IDVision with iovation

Insurance

Insight Guide

Prevent Application Fraud While Growing New Accounts.

Make it easier for policyholders and harder for fraudsters.

The insurance industry is undergoing a digital transformation, with more and more insurers looking for ways to provide their policyholders with online access to quotes and policies.

These emerging digital channels allow for greater customer access and elevate the customer experience, but they also make collusion and criminal collaboration easier than an in-person agency model does. Connecting the dots between devices and conspirators can be difficult and time consuming.

With so many businesses now providing consumers with online solutions, policyholders have high expectations for secure, easy access to all their accounts, across all channels, at all times. If there is too much friction at policy application, underwriting, account login or even claim processing, customers can easily click over to a competitor offering a smoother experience. TransUnion IDVision with iovation provides insurers with solutions they need to accurately identify and authenticate good customers, detect and prevent fraud, and provide an outstanding customer experience.

Our Experience

Types of insurance companies that use TransUnion:

- Property and Casualty
- Insurance Brokers
- Life Insurance & Annuities
- Group Insurance
- Wealth & Reinsurance
- Insurance Aggregators
- Long-term Care

Coverage provided by TransUnion over the past 12 months	**Global insurance customers**	**All customers**
Number of transactions protected	82.3 million	11.9 billion
Number of risky transactions stopped	7.9 million	631 million
Number of reputation reports submitted by analysts	249,530	20.8 million
Percent of devices previously seen by TransUnion	66%	73%

Create an Outstanding Experience and Shut Down Fraud

The need for customer authentication and fraud prevention solutions for insurance companies, globally.

Since 2005, the U.S.[1] and European[2] insurance industries have each written more than $1 trillion and €1 trillion respectively in premiums each year. These premium volumes are only growing, and serve as irresistible targets for cyberciminals. Conservative calculations estimate that fraud steals $80 billion per year, globally, across all lines of insurance.[3]

[1] Insurance Handbook, Insurance Information Institute, 2019.

[2] European Insurance Industry database, Insurance Europe, 2019.

[3] By the numbers: fraud statistics, Coalition Against Insurance Fraud.

[4] Insurers: Strike The Right Balance Between Fighting Fraud And CX (September 2018)

Fraud prevention methods are critical, yet they can be burdensome on good customers. [4]

Customers expect a consistent experience across all of their devices.

Skilled fraudsters will look for workarounds to every fraud-fighting technique you try. Combating this threat requires resources that will evolve with new trends and fraud vectors: smart tools, machine learning and crowd-sourced intelligence. Of course, it's critical to implement friction-right solutions for establishing identities, authenticating customers and preventing digital fraud in order to keep policyholders both happy and protected.

Policyholders Expect a Friction-Right Experience

Today's insurance consumers want secure, easy access to services across all channels and at all times, from policy application to account login to claim submissions. Too much friction at any point paves the way for your customers to easily click over to a competitor that offers a smoother digital experience. Instead, give your policyholders secure protection while reducing friction and keeping fraudsters out.

Your challenges:

- Stopping fraud at the application stage before a policy is incepted
- Improving the login experience without sacrificing security
- Authenticating policyholders on any device while stopping account takeover (ATO)
- Accurately verifying consumer-provided information to weed out stolen or synthetic identities
- Enhancing usability, even as prices and margins decline

The solution: Focus on your customer's device

Every purchase. Every engagement with your brand. Every attempt at fraud. They all rely on a web-enabled device, and TransUnion's powerful device recognition technology can confirm the reputation of over seven billion devices.

How TransUnion Stops Insurance Fraud

TransUnion's fraud prevention solutions use flexible business rules and advanced machine learning algorithms to detect devices with risky attributes and behavior. Our patented technology identifies and helps to quickly shut down coordinated fraud rings by recognizing connections between accounts and devices, regardless of business or industry. This technology is further supported by our global network of fraud and security analysts, who submit millions of device reputation reports that detail the type of fraud or abuse a device is confirmed to have committed, such as:

- Policy and inception fraud
- Claims fraud
- Payments fraud
- Application fraud
- Contact center fraud
- Synthetic identity

Your Challenges	Our Solutions
You're struggling to prevent quote, application and/or policy fraud. Criminals use tactics such as address fronting, misrepresentation and synthetic identities to defraud insurance companies and policyholders. Fraud rings and ghost broking are particularly difficult to detect and shut down.	Through a combination of device reputation and precise identity verification, you can identify good customers from fraudsters, even if it's the first time you've seen them. Our global network of fraud analysts report when fraudulent activity has been confirmed, and when the same device or associated devices reappear in our network, we report its history of fraud.
You have no shared fraud intelligence source. A study from Coalition Against Insurance Fraud found that 84% of insurance organizations say the fraud cases they investigate involve more than one industry.[3] How can you tap into that intel to stop fraud sooner?	Our vast network of global fraud professionals use our unique device reputation database to share confirmed fraud and abuse reports with each other. With over 7 billion devices and 83 million incidents reported, this comprehensive database stops fraudsters before they can move from business to business.
Contact center fraud is increasing. Fraudsters gather data about policyholders, combine high-pressure tactics with spoofing technology to socially engineer your agents, and take over user accounts.	Multifactor authentication methods strengthen your online and offline security, while transparent two factor authentication and One Time Passcode (OTP) solutions give your call center agents confidence that your customers are who they say they are.
Your Special Investigations Unit (SIU) needs more tools. Fraudulent claims are costly to your business and cause friction for policyholders waiting for a claim settlement. Your SIU doesn't have the resources they need to build strong cases.	We let you know when disparate devices are used to access the same account or sets of accounts. Connecting the dots between devices and conspirators result in stronger legal cases, less pay-and-chase, and a more focused SIU.

