5 IAM considerations and lessons learned in the insurance industry





The insurance industry’s IAM challenges

Insurance companies are prime targets for fraud and identity-based attacks. They manage vast stores of sensitive data, accounts are highly valuable, and policyholders are often vulnerable. The industry deals with a myriad of unique challenges: policy origination is often independent from online account registration, infrequent policyholder check-in delays fraud detection, and complexities like delegated access require unique verification and authentication paths, to name only a few.

Fraudsters are aware of the immense opportunity the industry represents and are exploiting it. All the more reason that customer identity access management (CIAM) is so critical across this sector and others.

Key identity and access management (IAM) considerations for the insurance industry

Addressing the industry’s specific weaknesses requires an orchestrated and risk-based approach. There are five specific vulnerabilities insurers need to be aware of and mitigate:

1. Underserved users: The verification gap

Insurers serve millions of policyholders, including older and/or lower-income individuals, who may be uncomfortable with

identity verification methods that require tech-savvy (e.g. capturing a biometric with a smartphone) or have limited footprints with traditional data sources used for identity verification (e.g. lack of credit history with the bureaus), respectively.

Unlike banks, insurers often lack physical locations, forcing them to rely on digital verification methods. To eliminate that friction, insurance providers relax verification standards. Fraudsters then exploit by successfully impersonating the real policyholders. CIAM solutions must support a multitude of equally strong verification and authentication options to mitigate fraud while still reducing friction.

2. Cross-channel fraud: When fraudsters pivot

Security efforts have traditionally focused on digital channels, overlooking call center vulnerabilities. Fraudsters exploit outdated verification methods that are easier to bypass.

Attackers move fluidly between human-assisted and digital channels. For example, weak call center authentication can allow an attacker to reset security credentials. From there, they can seamlessly transition to the insurer’s online portals – taking over policies, filing fraudulent claims, or re-routing payouts. CIAM solutions must be flexible enough to be deployed across channels and be sophisticated enough to detect fraud holistically.

3. Dormant risk: The challenge of outdated customer directories

When policyholder identity is verified once – at policy issuance – and then rarely reassessed, it can create a dangerous blind spot: dormant accounts with outdated records that attackers can readily exploit.

Without regular re-verification, outdated records and dormant accounts remain prime fraud targets. Insurance providers need a structured program to review and re-verify dormant users, otherwise they risk leaving this “side door” wide open.

4. Delegated access: A persistent vulnerability

Unlike other industries, insurers must frequently enable third-party access to policies due to medical necessity, power of attorney, or the authority of a personal representative. Fraudsters exploit delegated access by impersonating legal representatives. Identity verification and authentication paths must be specifically architected to secure delegated access.

5. Employee onboarding: The insider threat evolution

Identity fraud in the employment onboarding process is a growing trend, with more organizations encountering sophisticated attempts to bypass hiring controls.

As an example, a major United States insurer recently discovered North Korean actors using interview proxies to pass hiring checks under false identities. Enhancing CIAM and privileged access management (PAM) programs are only as good as robust identity verification at employee onboarding.

Lessons learned: Strengthening IAM to address evolving threats

The insurance industry’s identity proofing challenges require insurers to rethink IAM as a continuous, interconnected process and work with trusted partners who do the same, rather than managing an ever-growing set of static security measures.

Integrating identity verification, authentication

and directory cleanup

Many Insurers verify identities at sign-up, require authentication at login, and clean directories – but rarely unify these interconnected parts of the same lifecycle.

Consider it this way: if identity verification is like putting a new lock on the door, and authentication ensures the right people have the keys, then directory cleanup is searching within the house to ensure the bad actors aren't already hiding in your basement. Without this full lifecycle approach insurers remain exposed.

Systems must talk to each other

Siloed data environments prevent cross-department fraud detection. Unified identity data improves prevention.

To stop sophisticated fraud, insurers must link platforms and unify identity data across channels and departments. This allows fraud investigators to see cross-department patterns, react quickly, and lower investigative costs. An orchestrated, single source of truth can dramatically improve fraud prevention.

Cybercriminals move fast – Insurers must move faster

Fraud tactics evolve rapidly. AI amplifies fraud, making traditional attacks harder to detect.

As insurers develop rules-based detection to screen out a set of anomalies, fraudsters adopt different tactics. This cat-and-mouse dynamic means insurers must update their fraud defenses regularly. Relying on once-a-year tweaks is risky because criminals will always look for – and find – the next loophole.

The customer experience matters

Overly rigid CIAM controls can frustrate users. Low-risk customers with consistent behavior should pass through with minimal friction. Higher-risk interactions – like a large claim, a recent account takeover, or an unusual login location – get flagged for additional authentication or even full re-verification.

This adaptive approach depends on dynamic risk scoring and behavioral analytics, making it possible for legitimate customers to enjoy a smooth process while fraudsters hit more hurdles. A hassle-free experience also gives insurers a competitive edge by boosting customer satisfaction and loyalty.

Final thought: CIAM as a competitive advantage

Robust IAM builds trust, reduces fraud and strengthens reputation. Insurers that invest in comprehensive, flexible IAM solutions will not only reduce fraud losses but also enhance customer satisfaction and improve operational efficiency.

https://www.securitymagazine.com/articles/101426-5-iam-considerations-and-lessons-learned-in-the-insurance-industry