

SOLUTION BRIEF

Safeguarding Insurance

Identity fraud is driving claims losses

Insurance organizations are increasingly targeted by identity-based attacks that exploit weaknesses across the policy lifecycle—from onboarding to claims. Rather than breaching systems, attackers use stolen credentials, phishing, and social engineering to gain legitimate access to customer and agent accounts. This enables fraudulent policy creation, account takeover, and false claims submissions, often involving synthetic identities or manipulated personal data. Because these activities appear to originate from trusted users, they are difficult to detect using traditional security controls.

The challenge is compounded by complex ecosystems that include customers, agents, brokers, and internal employees, each introducing additional identity risk. Overprivileged access, insider threats, and weak identity verification during onboarding and claims processing further expand the attack surface. At the same time, insurers must balance fraud prevention with seamless digital experiences and regulatory compliance, limiting the use of high-friction controls.

These trends highlight the need for continuous identity threat detection—capabilities that assess every digital interaction, from account creation and profile changes to claim submissions, to determine in real time whether it is initiated by a legitimate user or a threat actor.



The impact of the identity crisis in insurance

- Increased **fraud losses**
- Operational **inefficiencies**
- **Loss** in customer trust
- Compliance **exposures**

The need to move beyond credential-only authentication

Traditional identity and access management (IAM) solutions focus on verifying whether a user is authorized to access a system or resource. However, modern attackers frequently bypass authentication controls using stolen credentials, social engineering, or AI-powered impersonation techniques.

To combat these threats, insurers must expand their identity security strategy beyond credential-only authentication and incorporate continuous identity threat detection and risk mitigation across all digital interactions.

This includes protecting all identity-related attack vectors across the organization:



Continuous, reliable identity threat detection

Detect identity risk in real time and stop fraud without disrupting legitimate users and customers.

ID Dataweb™ helps you stay ahead of identity fraud and account-related threats while maintaining a seamless digital experience for your customers, third parties, and workforce.

In turn, you can

- Prevent fraudulent claims
- Secure customer and agent portals
- Improve onboarding and verification
- Minimize insider threats

Typical use cases

Account creation (in-branch or online)

Contractor and employee onboarding

Account login

Call center fraud prevention

Credential reset

Account recovery

Age verification

High-risk interactions (i.e., claims)

Identity database hygiene

And more...

The ID Dataweb solution

The ID Dataweb platform combines:

- Adaptive identity verification
- Behavioral analytics
- Device and credential intelligence
- AI-driven risk scoring
- Expert human insights

Together, these capabilities detect and prevent identity attacks in real time while minimizing friction for legitimate users.

Unlike traditional identity verification tools that are static and siloed, ID Dataweb delivers dynamic, multi-layered risk orchestration that adapts to evolving threats.

The cloud-native platform:

- Deploys quickly
- Integrates easily with existing identity infrastructure
- Supports low-code policy customization
- Continuously evolves with the threat landscape

Safeguarding every identity attack vector

The traditional security perimeter has disappeared. Stolen credentials are widely available, and static security controls cannot keep pace with modern threats. ID Dataweb helps insurers adapt with a single platform that protects all identity attack vectors.



The ID Dataweb advantage

Quick and easy implementation

- Flexible integration options
- Pre-built templates
- OpenID Connect support

Scale and adapt easily

- Low-code platform
- Easy updates
- Robust APIs and SDKs

Tailor the solution to your needs

- Industry's broadest range of authoritative identity data sources and risk signals, giving you the flexibility to tailor identity verification and adapt to any use case you require
- Full identity lifecycle coverage



**One platform. One vendor.
Comprehensive identity protection.**

ID dataweb

ID Dataweb™ delivers identity threat detection and mitigation solutions to safeguard against identity fraud and account-related threats, all without disrupting the user experience.

[Book a demo](#)



iddataweb.com

ID Dataweb, Inc.
5875 Trinity Parkway
Suite 110
Centreville, VA 20120
United States