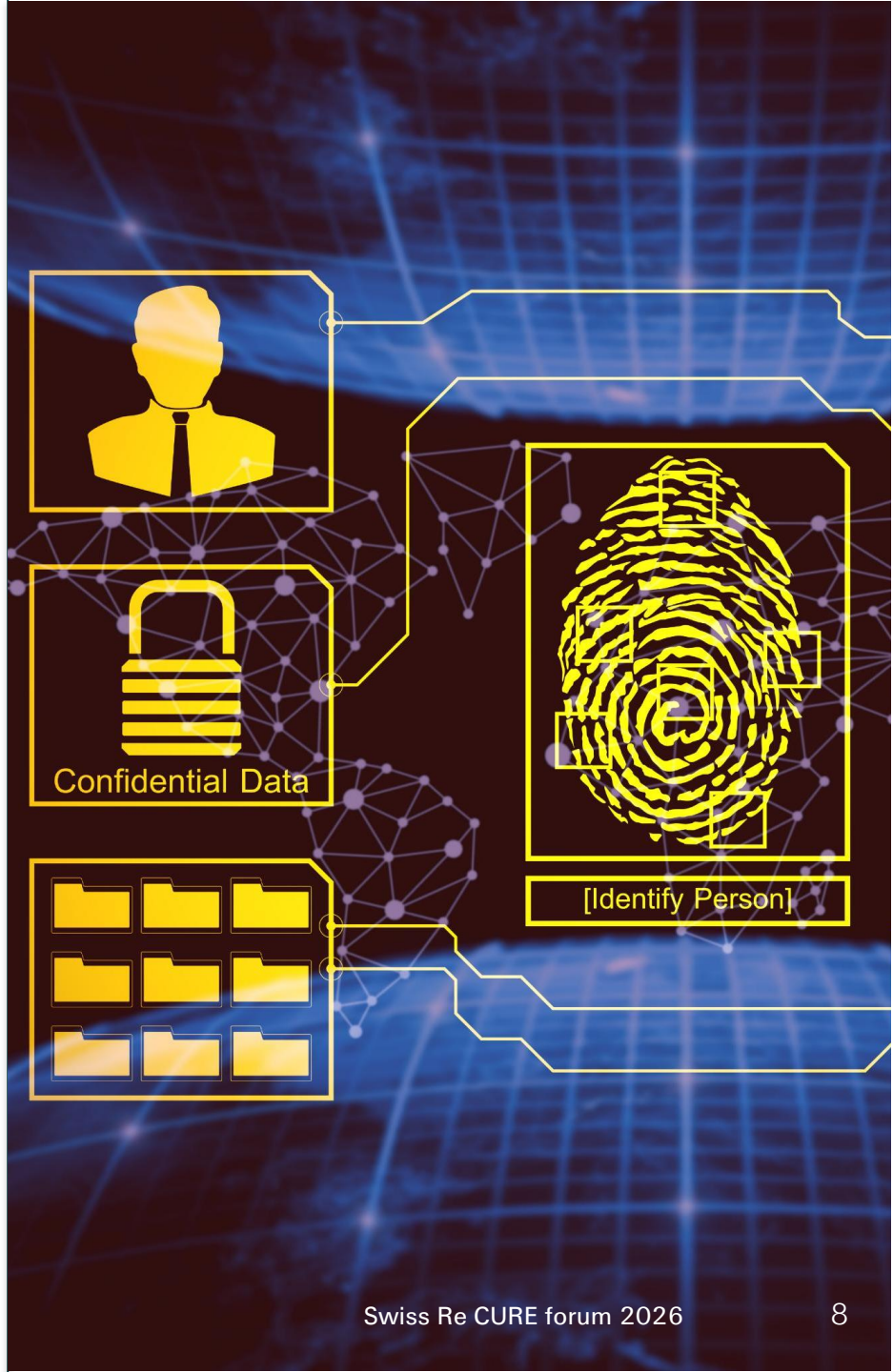
Fraud networks manipulate medical records and forge documents, creating credible evidentiary chains.

Behavioral Manipulation Tactics

Fraudsters use escalation, legal threats, and pressure tactics to bypass insurance controls effectively.

