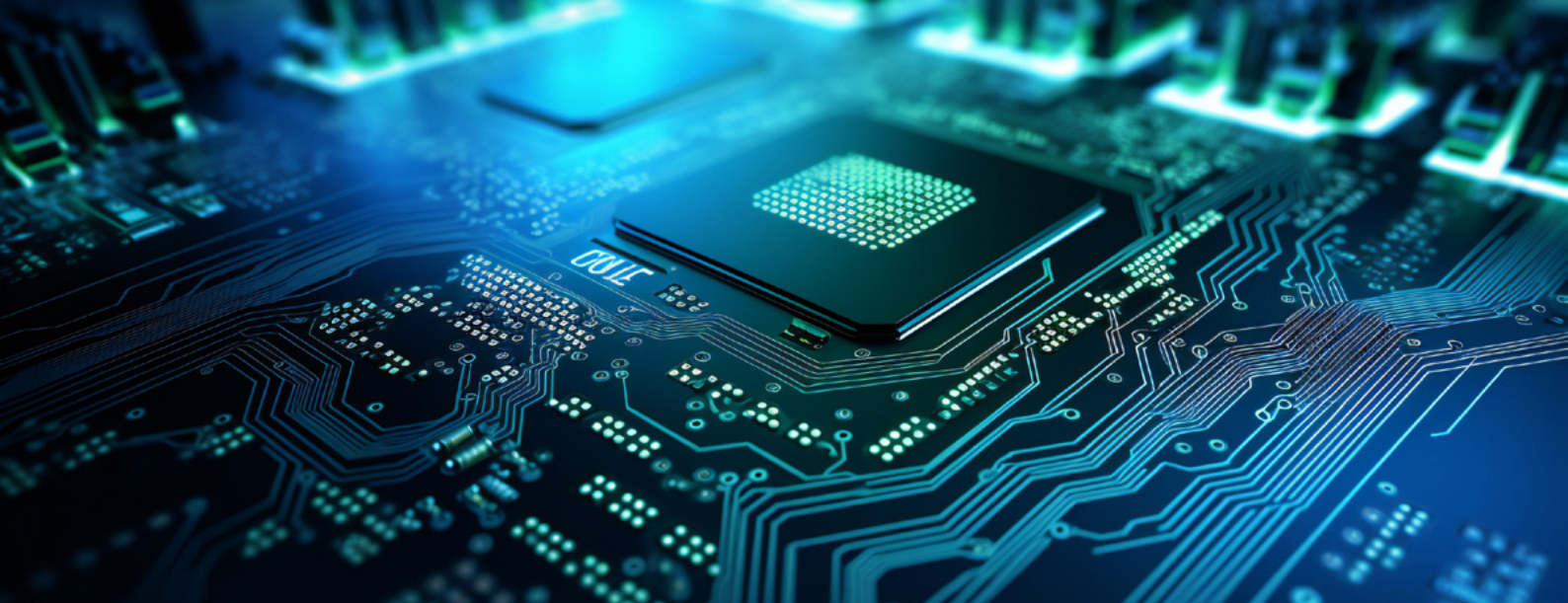


# Trust in the Age of AI-Driven Insurance

How insurers can balance automation, efficiency and fraud prevention across the customer lifecycle.





“AI is accelerating insurance workflows, from underwriting and servicing to claims. Faster decisions, however, increase risks associated with poor data and weak verification. As insurers automate more of the customer lifecycle, they need reliable ways to verify identities, bank accounts and payment instructions.”

By Jennifer Balentine  
Director of Sales, Partnerships & Account Management  
North America at LSEG Risk Intelligence

Insurers are already applying artificial intelligence (AI) to practical tasks around underwriting, claims and customer service: extracting information, enriching submissions, triaging cases, generating routine documentation and guiding employees and customers towards relevant information. These uses of AI help to reduce administrative work and free up human expertise for decisions that genuinely require judgement.

Deploying AI also increases the importance of the controls around automated workflows, however. In a manual process, an employee may spot an inconsistency simply because they have to review the information. In a highly automated process, a plausible but flawed input may be accepted and acted on at scale.

