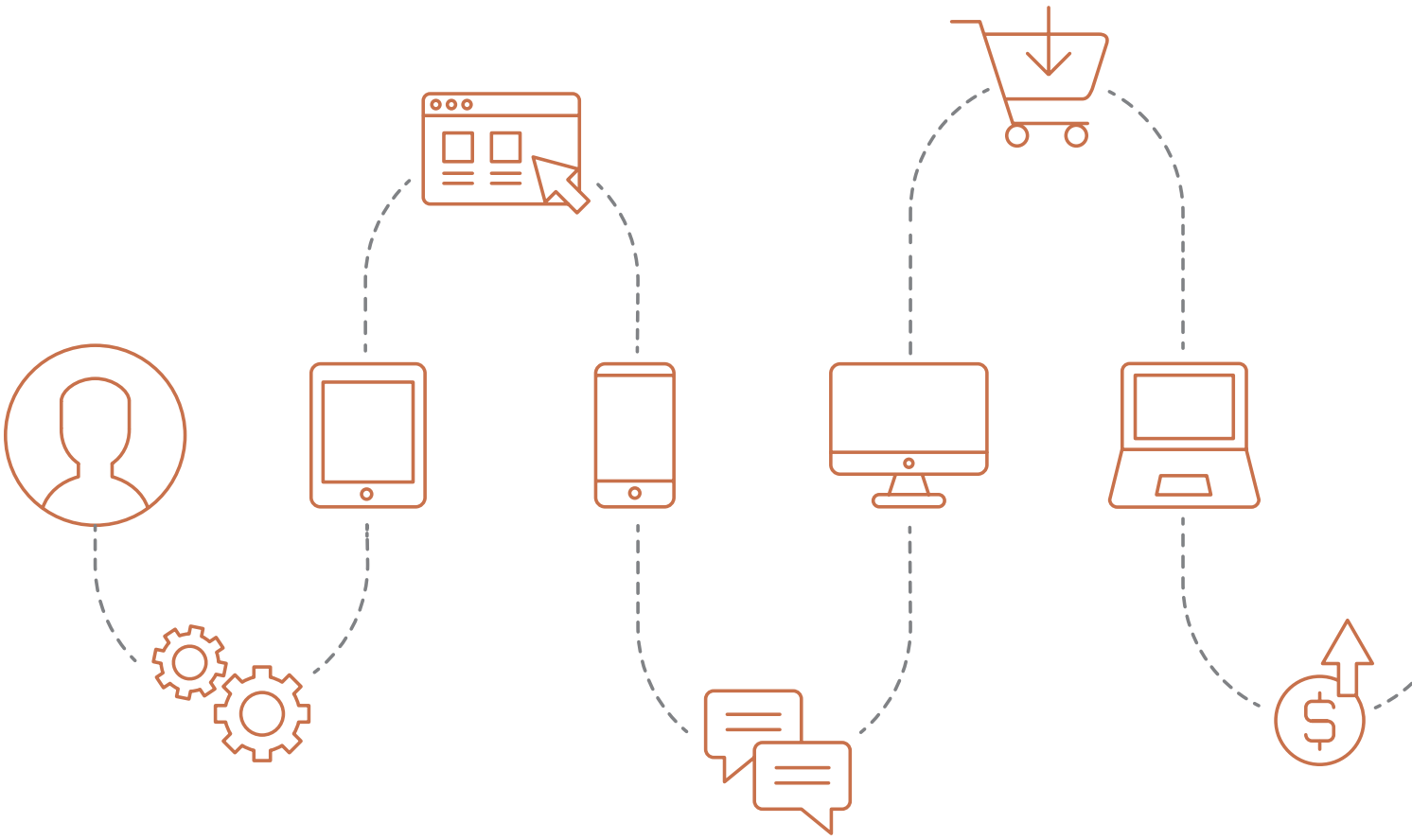
E-COMMERCE

DELIGHT CUSTOMERS & CLOSE THE DOOR ON FRAUDSTERS

In e-commerce, user experience is paramount.

As part of the customer's overall brand experience, new standards have emerged for frictionless, immediate access to sites and mobile applications. Yet this experience needs to be balanced against the realities of organized fraud, and new regulatory mandates for stronger customer authentication. iovation provides e-commerce solutions that satisfy the competing demands of catching fraudsters, authenticating good customers, and providing outstanding user experiences.



