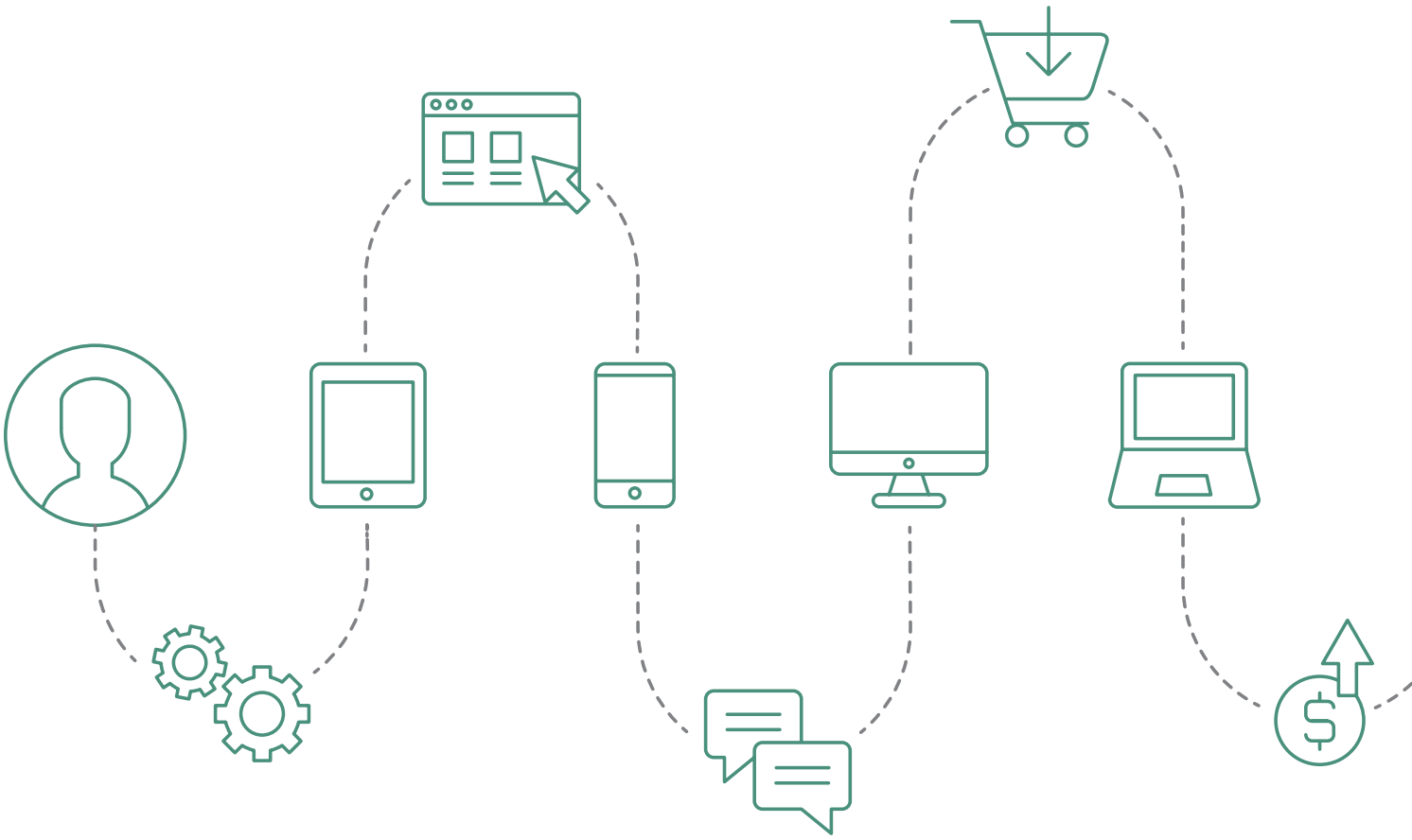
ONLINE BANKING

DEVELOP NEW BUSINESS. DENY ACCOUNT TAKEOVER.

Reduce Fraud Losses.
Exceed Customer Expectations.

Customer experience is critical in online banking. As part of the customer's overall brand experience, new standards have emerged for frictionless, 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 banks solutions that balance the competing demands of catching fraud, authenticating good customers, and providing outstanding user experience.



Our Experience

Preventing Fraud and Protecting Financial Services

Transactions Protected by iovation OVER THE PAST 12 MONTHS	Financial Services	Total
TOTAL NUMBER OF TRANSACTIONS PROTECTED	4.8B	8.2B
NUMBER OF RISKY TRANSACTIONS STOPPED	31M	514M
REPUTATION REPORTS SUBMITTED BY ANALYSTS	1.4M	13M
DEVICES PREVIOUSLY SEEN BY IOVATION	76%	74%

Types of financial institutions that protect their online business with iovation

- Credit Unions
- Retail Banks
- Online Banks
- Commercial Banks
- Investment Banks

Create An Outstanding Experience and Shut Down Fraud

Customer authentication and fraud prevention solutions for online banking

Massive digital disruption has redefined the financial services industry. Over 5,000 FinTechs have appeared on the market, increasing competition. Regulations such as PSD2 and GDPR have elevated standards for security and privacy. Customers expect easy, omnichannel access and instant service. Banks have only seconds to process transactions & applications. And only milliseconds to stop cybercriminals.