Model accuracy is only part of the issue. Insurers also need confidence in the data feeding AI and the actions it triggers. Alongside explainability, auditability and human accountability, they need to establish that the person, account and payment instruction involved in a transaction are genuine.

LSEG Risk Intelligence capabilities across identity and account verification provide trusted signals within onboarding, claims and payment workflows, helping routine cases proceed quickly while directing anomalies for additional scrutiny.

# Trust runs through the customer lifecycle

Insurance depends on a chain of trust. A customer provides personal information, an insurer assesses risk, a policy is issued and, if an insured event occurs, money may be paid to a claimant, beneficiary, provider or other recipient. Digitisation – and especially AI – makes this chain faster and potentially more convenient, but also creates opportunities for trust to be compromised.



**Onboarding:** Insurers typically need to establish that an applicant is a genuine person or business and that the information supplied is credible. Synthetic identities complicate this by combining real and fabricated information in ways designed to pass conventional checks. The risk is particularly acute in life insurance, where synthetic identities have been estimated to account for up to 85% of identity fraud.<sup>1</sup>



**Servicing:** Risk persists after onboarding. A customer may change an address, beneficiary or bank details. Fraudsters exploit these change events because a previously trusted relationship makes a new instruction appear routine. Account takeover, for example, may use a genuine customer relationship to redirect a legitimate payment.



**Claims and payouts:** Insurers need to distinguish legitimate claims from manipulated documents, impersonation or organised fraud while still meeting expectations for rapid decisions. At payout, they must also establish that the destination account is valid and controlled by the intended recipient. A valid claim paid to the wrong account is still a failed outcome. Life insurance illustrates this gap clearly: the insurer will generally have completed know-your-customer checks on the policyholder when the policy was taken out, but the eventual payout goes to a beneficiary who may never have been subject to the same checks. Before releasing funds, the insurer may therefore need to establish that the beneficiary is legitimate and that the bank account belongs to them.

These vulnerabilities are connected across the customer lifecycle. A weakness at onboarding may not surface until a claim is filed or payment released, while a legitimate relationship can be compromised later through account takeover or changed bank details. As insurance processes accelerate, trust needs to be reassessed whenever the risk changes.

<sup>1</sup> <https://www.bia.com/synthetic-identity-fraud-statistics-2026-hard-numbers-big-threats/>



## Re-establish trust when risk changes

Treating verification as a one-off onboarding event is increasingly difficult to justify. Identity and account risk change over time: accounts close or change ownership, contact details are compromised and fraudsters take over genuine accounts. A customer correctly verified two years ago may still be the same person, but the instruction received today may not be theirs.

At onboarding, identity verification helps establish that a person or business is genuine, while account and ownership checks establish whether supplied bank details are valid and connected to the intended party. In life insurance, establishing identity at the outset helps support faster, more personalised application journeys and allows advisers to concentrate on interactions where their judgement adds most value.

Trust may then need to be refreshed as the relationship changes. New bank details, beneficiary amendments or other sensitive updates should not automatically inherit the assurance attached to the original policy. Re-verification provides a fresh signal before new information becomes authoritative, while ongoing monitoring can identify changes in risk between key events.

Real-time verification becomes increasingly important as insurance processes accelerate. Document-based evidence, historic checks or cached information may be less suited to automated workflows in which decisions can be made almost immediately.

# Make the payout fast – and with confidence

Claims are the point at which the insurance promise becomes tangible, and payment is often the final interaction in the claims journey. Customers waiting for money after a loss, medical expense or other disruptive event have little tolerance for unnecessary complexity, putting pressure on insurers to make payouts faster.

A useful parallel comes from emergency relief payments. In one US deployment, tornado victims received instant payments at midnight on a Saturday, when some no longer had mailboxes to receive paper cheques. Funds could reach people precisely when conventional delivery methods had become impractical.

Faster payment, however, leaves less time to recover money sent to the wrong destination. Verification therefore has to keep pace. Before releasing funds, an insurer may need to establish that the recipient is legitimate, the account is current and the intended payee controls it. This is particularly relevant for health insurers handling large volumes of member reimbursements and other claims-related disbursements, but the same issue arises when paying policyholders, beneficiaries and providers.