Lifecycle Fraud Controls

Effective fraud prevention requires early underwriting checks, ongoing reviews, and AI-human collaboration.



Health insurance fraud: Provider-driven patterns and network dynamics

Provider-Driven Fraud Patterns

Health insurance fraud often involves overbilling, upcoding, phantom procedures, and identity swapping by providers.

Network Dynamics in Fraud

Providers act as central nodes connecting patients and services, enabling organized fraud schemes within networks.

Challenges in Fraud Detection

Fragmented data and inconsistent coding complicate establishing baselines and detecting fraudulent provider behavior.

Effective Fraud Management Strategies

Combining provider benchmarking, network analytics, audits, and AI improves fraud detection while protecting customer experience.

Key structural challenges: Data fragmentation, identity complexity, and reactive controls

STRUCTURAL CONSTRAINT	WHAT IT LOOKS LIKE IN PRACTICE	CONTROL IMPLICATION
Data fragmentation	Disconnected UW/claims/provider systems; inconsistent fields	Invest in data standards and cross-silo visibility
Identity complexity	Synthetic IDs; weak cross-institution validation	Layered identity checks and longitudinal consistency tests
Cross-border documents	Authentic-looking certificates; upstream manipulation	Contextual verification; investigator networks
Behavioural pressure	Escalation, urgency, legal threats to accelerate payout	Capture interaction signals; protect decision governance
Reactive detection	Discovery after payment; limited feedback to UW	Early-claim programs and closed-loop remediation

03

CASE STUDIES: HOW STRUCTURAL GAPS ARE EXPLOITED

Why case studies matter: Turning structural challenges into actionable lessons

Value of Case Studies

Case studies translate structural challenges into concrete, actionable lessons for leadership teams to implement.

Common Fraud Mechanics

Fraud schemes share mechanics like identity manipulation, onboarding misrepresentation, and weak process controls.

Early Warning Signals

Case studies reveal early red flags often missed due to siloed data and reactive controls in fraud detection.

Cross-Functional Alignment

Case-based learning fosters collaboration across underwriting, claims, and special investigation units to improve fraud controls.

Singapore case study: Policy accumulation, financial justification, and non-disclosure

Policy Accumulation Risks

Rapid accumulation of insurance policies signals risk when cover exceeds income-based underwriting norms, necessitating cross-policy aggregation checks.

Non-Disclosure Challenges

Material non-disclosure and misrepresentation during application complicate claims and highlight the need for rigorous underwriting and verification.

Importance of Documentation

Clear evidence trails including disclosures, underwriting rationale, and investigation findings are crucial in contested claims and dispute resolution.

Fraud Management Strategy

Effective fraud management involves early detection, portfolio steering, and consistent governance to reduce exposure and maintain customer experience.

Malaysia case study: Organized syndicate, forged applications, and beneficiary abuse

Organized Syndicate Risk

Fraud driven by coordinated groups targeting vulnerable individuals and exploiting weak onboarding controls.

Forged Applications and Identify Manipulation

Policies created without genuine consent using forged signatures and falsified documentation.

Beneficiary Structuring Abuse

Unrelated or non-obvious beneficiaries used to extract payouts, bypassing insurable interest expectations.

Staged or Manipulated Claim Events

Claims supported by fabricated or misrepresented events to trigger policy payouts,

Control Implications

Reinforces need for stronger onboarding validation, beneficiary checks, and early-stage risk detection.

Indonesia case study: Repetitive claims, document forgery, and regulatory response

Patterns of Fraudulent Claims

Fraud appears as repetitive claims with forged documents and regional patterns, indicating organized activity.