Our Experience

Transactions Protected by iovation OVER THE PAST 12 MONTHS	E-commerce	Total
TOTAL NUMBER OF TRANSACTIONS PROTECTED	1.6B	8.2B
NUMBER OF RISKY TRANSACTIONS STOPPED	200M	514M
# REPUTATION REPORTS	1.8M	13M
% OF DEVICES THAT IOVATION HAS SEEN BEFORE	67%	74%

E-commerce companies that use iovation

- Computers & Electronics
- Lifestyle & Home
- Automotive & Industrial
- Wholesale
- Outdoors & Health
- Fashion, Beauty & Bridal
- Hobbies & Travel
- Business & Education
- Entertainment & Media

Create An Outstanding Experience and Shut Down Fraud

Customer authentication and fraud prevention solutions for e-commerce

The e-commerce industry's meteoric rise – a 20% year-over-year increase and $2.7 trillion in worldwide online revenue – has attracted fraud. Lots of fraud.

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

And what do your customers want?

They want an easy and fast online experience, from login to check-out. ID proofing, authentication, purchase: too much friction at any point in their journey may push them to a competitor offering a smoother path to purchase. Your team's job is to make it easier for shoppers and harder for fraudsters.

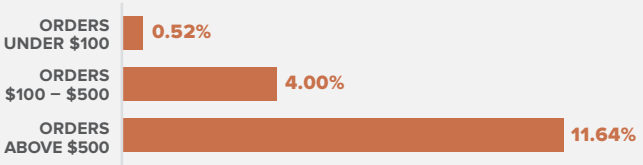
Your challenges:

- Improve the login experience without sacrificing security
- Authenticate shoppers while stopping account takeover
- Fight fraud and abuse across ever-changing vectors
- Enhance usability, even as prices and margins decline
- New accounts are your lifeblood, but a doorway to fraud
- Different risks exist at each part of customer journey
- Stop friendly fraud without hurting your good customers
- You can no longer just look at "risky interaction points" but need to extend risk insights to every customer login

E-commerce fraud is up 5.5% year-over-year across all industries, but rose significantly higher in several sub-segments.[1]

Fraudsters show a strong preference for high-value targets.[1]

FRAUD PERCENTAGE INCREASE BY ORDER AMOUNT:



The Solution: Focus On Your Customer's Device

Every purchase. 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]Global Fraud Index, Pymnts.com, October, 2017.

How iovation Stops E-Commerce 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 identifiable 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: **identity theft, credit card fraud, card-not-present fraud, friendly fraud, triangulation fraud, promotions abuse fraud, policy and license violations, and shipping fraud**.

Your Problem	Our Solution
Sophisticated, Big-Business Fraud Rings You believe that the same group of well-organized fraudsters are hitting you from multiple directions using sophisticated methods and different devices, but can't prove it, much less stop it.	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. Specify a transaction velocity for an account, device, or IP address to stop bad actors before they strike
Intelligence is Out There: How Can You Leverage It? At an industry conference you heard others in your industry are being hit by the same fraud ring. Why can't you work together to fight these guys?	Over 4,000 global fraud professionals use our unique device reputation database to share confirmed fraud and abuse reports. With over 5B devices and 50M incidents reported, this real-time intelligence stops fraudsters as they move from business to business.
Synthetic Identities Are Hard To Spot Fraudsters are outmaneuvering you using techniques such as synthetic or forged or hybrid identities, automated attacks, device spoofing, and proxies.	With patented, highly accurate device recognition technology, we help you spot risks from device behavior/characteristics using advanced machine learning analytics, uncover false IP addresses/ geolocations, and detect techniques that fraudsters use such as evasion, jailbreaks, and emulators.
You Have Internal Pressures, Too You are constantly pressured by your sales and marketing departments to reduce the user 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 programs. Thus, good users receive the best user experience and the fraudsters are stopped cold.

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 e-commerce companies 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 drops, too.	Users register their devices with ClearKey, which recognizes them in future visits and provides an additional authentication factor. This additional assurance is invisible and frictionless to customers.
Credentials Are Everywhere Nearly 6 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.
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 even more nuance, we augment the subtle aspects of reputation and risk that FraudForce reveals. The authentication challenge adjusts with the detected threat.
Your Current Tools Miss Risk Signals Does your customer just want to see their order history? What if they want to repeat an order to the same address? 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.
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?"	LaunchKey provides built-in authorization, allowing your customers to respond in real time to a specific request, like "Transfer $50,000 to Acme Company?" Or even, "Do you grant permission for this package to be delivered without signature?" 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. On the phone, callers answer KBA questions. At the POS, customers enter a card and PIN. At the customer service desk they provide photo ID and maybe a thumbprint. Imagine a time in the near future when every channel will use the same simple authentication method: the user's device.

To win the user experience battle, your e-commerce brand must continually balance ease of use 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 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

iovation®