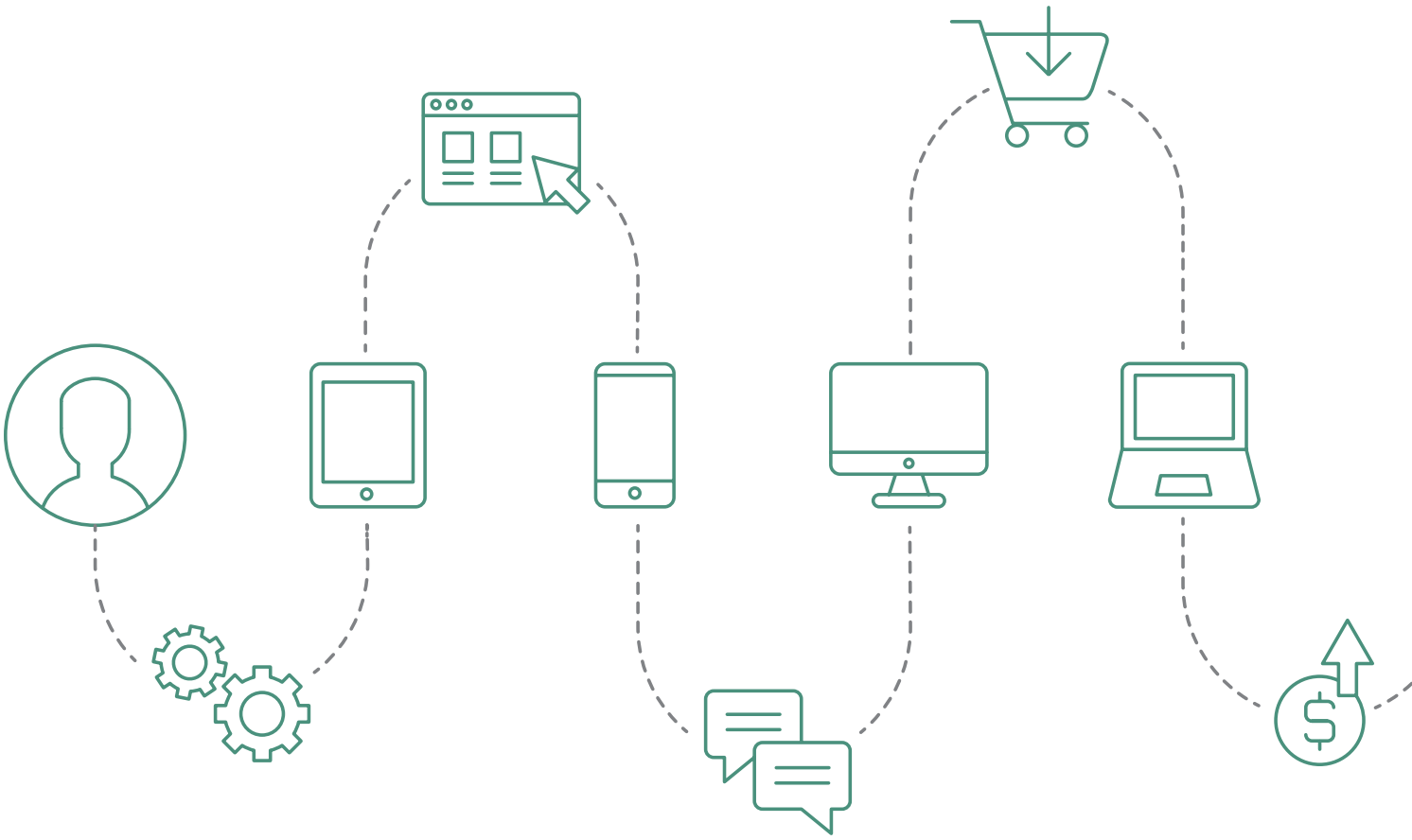
ENABLE AN OMNICHANNEL BANKING EXPERIENCE. PREVENT ACCOUNT TAKEOVER.

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 balanced against the realities of organized fraud, and new regulatory mandates for stronger customer authentication. iovation provides banks with solutions that satisfy the competing demands of catching fraud, authenticating good customers and providing an outstanding user experience.



Our Experience

Preventing fraud and protecting financial services

Transactions protected by iovation OVER THE PAST 12 MONTHS	Financial services customers	All customers
NUMBER OF TRANSACTIONS PROTECTED	4.8 billion	8.2 billion
NUMBER OF RISKY TRANSACTIONS STOPPED	31 million	514 million
NUMBER OF REPUTATION REPORTS SUBMITTED BY ANALYSTS	1.4 million	13 million
PERCENT OF DEVICES PREVIOUSLY SEEN BY IOVATION	76%	74%

Types of financial institutions that use 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 financial technology companies 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 and applications. And to detect and stop cybercriminals.

The race with customers' expectations and against criminals' tactics [1]

Banks' priorities for digital transformation:

- 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]**

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 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 (ATO)
- 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 a web-enabled device. iovation knows the reputation of over five billion 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 the need of customers' 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:

- Loan stacking
- Account registration fraud
- New account fraud
- ATO
- Call center fraud
- Synthetic identity fraud

Your challenges	Our solutions
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.	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.
Account registration fraud Fraud rings take advantage of legitimate customers that set up accounts in a branch and forget to register it online, registering and taking over the account.	We let you know when disparate devices are used to access the same account or when the same device accesses many different accounts. Specify a transaction velocity for an account, device, or IP address to stop high-volume transactions, a common symptom of a fraud ring.
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.

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 challenges	Our solutions
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. Passwords 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 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, 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 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 knowledge-based authentication 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.
- **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 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 **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

iovation®
A TransUnion® Company