Regulatory and Control Responses

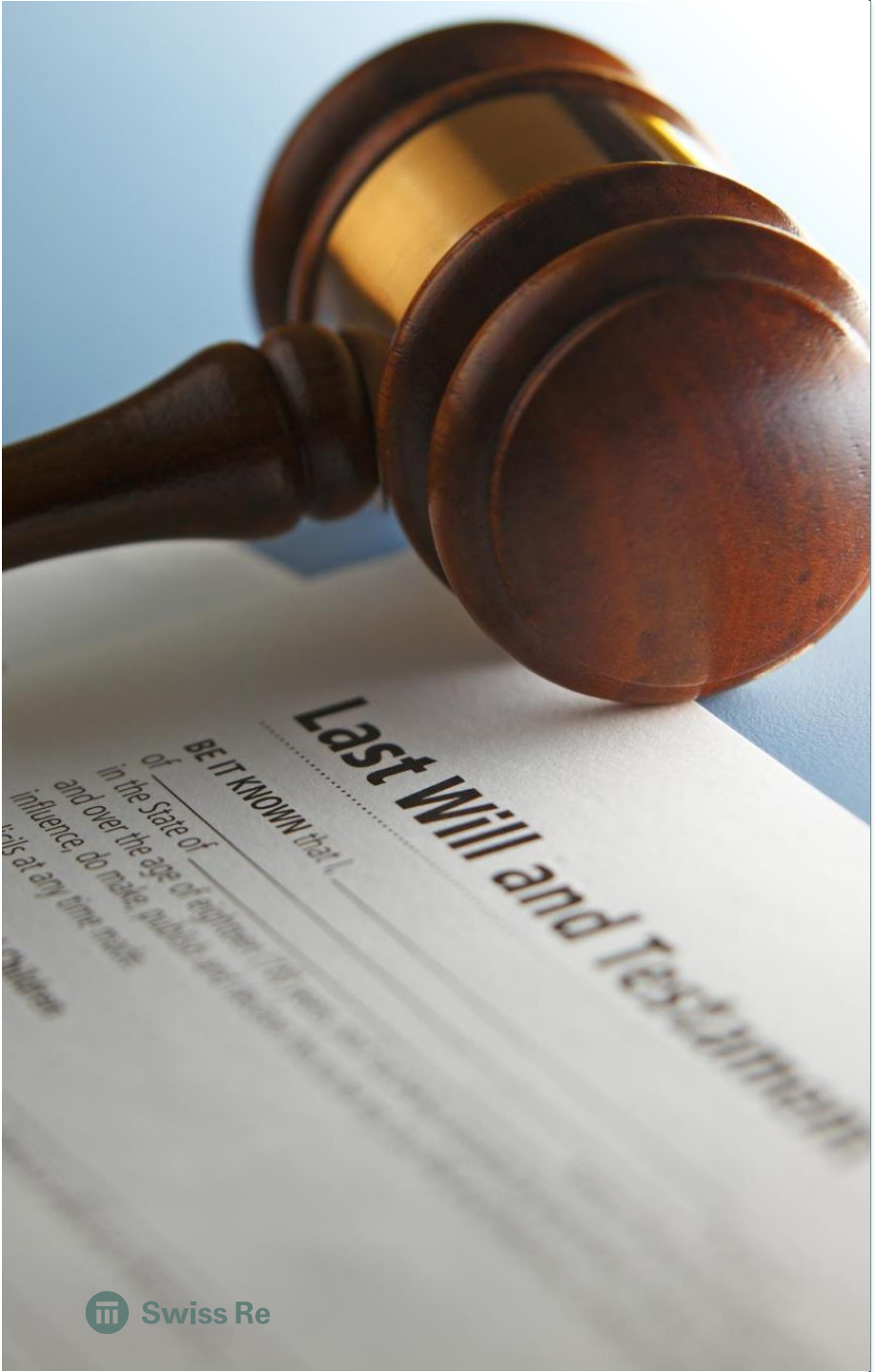
Regulators strengthened anti-fraud strategies and verification to address systemic risks in insurance claims.

Data Analytics for Fraud Detection

Analytics identify similarity patterns and clusters across regions, aiding early detection of fraud waves.

Governance and Control Measures

Strong governance, internal controls, and feedback loops with underwriting improve fraud resilience.



Vietnam case study: Insurable interest and non-disclosure tested in court

Insurable Interest Challenges

Cases in Vietnam reveal disputes over unclear insurable relationships and fraudulent policy setups lacking legitimate ties.