How to Provide Fast and Secure Access

The flood of breached credentials over the last decade has made it easier than ever for criminals to take over good customers' accounts. While insurers work to strengthen their authentication and identity proofing solutions, customers expect the best possible online experience, beginning at login.

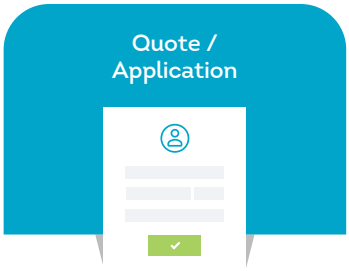
Your Challenges	Our Solutions
ATO is rising. Your policyholders trust you to provide the coverage that they need, but ATO can put them at risk of losing their coverage without realizing it. Adding more layers of authentication decreases the risk of ATO, but can also harm the quality of the user experience.	Protect your policyholders from ATO with device-based authentication. This transparent layer of authentication recognizes returning devices in real-time, providing an invisible layer of account protection and reducing friction.
As insurers move to providing services primarily through digital channels, customers are finding themselves being treated the same as fraudsters. If every visitor is subject to the same authentication prompts, you're either letting too much fraud in or creating too much friction for good customers.	Implement fraud prevention and authentication solutions that dynamically adjust based on detected risk. With device recognition in place, policyholders can log in and access their accounts without needing a password. If any unusual geolocations, known risky devices, or risky device anomalies appear, apply mobile multifactor step-up authentication.
Your current tools miss risk signals. Does your policyholder just want to view their policy or change their contact information? What if they want to make a mid-term adjustment or submit a claim? Each action represents a different level of risk, but most authentication solutions treat all actions the same.	Dynamic authentication combines interactive, mobile multifactor authentication with transparent, easy-to-use device recognition to ensure the appropriate friction-right method is being deployed at the right time. The built-in intelligence of these solutions acts as a decisioning engine to layer additional protection as needed.
Authorization is difficult to manage and track. Regulatory standards such as the GDPR and PSD2 not only demand strong authentication, they also require authorization as an explicit and separate function.	Build authorization capabilities within your native app that allow your customers to authorize specific requests in real time, such as "Approve new claim submission?" Or even, "Do you grant permission for this mid-term adjustment?" Automate authorization, improve validation and gain audit-ability.

Protect and Enhance the Entire Policyholder Journey

Personal Identity Solutions with TransUnion

Digital Identity Solutions

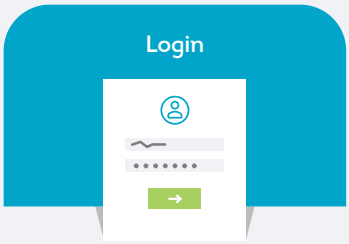
1 Quote / Application



- Expedite Applications and Reduce Rate Evasion with Verified Pre-fill
- Prevent Misrepresentation
- Verify Emails and Phone Numbers
- Avoid Bad Debt from Consumers with a Higher Likelihood of Payment Issues
- Streamline the Application Process for Low Risk Customers and Focus Efforts on Unverifiable Identities
- Identify and Stop Applications Submitted by Ghost Brokers

- Stop Application Fraud
- Prevent Ghost Brokers
- Uncover Synthetic identities
- Reduce Abandonment
- Expose Underwriting Fraud

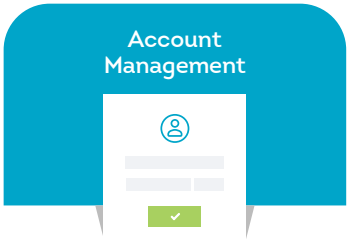
2 Login



- Identity Verification (OTP, KBA)
- Prevent Account Takeover

- Stop Account Takeover
- Authenticate Customers
- Reduce Login Friction
- Provide Multi-factor Authentication
- Authorize Devices

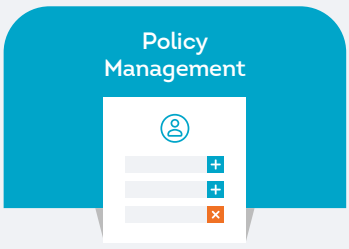
3 Account Management



- Email and Phone Number Verification
- Confirm the Identity of the Person Accessing the Policy is Authorized to Do So

- Authenticate Customers

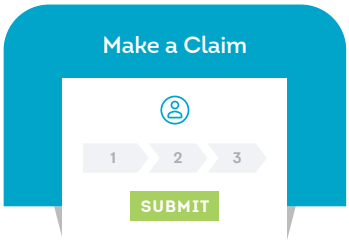
4 Policy Management



- Identity Verification Dissipates Underwriting Exposure
- Reduce Risk of Premium Leakage and Misrepresentation

- Prevent ATO
- Add a Line of Coverage

5 Make a Claim



- Claims Fraud
- Reduce Customer Friction
- Arm SIU Team with Data to Expedite Investigations

Fraud Prevention and Authentication Solutions

To remain competitive, insurance carriers must balance experience with security. That's what our products are built to do. Learn more about the solutions by visiting iovation.com.

Establish Identity

Establish identity with greater confidence by verifying against a broad set of personal and digital data.

Authenticate Consumers

Secure each point of the customer journey with authentication methods tailored to the transaction risk level.

Prevent Fraud

Proactively identify fraudulent transactions and behaviors of any given device in real time.

Get in Touch

Find out more about our authentication and fraud prevention solutions. Contact us for a demo or visit iovation.com

TransUnion
Formerly iovation

Portland Office
555 SW Oak Street, Suite #300
Portland, OR 97204 USA
PH +1 (503) 224 6010
EMAIL info@iovation.com

United Kingdom
PH +44 (0) 800 058 8731
EMAIL uk@iovation.com

iovation.com