

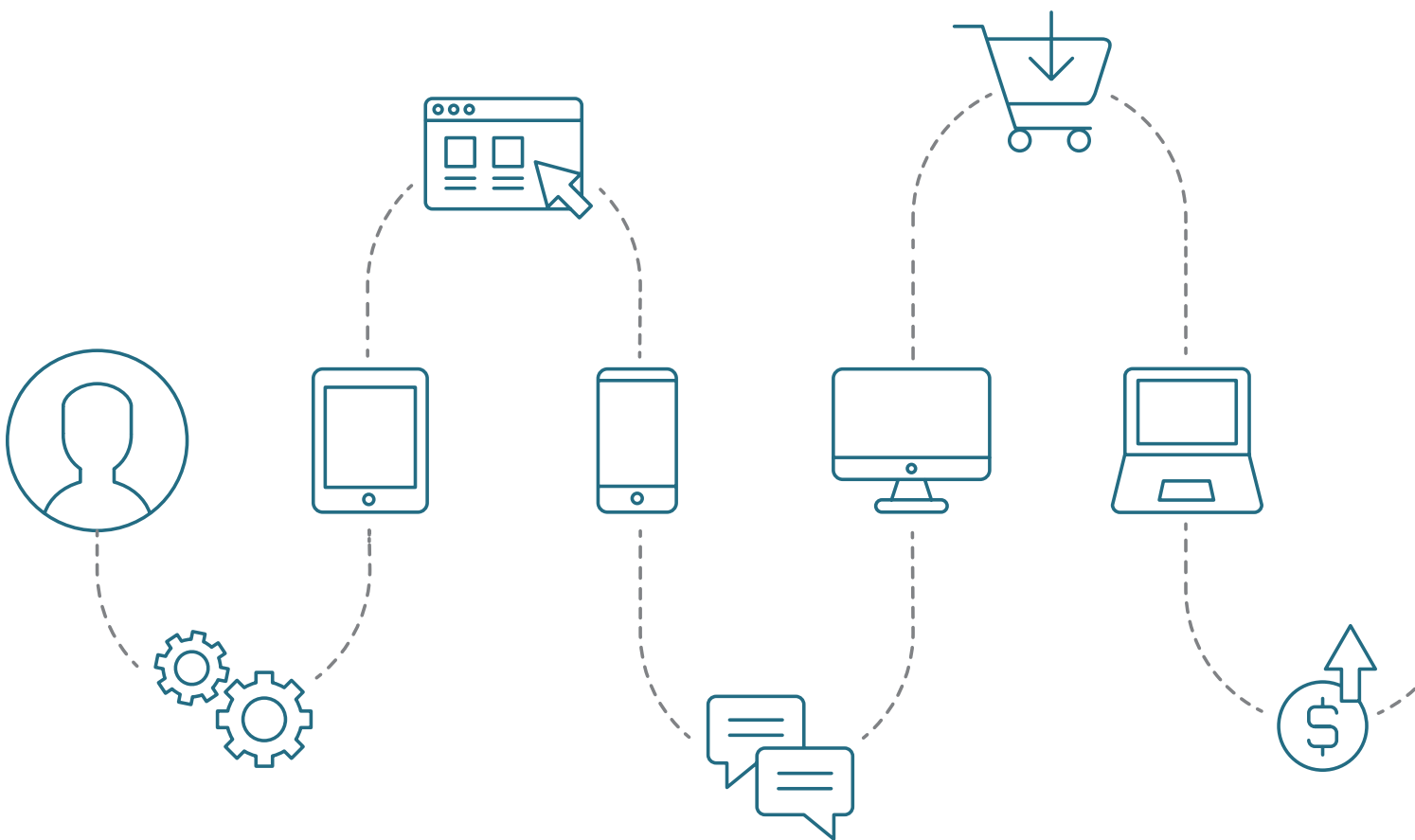
US INSURANCE

REDUCE FRICTION FOR POLICYHOLDERS AND CLOSE THE DOOR ON FRAUDSTERS







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 solutions that balance the competing demands of catching fraud, authenticating good customers, and providing an outstanding user experience.



