# GROW NEW INSURANCE ACCOUNTS. PREVENT APPLICATION FRAUD. DETECT FALSE CLAIMS.

In the Insurance Industry,
User Experience is Paramount

New standards have emerged for easy, instant access to sites and mobile apps. Yet this experience needs to be weighed against the realities of rising fraud, and new regulatory mandates for stronger customer authentication. iovation provides insurers the solutions that balance the competing demands of catching fraud, authenticating good customers and providing an outstanding user experience.
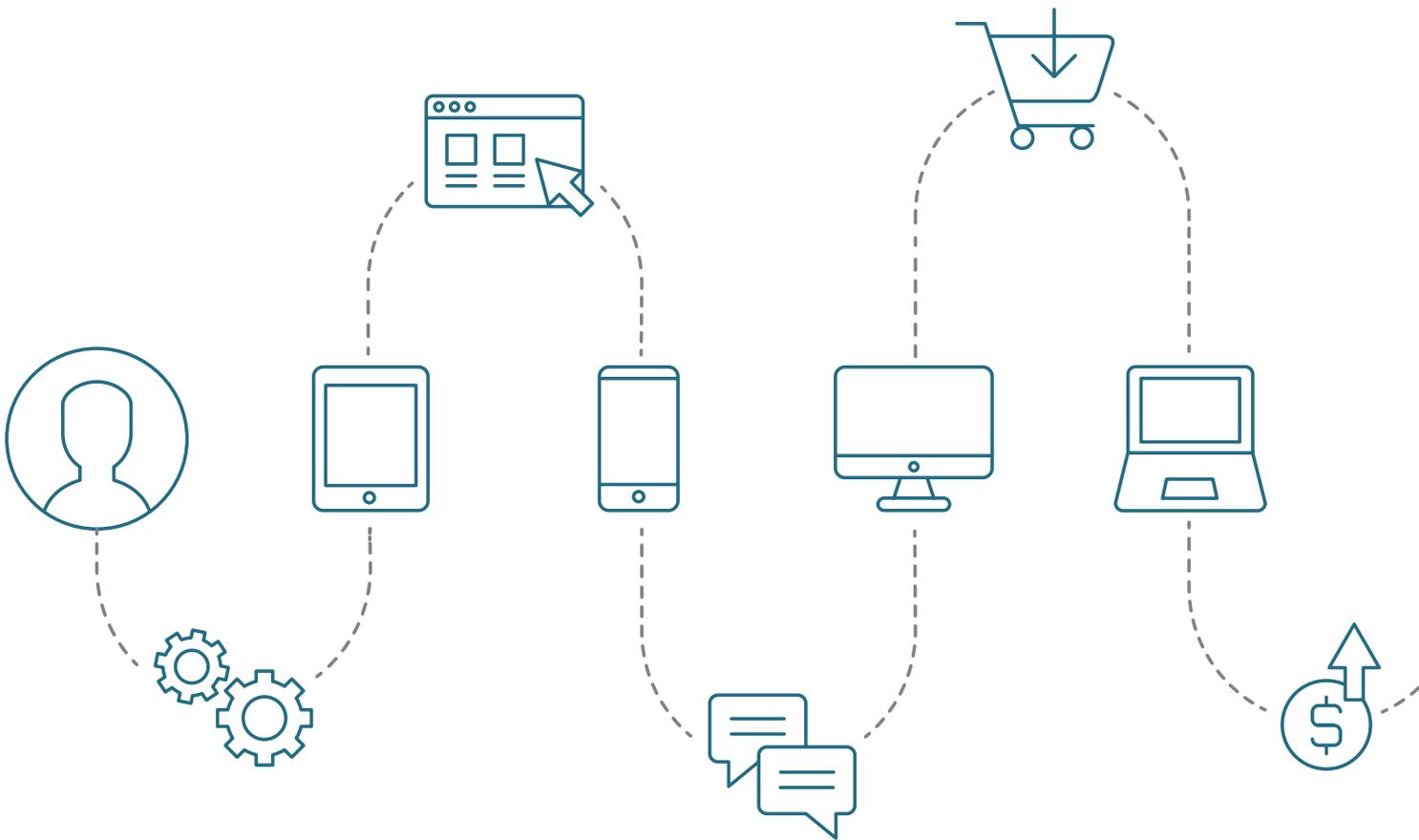
Our Experience