Non-Disclosure Risks

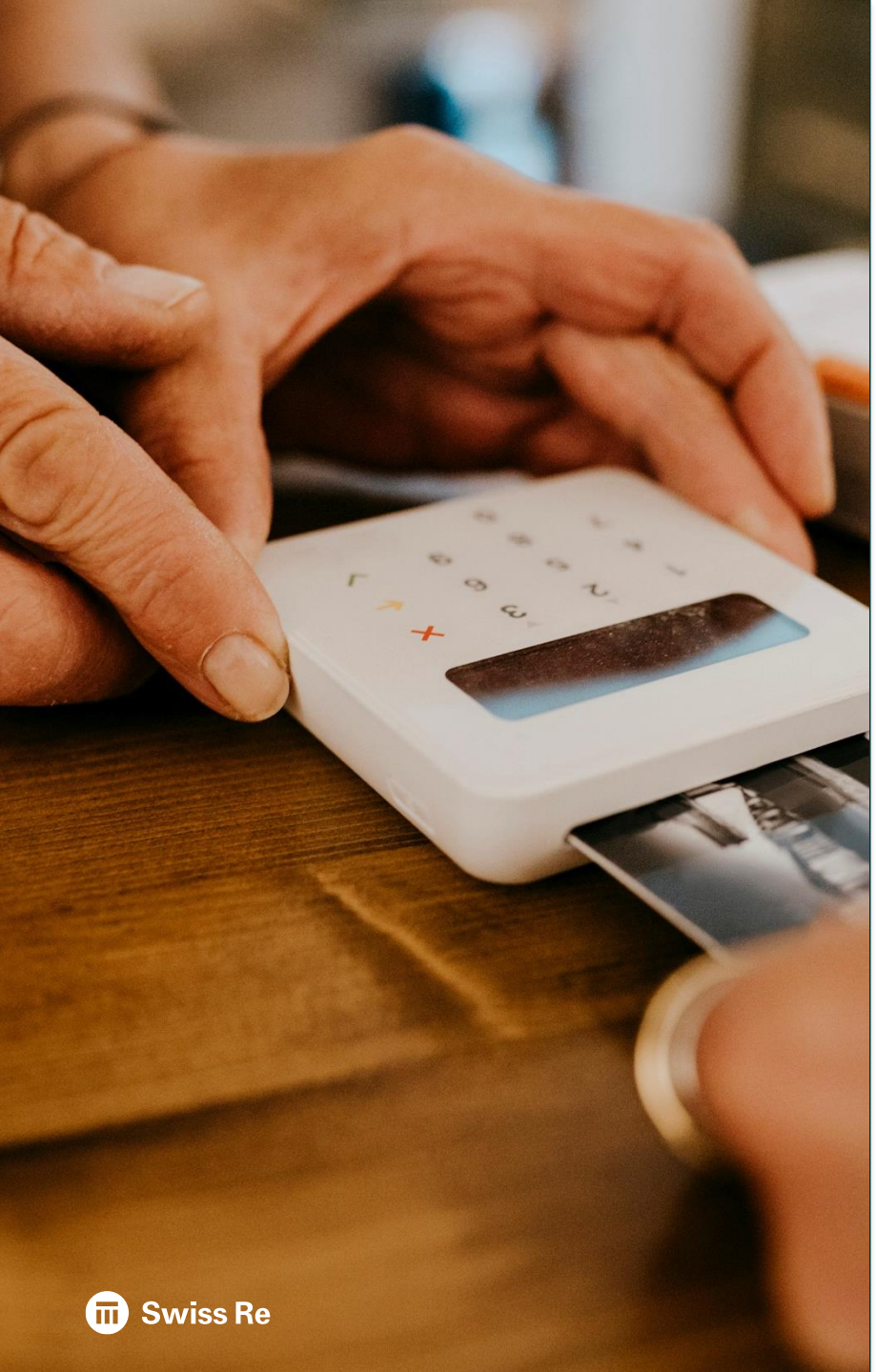
Concealment of pre-existing health conditions on applications led to claim denials and legal scrutiny in insurance cases.

Control and Governance Measures

Operationalizing insurable interest validation and balanced disclosure controls are crucial for fraud risk management.

Legal Defensibility Importance

Strong audit trails, signed documents, and clear disclosures enhance legal defensibility in contested insurance claims.