Our Experience

Coverage Provided by iovation OVER THE PAST 12 MONTHS	Insurers	Total
 TOTAL NUMBER OF TRANSACTIONS PROTECTED	63M	8.2B
 NUMBER OF RISKY TRANSACTIONS STOPPED	4.8M	514M
 REPUTATION REPORTS SUBMITTED BY ANALYSTS	305K	13M
 DEVICES PREVIOUSLY SEEN BY IOVATION	70%	74%

Types of Insurance companies that use iovation

- Property & Casualty
- Life Insurance & Annuity*
- Wealth & Reinsurance*
- Healthcare
- Long-Term Care*
- Insurance Brokers

*Both Individual and Group

Create An Outstanding Experience and Shut Down Fraud

Customer authentication and fraud prevention solutions for US insurers

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

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.

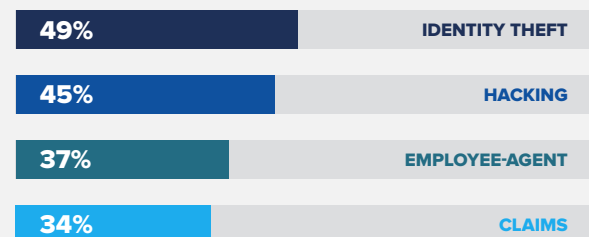
Your challenges:

- Improving login experience without sacrificing security
- Authenticating policyholders on any device while stopping account takeover
- 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



Key areas of fraud concern for insurers include.³



The Solution: Focus On Your Customer's Device

Every transaction. Every engagement with your brand. Every attempt at fraud. They all rely on an Internet-enabled device. iovation knows the reputations of over 5B 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 need of directly identifying personal information. Our comprehensive network of cybercrime fighting professionals submit device reputation reports that detail the type of fraud or abuse a device is confirmed to have committed such as:

- Policy Fraud
- Payments Fraud
- Call Center Fraud
- Claims Fraud
- Application Fraud
- Identity Theft

Your Problem

Policy Quote, Application and Inception 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 organisations say fraud cases they investigate involve more than one industry. 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 extremely costly to your business, but your SIU doesn't have the time to track down every case.

Our Solution

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 5B devices and 50M 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. Empowering call center agents 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 or 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.

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 Problem

Account Takeover 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- and knowledge-based authentication 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 Solution

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 invisible 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 acts as a decisioning engine that drives intelligent step-up activity.

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 breached over the past decade, fraudsters will take over every account possible. Legacy authentication systems reliant on passwords, knowledge based authentication (KBA) and text-based one time passwords don't stand a chance. It's time to move on.

Overcoming modern fraud and authentication problems – while improving customers' shopping experience – calls for a completely new way of thinking and design. LaunchKey anticipates the challenge with:

- **Decentralized architecture:** Remove the target, and hackers have no way of stealing and reusing payment and identity information at scale. We separate the authentication process from the application, reducing your liability and keeping encrypted credentials – and risk – dispersed on each end-user's device.
- **Modular construction:** New biometric 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 would readily adapt to new methods with modification to its SDK.
- **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 KBA 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 www.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 protects online businesses and their end users against fraud and abuse, and identifies trustworthy customers through a combination of advanced device identification, shared device reputation, customer authentication and real-time risk evaluation.

More than 4,000 fraud managers representing global retail, financial services, insurance, social network, gaming and other companies leverage iovation's database of more than 5 billion Internet devices and the relationships between them to determine the level of risk associated with online transactions.

The company's device reputation database is the world's largest, used to protect 25 million daily transactions and stop an average of 300,000 fraudulent activities every day.

The world's foremost fraud experts share intelligence, cybercrime tips and online fraud prevention techniques in iovation's Fraud Force Community, an exclusive virtual crime-fighting network.

Global Headquarters

iovation Inc
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

www.iovation.com