Preventing fraud at point of quote, policy inception, claims and beyond

Coverage provided by iovation OVER THE PAST 12 MONTHS	Insurance customers	All customers
NUMBER OF TRANSACTIONS PROTECTED	63 million	8.2 billion
NUMBER OF RISKY TRANSACTIONS STOPPED	4.8 million	514 million
NUMBER OF REPUTATION REPORTS SUBMITTED BY ANALYSTS	305,000	13 million
PERCENT OF DEVICES PREVIOUSLY SEEN BY IOVATION	70%	74%

Types of insurance companies that use iovation:

- Property and casualty
- Life insurance and annuity*

  Both individual and group

- Wealth and reinsurance*
- Healthcare

- Long-term care*
- Insurance brokers

Create an Outstanding Experience and Shut Down Fraud

Customer authentication and fraud prevention solutions for U.S. insurers

In each year since 2011, the U.S. insurance industry has written more than $1 trillion in premiums. This enormous trove is an irresistible target for cybercriminals. [1]

Do you feel like fraudsters find workarounds to every fraud-fighting technique you try? Then you need resources that will evolve with new trends and fraud vectors: smart tools, machine learning and crowd-sourced intelligence. And as always, this needs to balance with what your policyholders want.

And what do your policyholders want?

They want secure, easy access to services across all channels at all times. Policy application. Account login. Claim submission. Too much friction at any point and customers could click over to a competitor offering a smoother experience. Your team's job is to make it easier for policyholders and harder for fraudsters.
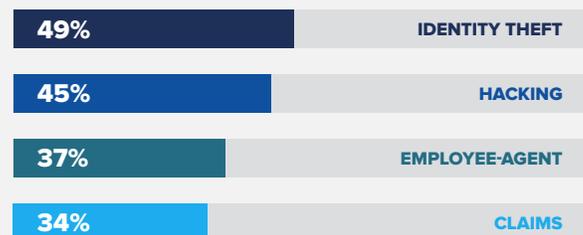
Your challenges:

- Stopping fraud at the application before a policy is incepted
- Improving the login experience without sacrificing security
- Authenticating policyholders on any device while stopping account takeover (ATO)
- Fighting fraud and abuse in ever-changing vectors
- Enhancing usability, even as prices and margins decline

Fraud is a persistent problem, costing the industry $80 billion per year. [2]

60%
OF INSURERS AGREE FRAUD IS INCREASING

57%
PREDICT INCREASES IN PERSONAL PROPERTY FRAUD

58%
PREDICT INCREASES IN AUTOMOTIVE FRAUD

Key areas of fraud concern for insurers [3]

49%	IDENTITY THEFT
45%	HACKING
37%	EMPLOYEE-AGENT
34%	CLAIMS

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.
iovation knows the reputations of over five billion devices.

[1] Insurance Handbook, Insurance Information Institute, 2016.
[2] By the numbers: fraud statistics, Coalition Against Insurance Fraud.
[3] Ibid.

How iovation Stops Insurance Fraud

iovation's fraud prevention solution uses flexible business rules and advanced machine learning algorithms to stop devices with risky attributes and behavior

Patented technology allows us to spot and stop coordinated fraud rings by determining connected devices and accounts that span businesses and industries without the need of directly identifying personal information. Our comprehensive network of cybercrime fighting professionals submits 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

- Call center fraud
- Synthetic identities

Your challenges

Quote, point of sale and policy fraud
Criminals use tactics such as address fronting, misrepresentation and synthetic identities to defraud. Fraud rings are particularly difficult to detect and shut down.

You have no shared fraud intelligence source
A study from Coalition Against Insurance Fraud found that 84% of insurance organizations say fraud cases they investigate involve more than one industry. [1] How can you tap into that intel to stop fraud sooner?

Call center fraud is increasing
Fraudsters gather data about policyholders and then combine high-pressure tactics with spoofing technology to socially engineer your agents to take over policyholders' accounts.

Your Special Investigations Unit (SIU) can't keep up
Fraudulent claims are costly to your business, but your SIU doesn't have the time to track down every case.

Our solutions

Our global network of fraud analysts collaborate and fight these types of fraud by reporting when fraudulent activity has been confirmed. When the same device, or even associated devices, reappear in our network, we report its past history of fraud. In addition, our ability to identify high transaction velocities for devices or IP address is effective in fighting these types of fraud.

Over 4,000 global fraud professionals use our unique device reputation database to share confirmed fraud and abuse reports with each other. With over 5 billion devices and 55 million incidents reported, this comprehensive database stops fraudsters as they move from business to business.

Multifactor authentication methods in LaunchKey strengthen security both online and offline, without slowing down service. Call center agents are empowered to quickly validate callers' devices before providing service.