Thailand case study: Agent Fraud & Premium Misappropriation

Premiums diverted through agent channels

Customers were instructed to transfer premiums to the agent instead of the insurer, exploiting weak verification of payment flows.

False promises used to induce policy purchase

Incentives such as discounts or gifts were used to encourage early or larger premium payments, increasing fraud scale.

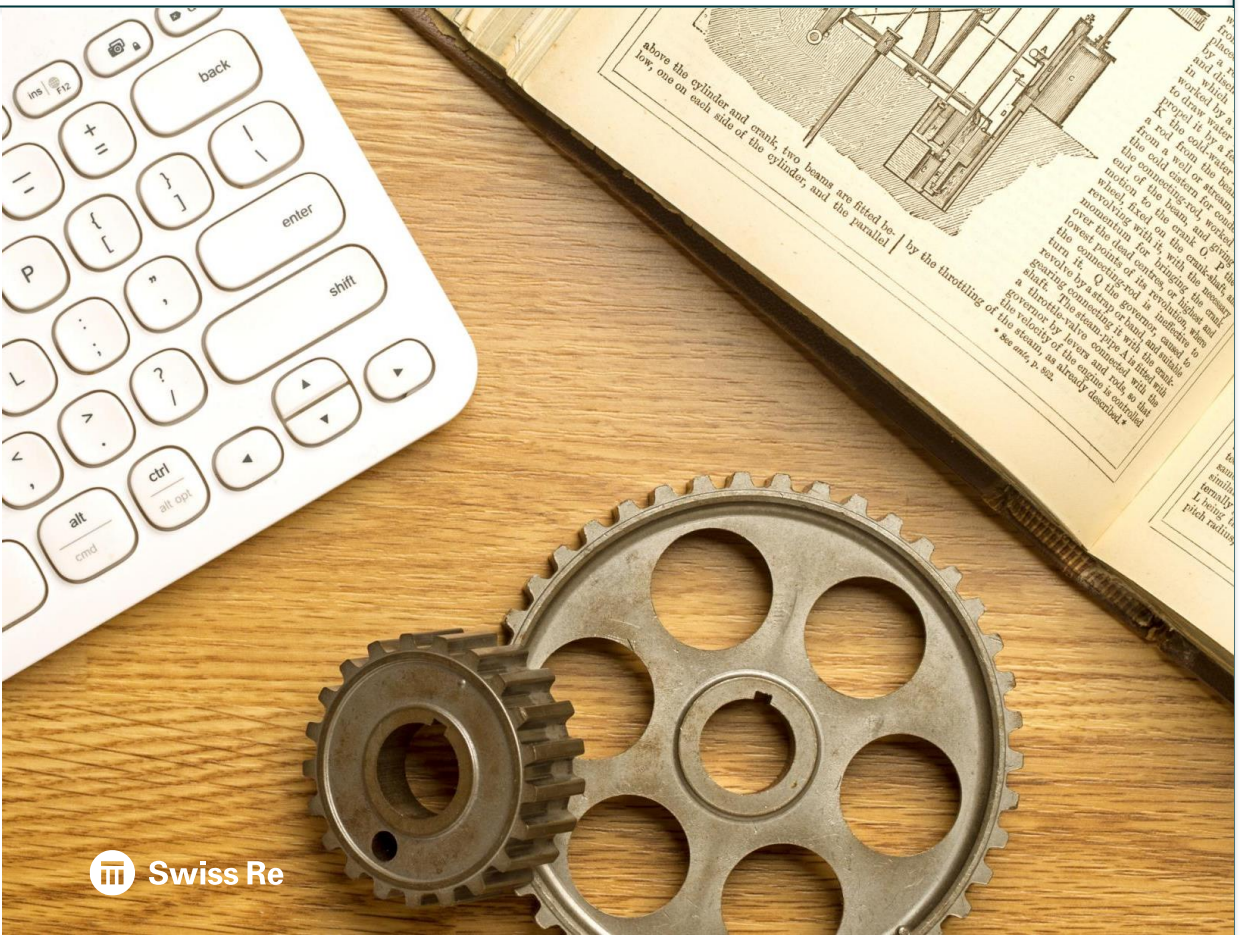
Forged or fabricated receipts issued to customers

Fake documentation was created to simulate valid policy issuance and conceal non-remittance of premiums.