The race with customers' expectations and against criminals' tactics

Banks' priorities for digital transformation:[1]

- Customer-centricity (for 78% of banks)
- Omnichannel digital experience (74%)
- Maximizing mobile and social technologies (68%)

> **FINANCIAL SERVICE PROVIDERS NEED TO DESIGN THEIR MOBILE BANKING SERVICES WITH THE DEVICE IN MIND, FOCUSING ON OPPORTUNITIES TO MINIMIZE THE EFFORT REQUIRED TO USE THEM.[6]**
>
> - Nielsen

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 new fraud vectors: smart tools, machine learning, and crowd-sourced intelligence. And as always, this needs to balance with what your customers want.

And what do your customers want?

They want secure, easy access to services across all channels at all times. Account creation. Login. Payment processing. 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 customers and harder for fraudsters.

Your challenges:

- Authenticate customers while stopping account takeover
- Fight fraud and abuse across ever-changing vectors
- Improve the login experience without sacrificing security
- Encourage new accounts while stopping fraud
- Mitigate different risks at each part of the customer journey

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 reputation of over 5B devices.

[1] Innovation in Retail Banking, Efma and Infosys Finacle, 2016
[2] Identity Fraud Hits Record High with 15.4 Million U.S. Victims in 2016, Up 16 Percent, Javelin Strategy & Research, 2018
[3] Ibid.
[4] Identity Fraud Hits All Time High With 16.7 Million U.S. Victims in 2017, Javelin Strategy & Research, 2018
[5] Digital Lending Fraud, Javelin Strategy & Research, 2017
[6] Global Mobile Shopping, Banking and Payment Report, Nielsen, 2016

How iovation Stops Online Banking 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 customers' 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:

- Card Not Present (CNP)
- Payment Fraud
- New Account Fraud (NAF)
- Account Takeover (ATO)
- Call Center Fraud
- Synthetic Identity Fraud

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 drops as well.	Users register their devices with ClearKey, which recognizes them in future visits and provides an additional authentication factor. This extra assurance is invisible and frictionless to customers.
New Account Fraud Criminals use stolen or synthetic identities to create new accounts, bypassing ATO defenses. Once they earn trust with a series of small transactions, they apply for – and then max out – new cards and loan products before disappearing.	Our patented multi-layered approach to device recognition analyzes thousands of permutations of device attributes to recognize every visiting device while minimizing false positives. Devices with bad reputations – and associated devices – are stopped in real time from creating accounts.
Call Center Fraud is Increasing Fraudsters gather data about customers and then combine high-pressure tactics with spoofing technology to socially engineer your agents and take over customers' accounts.	Multifactor authentication methods in LaunchKey strengthen security both online and offline, without slowing down service. It empowers call center agents to quickly validate callers' devices before providing service.
You Have No Shared Fraud Intelligence Source At an industry conference you heard other banks are being hit by the same fraud ring. Why can't you work together to fight back?	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 and industries.

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 banks race to strengthen their authentication solutions, customers expect the best possible online experience, beginning at login.

Your Problem	Our Solution
Your Fraud Solutions Add Customer Friction You are constantly pressured to reduce friction caused by your fraud prevention efforts, especially during sales promotions. But, when you do, your fraud rates go up.	Through a combination of machine learning, device behavior, and device reputation, you can separate honest, good customers from repeat abusers of your promotions. Thus, good users receive the best user experience. Fraudsters are declined.
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, delivering insight on access requests, step-up authentication processes, and device histories. For greater customization, LaunchKey simplifies and unifies every customer experience, whether online or in-person, with a single user-selectable method of authentication.
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 solutions. With LaunchKey you can layer in multiple authentication options, from transparent and frictionless to interactive and fully integrated.
Your Current Tools Miss Risk Signals Does your customer just want to view their statement? What if they want to make a payment or change their account settings? And if they want to make a large transfer? 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.
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 "Are these the right people?" to "Are these people authorized for this transaction?"	LaunchKey offers a unique and patented multifactor authorization capability. Require multiple users or a quorum of named authorities to remotely authenticate and authorize requests or transactions. Adjust the number of required approving parties according to the size of the requested transfer automatically. Improve validation. Gain audit-ability.

Rethink Authentication and Improve Access

Armed with billions of user credentials breached over the past decade, and plenty of incentivized 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 customers' service experiences – calls for a completely new way of thinking. LaunchKey anticipates the challenge with:

- **Omnichannel flexibility:** Today, authentication varies by the channel. On the web, customers enter their username and password, and possibly a one-time password. They enter the same credentials on your mobile app, but with a tiny, typo-prone keyboard. When calling for help, they answer KBA questions. Imagine a time when every channel will use the same simple authentication method: the user's device.
- **Decentralized architecture:** Remove the target, and hackers have no way of stealing and reusing 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 will readily adapt to new methods with modification to its SDK.

To remain competitive, online banking 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®