To win against fraud rings, your SIU needs to detect and connect a myriad of dots. We let you know when disparate devices are used to access the same account, sets of accounts or when the same device accesses many different accounts. Connecting the dots between devices and conspirators. Resulting in stronger legal cases, less pay-and-chase and a more focused SIU.

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

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 solutions, customers expect the best possible online experience, beginning at login.

Your challenges

ATO is rising
The risk of ATO drops as you introduce more authentication factors, but the quality of the user's experience drops as well.

Stolen credentials are everywhere
Over 9 billion credentials, account details and passwords have appeared on the dark web in the last 10 years. Password systems have been rendered obsolete.

Customers are treated like criminals
Every visitor sees the same authentication challenges. As a result, good customers receive the same greeting as potential threats. Risk signals — such as sessions coming through a proxy, or mismatches between the device's reported and observed geolocation — are ignored.

Your current tools miss risk signals
Does your policyholder just want to view their policy? What if they want to make a mid-term adjustment or submit a claim? And if they want to change their contact information? Each action represents a different level of risk, but most authentication solutions treat them all the same.

Authorization is difficult to manage and track
New regulatory standards such as the GDPR and PSD2 not only demand strong authentication, they also require authorization as an explicit and separate function. How do you go from "Is this the right person?" to, "Is this person authorized for this request?"

Our solutions

Users register their devices with ClearKey, which recognizes them in future visits and provides another authentication factor. This additional assurance is invisible and frictionless to customers.

You can no longer rely on single-factor authentication. With LaunchKey you can layer in multiple authentication options, from transparent and frictionless, to interactive and fully integrated. It doesn't require users' private information or centralized credential storage.

ClearKey adds an essential dimension of context and risk to the authentication process. It delivers insight on access requests, step-up authentication processes and device histories. FraudForce reveals even more nuance via the subtle aspects of reputation and risk. The authentication challenge adjusts with the detected threat.

Combine LaunchKey's interactive, mobile multifactor authentication with ClearKey's transparent, easy-to-use device recognition for dynamic authentication. The result: The right method at the right time, with the right balance of friction and user experience. The built-in intelligence of this solution acts as a decisioning engine that drives step-up activity as needed.

LaunchKey provides built-in authorization, allowing your customers to respond in real time to specific requests such as "Approve new claim submission?" Or even, "Do you grant permission for this mid-term adjustment?" Allowing you to automate authorization, improve validation and gain audit-ability.

Rethink Authentication and Improve Access

Armed with billions of user credentials and plenty of patience, fraudsters will take over every account possible. Legacy authentication systems reliant on passwords, and text-based, one-time passwords alone don't stand a chance. It's time to move on.

Overcoming modern fraud and authentication problems — while improving user experience — calls for a new way of thinking. LaunchKey anticipates the challenge with:

- **Decentralized architecture** - Remove the target, and hackers have no way to steal and reuse identity information at scale. We separate the authentication process from the application. This keeps encrypted credentials — and risk — dispersed on each end-user's device.

- **Updatable platform** - New authentication methods will enter the mainstream soon. Users will be able to authenticate with their voice, heartbeat, iris or more. We designed LaunchKey as a mobile multifactor authentication platform that will keep up with new methods.

- **Omnichannel flexibility** - Today, authentication varies by the channel. In your web portal, customers enter their username and password, and possibly a one-time password. When contacting your call center, they have to answer knowledge-based authentication questions. In person, they provide their driver's license, and perhaps a PIN. Imagine a time where every channel uses the same simple authentication method: The user's device.

To remain competitive, insurers must balance experience with security. That's what our products do. Learn more about the solutions mentioned in this industry brief by visiting **iovation.com**.

ClearKey

Provide your customers with a transparent authentication method that stops ATO but doesn't slow them down.

LaunchKey

Increase security, kill passwords and provide your customers with mobile multifactor authentication.

FraudForce

Establish fraud risk based on suspicious behavior and risky data. Uncover more fraud through device associations.

SureScore

Predict the outcome of any given online transaction, even if you have no history with the customer involved.

ABOUT IOVATION

iovation, a TransUnion company, was founded with a simple guiding mission: to make the Internet a safer place for people to conduct business. Since 2004, the company has been delivering against that goal, helping brands protect and engage their customers, and keeping them secure in the complex digital world. Armed with the world's largest and most precise database of reputation insights and cryptographically secure multi-factor authentication methods, iovation safeguards tens of millions of digital transactions each day.

iovation.com

Global Headquarters

iovation, a TransUnion company
555 SW Oak Street, Suite #300
Portland, OR 97204 USA

PH   +1 (503) 224 - 6010
FX   +1 (503) 224 - 1581
EMAIL   info@iovation.com

United Kingdom

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