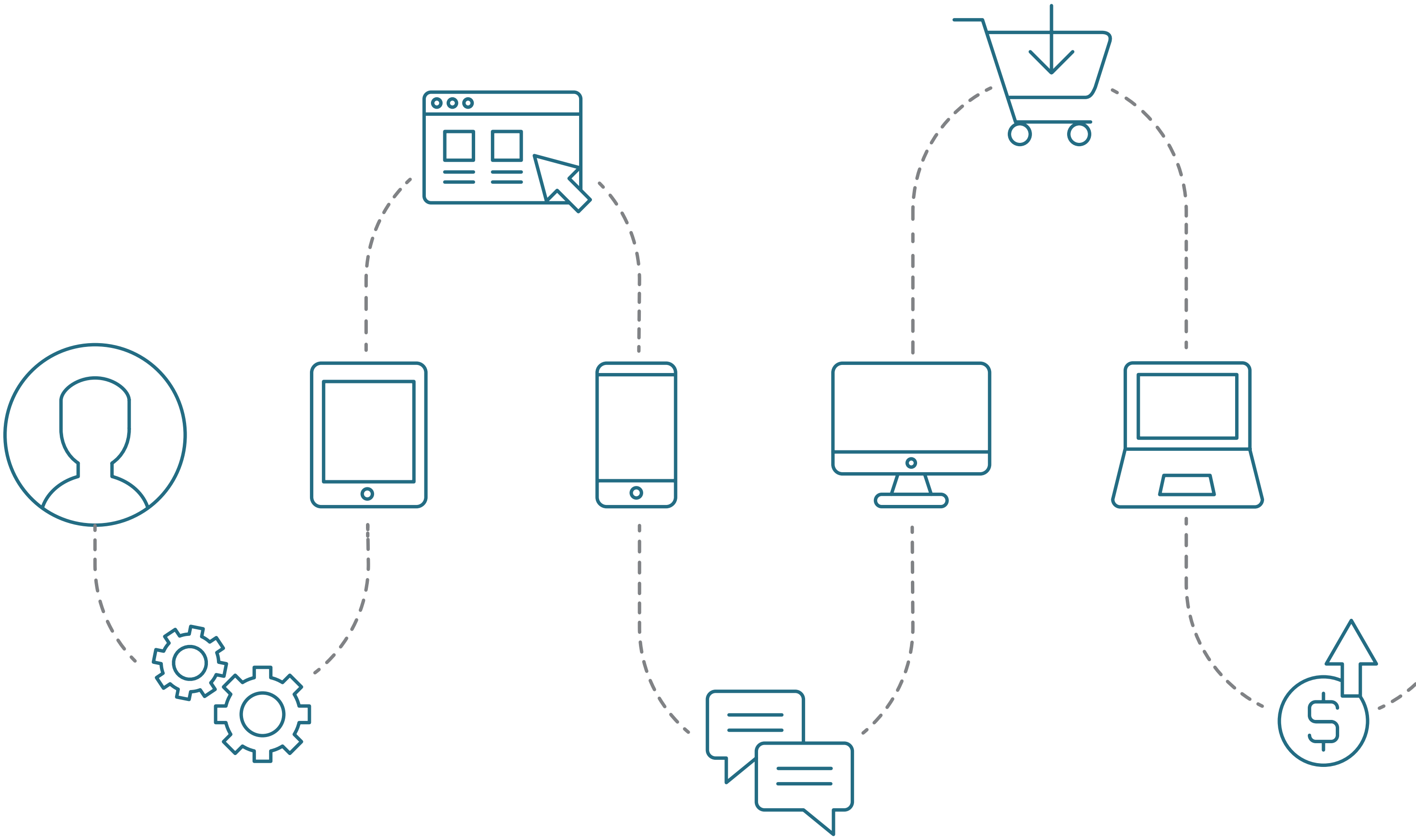
INDUSTRY BRIEF

EU INSURANCE

PREVENT INSURANCE FRAUD WHILE IMPROVING CUSTOMER EXPERIENCE

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 carriers solutions that balance the competing demands of catching fraud, authenticating good customers, and providing 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**	**All Customers**
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
- Insurance Brokers
- Insurance Aggregators

Stop Claims Fraud, Ghost Broking, and Identity Theft – Minus the Friction

Customer authentication and fraud prevention solutions for insurance

In each year since 2005, the European insurance industry has written more than €1 trillion total direct 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 in their journey and they can easily 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:

- Creating a frictionless online experience for policyholders while preventing fraud
- Blocking fraudulent online applications at submission
- Fighting fraud and abuse in ever-changing vectors
- Enhancing usability, even as prices and margins decline

Fraud represents up to 10% of all claims expenditure in Europe.[2]

Types of fraud most likely to go undetected:[3]

46%	39%	39%	18%
STAGED ACCIDENTS	INTERNAL FRAUD	APPLICATION FRAUD	GHOST BROKING

Only **22% of carriers** feel they're successful in fighting fraud before the claim.[4]

Insurers' biggest challenges in effectively responding to fraud:[3]

50% **Internal data quality**

43% **Undetected fraud**

29% **Overcoming internal silo mentality**

25% **Inadequate access to external data**

18% **Inability to collaborate with external parties**

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, and iovation knows the reputation of over 5B devices.

[1] European insurance industry database, Insurance Europe, 2018.
[2] The Impact of Insurance Fraud, Insurance Europe, 2013.
[3] Insurance Fraud Survey, Insurance Nexus, 2016.
[4] Insurance Fraud under the Microscope: Survey Results, Insurance Nexus, 2016.

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 behaviour.

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 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, claims fraud, application fraud, payments fraud, call centre fraud, identity theft, synthetic identities, and ghost broking**.

Your Problem	Our Solution
Policy, Quote, Application and Inception Fraud Criminals employ a variety of attack methods, such as: address fronting, misrepresentation and ghost broking to defraud. Ghost broking rings are particularly difficult to detect and shut down.	Our unparalleled ability to track and understand the reputation of a device over time, across different accounts and geographies, allows you to easily spot quote manipulation, follow the abuser into policy application, and uncover otherwise invisible associations. In tandem, we monitor for risk signals such as high transaction velocities for devices or IP address that indicate these types of fraud.
You Have No Shared Fraud Intelligence Source A survey[3] of over 200 european insurance professionals found that 50% of insurers identify internal data quality as the greatest challenge for effectively responding to fraud. How can you tap into better intel to stop fraud sooner?	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 across businesses, industries and countries.
Call Centre Fraud is Increasing Fraudsters gather data about policyholders and then combine high-pressure tactics with spoofing technology to socially engineer your agents and take over policyholders' accounts or apply for new policies.	Multifactor authentication methods in LaunchKey strengthen security both online and offline, without slowing down service. Call centre agents can quickly validate callers' devices before providing service.
Your Special Investigations Unit (SIU) is Overwhelmed Fraudulent claims are extremely costly to your business, but your SIU doesn't have the time or resources to track down every case.	To win against fraud rings, your SIU needs to detect and connect a myriad of dots. We let you know when disparate devices access the same 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 bad actors to take over good customers' accounts. While carriers race to strengthen their authentication solutions, customers expect the best possible online experience, beginning at login.

Your Problem	Our Solution
Account Takeover is Rising The risk of ATO drops as you introduce more authentication factors, but the quality of the user's experience suffers.	Users register their devices with ClearKey, which recognises them in future visits and provides an additional authentication factor. This additional assurance is invisible and frictionless to customers.
Stolen Credentials Are Everywhere Nearly 9 billion credentials, account details and passwords have been dumped on the dark web in the last 10 years. Password- and knowledge-based authentication systems have been rendered obsolete.	You can no longer rely on single- or even two-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 centralised credential storage.
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.	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.
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.	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.
Authorisation is Difficult to Manage and Track New regulatory standards such as the GDPR and PSD2 not only demand strong authentication, they also require authorisation as an explicit and separate function. How do you go from "Is this the right person?" to "Is this person authorised for this request?"	LaunchKey provides built-in authorisation, 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 authorisation, improve validation and gain audit-ability.

Rethink Authentication and Improve Access

Armed with billions of user credentials breached over the past decade, and plenty of incentivised patience, fraudsters will compromise not just singular accounts, but whole databases. Legacy authentication systems reliant on passwords, 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 policyholders' service experience – calls for a completely new way of thinking. LaunchKey anticipates the challenge with:

- **Decentralised 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 reduces your liability and keeps 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 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 centre, they have to answer KBA questions. In person, they provide their identification, and perhaps a PIN. Imagine a time where every channel uses the same simple authentication method: the user's device.

To remain competitive, carriers must balance experience with security. That's what our products are built to 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 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

iovation®

©iovation Inc.