LSEG's US Account Verification Solutions use direct connections to banking schemes to check consumer and business accounts, combining account status and ownership verification with additional fraud signals. Configurable decisioning allows verified payments to proceed automatically and directs uncertain or higher-risk results for further review.

Embedded in the payout workflow, these checks support faster straight-through processing for legitimate recipients while maintaining fraud controls. This becomes increasingly important as instant and near-real-time payment rails compress the recovery window.

The principle is part of a wider shift from reacting and recovering towards predicting and preventing. In property insurance, sensors and other data identify physical risks – such as leaking pipes or sparking wires – before they become losses. Applied to payments and identity, the same principle means detecting an invalid account, suspicious change or inconsistent identity signal before funds are released.

# Connect identity, account and fraud signals

Many insurers have built identity verification, account verification and fraud controls separately, often across different teams and systems. Identity verification may sit with onboarding, fraud tools with a specialist team, claims decisions in one system and payment data in another. AI initiatives may add another layer. The result can be blind spots at the hand-offs.

A more connected model allows identity, account and fraud intelligence to be reused across the customer lifecycle. The systems can remain separate, provided they can draw on consistent signals at the moments that matter.

The controls are complementary. Identity verification establishes whether a person or business is genuine. Account verification checks whether the supplied account is valid and suitable for the intended transaction. Ownership verification tests whether it belongs to the expected individual or organisation.

Behavioural fraud intelligence adds signals associated with account takeover, mule activity or synthetic identities that a simple pass-or-fail account check may miss.

LSEG's Account Insights adds behavioural fraud signals to account verification. Used alongside US Account Verification Solutions, Identity Verification provides a broader view of who is being paid and where the money is going. These capabilities integrate through real-time APIs, batch processing or a secure portal, allowing insurers to embed verification in existing workflows.

AI-assisted claims workflows also need access to these signals in real time, enabling consistent routing and escalation with an auditable record of why a transaction proceeded automatically or was referred for review. Human judgement can focus on genuinely ambiguous or high-risk decisions rather than compensate for missing data.



# Five questions every insurer should ask

As processes become faster and more automated, insurers should test where trust is established and where it needs to be refreshed:

## 1

Where do we verify identity today – only at onboarding, or also when sensitive details change and before high-risk payouts?

## 2

How do we confirm that a bank account is valid and belongs to the intended recipient immediately before money is released?

## 3

Which customer or account changes trigger re-verification, and which inherit trust from an earlier interaction?

## 4

Can fraud, claims, payment and AI systems use the same trusted identity and account signals, or do they operate with separate views of the customer?

## 5

When a verification or AI-driven result is uncertain, is there a clear, auditable route to human review?

The right controls will vary by product, claim type and risk appetite. A low-value routine reimbursement need not follow the same path as a large life insurance payout. The aim is to calibrate friction to genuine risk and remove it where it simply reflects weak data or manual processes.

# Trust becomes infrastructure

AI can make insurance workflows faster, more responsive and more efficient, but it also allows flawed inputs and fraudulent instructions to move through processes more quickly. The effectiveness of an AI-enabled process depends not only on the model, but also on the quality of its inputs, the controls around the actions it initiates and the availability of appropriate human review. Trusted identity and account data can therefore play an important role in the infrastructure and controls supporting increasingly automated insurance operations.

The practical goal is verification that is fast enough to support automation, carefully targeted to avoid unnecessary customer friction and sufficiently robust to stop questionable payments before money moves. As AI use expands, the quality of these underlying trust signals will matter as much as the sophistication of the models that use them.

## About LSEG Risk Intelligence

LSEG Risk Intelligence provides a suite of solutions to help organisations efficiently navigate risks, limit reputational damage, reduce fraud and comply with legal and regulatory obligations around the globe. From screening solutions through World-Check, to detailed background checks on any entity or individual through enhanced due diligence reports, and innovative identity verification and account verification – you can trust us to help you manage your risk, so you can operate more efficiently, more effectively and more confidently.

Learn more at [lseg.com/risk-intelligence](https://lseg.com/risk-intelligence)