Fraud detected only after policy servicing inconsistencies

The scheme surfaced when discrepancies were identified during servicing or claim verification – often too late.

India case study: Insider-enabled fraud and weak segregation of duties



Insider-Enabled Fraud Risks

Insider misuse involves forged documents, manipulated records, and fraudulent claims over years, highlighting internal threat dangers.

Importance of Governance Design

Segregation of duties is essential to prevent single roles from end-to-end control, reducing fraud risks effectively.

Auditability and Anomaly Detection

Systems must log changes and use analytics to flag unusual patterns like repeated approvals or suspicious payouts.

Human-in-the-Loop and Risk Culture

High-risk decisions require peer review and escalation, supported by whistleblowing and routine control testing.

Common patterns across APAC: Upstream origin, identity/document focus, and network effects

PATTERN	TYPICAL EARLY SIGNALS	BEST CONTROL POINT
Upstream origin	Early-duration claims; rapid policy accumulation	Underwriting & in-force monitoring
Identity/document focus	Inconsistent timelines; missing history; reused documents	Document intelligence + identity verification
Collusion	Too-perfect documentation; repeated facilitators	Network analytics + targeted investigations
Behavioural manipulation	Escalation pressure; legal threats; urgency	Governed decision workflows
Network effects	Claim clusters by region/provider/beneficiary	Portfolio dashboards & clustering

Implications for insurers: Upstream controls, integrated data, and collaboration

Early-Stage Controls

Strengthen early-stage controls like KYC, consent verification, and agent monitoring to prevent downstream losses effectively.

Integrated Data Lifecycle

Integrate underwriting, servicing, and claims data for a comprehensive lifecycle view to detect patterns and organized schemes.

Risk-Based Triage Model

Implement risk-based triage using analytics to fast-track low-risk claims and escalate suspicious ones efficiently.

AI with Human Oversight

Use AI for pattern recognition and document intelligence, ensuring decisions are explainable and human-reviewed.

Governance and Security

Reinforce governance with segregation of duties, access controls, and audit trails to manage insider risks effectively.

Collaboration Across Market

Share intelligence and collaborate across insurers and reinsurers to detect fraud waves early and benchmark best practices.

04

AI & THE MODERN FRAUD RESPONSE AT SCALE

Why is AI fraud growing so fast?

The result is **more attacks**, **at lower cost**, with **higher success rates**.

GenAI enables massive scale

Fraudsters can now launch thousands of attacks simultaneously using bots and automation.

Tools are cheap and accessible

Gen AI tools have lowered the barrier to entry, so advanced skills are no longer required.

Attacks are more convincing

Deepfake voices, synthetic identities, and AI-generated documents are increasingly indistinguishable.

AI-driven fraud has surged, increasing by 1,210% in 2025*

*Pindrop, AI Fraud Is Surging: What It Is, Why It's Growing, and What It Means for Businesses

Why Life Insurance is a Prime Target

Life insurance has a unique position in fraudsters' schemes. High-value payouts, extended timelines, and streamlined application processes create a perfect storm for synthetic identities to flourish.

Here's why:

Accelerated underwriting programs lower detection barriers.

Modern carriers increasingly rely on simplified and automated underwriting that uses fewer touchpoints and limited documentation. While this speeds up customer onboarding, it also opens the door for synthetic identities to bypass traditional checks.

Premium payments build a facade of legitimacy.

A classic tactic in synthetic identity fraud is to establish a consistent payment history. Fraudsters may pay premiums over months or even years, creating a false sense of credibility. By the time they submit a death claim, the synthetic identity looks seasoned and trustworthy.

Large, delayed payouts give fraudsters both time and reward

Life insurance claims can take months to process and often involve six- or seven-figure sums. This delay gives fraudsters a window to move money and cover their tracks before audit triggers.

Where fraud shows up across the L&H value chain

The important shift is not only more fraud, but how far upstream it now starts.

Distribution & acquisition

Life

- **Fake or stolen identity**
- Income / occupation inflation
- **Non-disclosure of medical history**

Health

- Ineligible dependents added to coverage
- Broker/employer collusion on enrollment status
- Identity changes on medical reports

Application & underwriting

Life

- Digitally altered medicals
- **Misrep of smoking, BMI, alcohol / drug use**
- Evasion of financial underwriting

Health

- Fake residency status
- Amending claims history or prior coverage
- **Moving through and amending answers to lower premium**

In-force & servicing

Life

- Address, bank or beneficiary changes
- Customer impersonation
- Timely coverage and GIO exercising

Health

- Membership sharing
- Misuse of pre-auth or referrals
- **Providers inflating severity to generate unnecessary treatments**

Claims

Life

- **Fabricating evidence**
- Medical practitioner fraud
- **Using AI to amend timings or change diagnoses**

Health

- Phantom billing where services never delivered
- **Forged documentation or duplicate billing**
- Upcoding or unbundling to increase reimbursement

05

NAVIGATING THE SOLUTION LANDSCAPE

A crowded marketplace?

Insurtech's are working across multiple disciplines, Swiss Re already have partnerships in some areas but our long-term ambition is to move to a more ecosystem proposition.

Swiss Re * Existing partner

Why traditional controls fall short: Predictability, scalability limits, and late detection

Predictability Challenges

Rule-based systems are predictable and can be bypassed by savvy fraudsters adapting their tactics.

Scalability Limitations

Manual reviews cannot scale with rising claim volumes and document complexity, causing delays and inconsistent fraud detection.

Late Fraud Detection

Detection often happens too late, after payouts, missing upstream fraud activities and network-based schemes.

Need for Data-Driven Controls

Modern fraud control needs adaptive, data-driven frameworks using analytics and risk-based triage to improve detection.

Practical AI use cases: real-time triage, translation, and investigator productivity

USE CASE	PRIMARY VALUE	OPERATIONAL IMPACT	TYPICAL RISK TO MANAGE
Real-time claims triage	Prioritise high-risk cases	Faster genuine claims;	False positives if data quality is weak
Document intelligence	Detect anomalies in unstructured docs	Reduced manual review; improved evidence quality	Adversarial document generation
Translation & extraction	Speed cross-border review	Shorter cycle times; consistent review	Context loss without expert oversight
Network analytics	Uncover hidden relationships	Identify organised schemes earlier	Explainability and governance needs

What leading insurers do: Hybrid models that blend AI, expert rules, and investigators

Hybrid Fraud Detection Model

Leading insurers adopt hybrid models combining AI, expert rules, and human investigators for effective fraud detection.

Layered Screening Process

Layered screening uses AI triage, rule-based filters, and investigator review to reduce false positives and improve accuracy.

Governance and Integration

Effective fraud models require governance maturity, workflow integration, and clear escalation and feedback processes.

Continuous Learning and Prevention

Mature insurers use fraud learning as a lifecycle engine to prevent fraud through underwriting and ongoing monitoring.

From detection to prevention and from individual claims to networks

Increasing Fraud Sophistication

Fraud methods will grow more advanced as digital tools empower organised actors to professionalise their techniques.

AI-versus-AI Dynamic

Insurers and fraudsters will engage in an AI arms race, advancing detection and evasion capabilities respectively.

Shift to Prevention

Industry focus will move earlier to underwriting, onboarding, and behavioral signals instead of just claims detection.

Network-Level Fraud Intelligence

Using graph and similarity analytics to detect organised fraud schemes by mapping relationships and patterns.

Risk-Based Workflow

Claims are processed according to risk levels with automated payments, targeted verification, and escalated investigations.

Ecosystem Collaboration

Information sharing and standardisation across insurers, reinsurers, and industry bodies will strengthen fraud prevention.

Key takeaways and actions: Data foundations, hybrid

Invest in Data Foundations

Consistent, integrated data across systems improves control and AI performance in fraud detection.

Hybrid Controls Model

Combine expert rules, AI anomaly detection, and human judgement for effective fraud management.

Network and Portfolio Analytics

Use clustering and relationship analysis to reveal fraud hotspots across regions and channels.

Governance and Collaboration

Strengthen controls internally and collaborate across the ecosystem to enhance fraud prevention.

Legal notice