IMPROVE CUSTOMER EXPERIENCE. PREVENT E-COMMERCE FRAUD. REDUCE CART ABANDONMENT.

In the E-Commerce Industry,
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 with solutions that satisfy the competing demands of catching fraudsters, authenticating good customers and providing an outstanding customer experience.
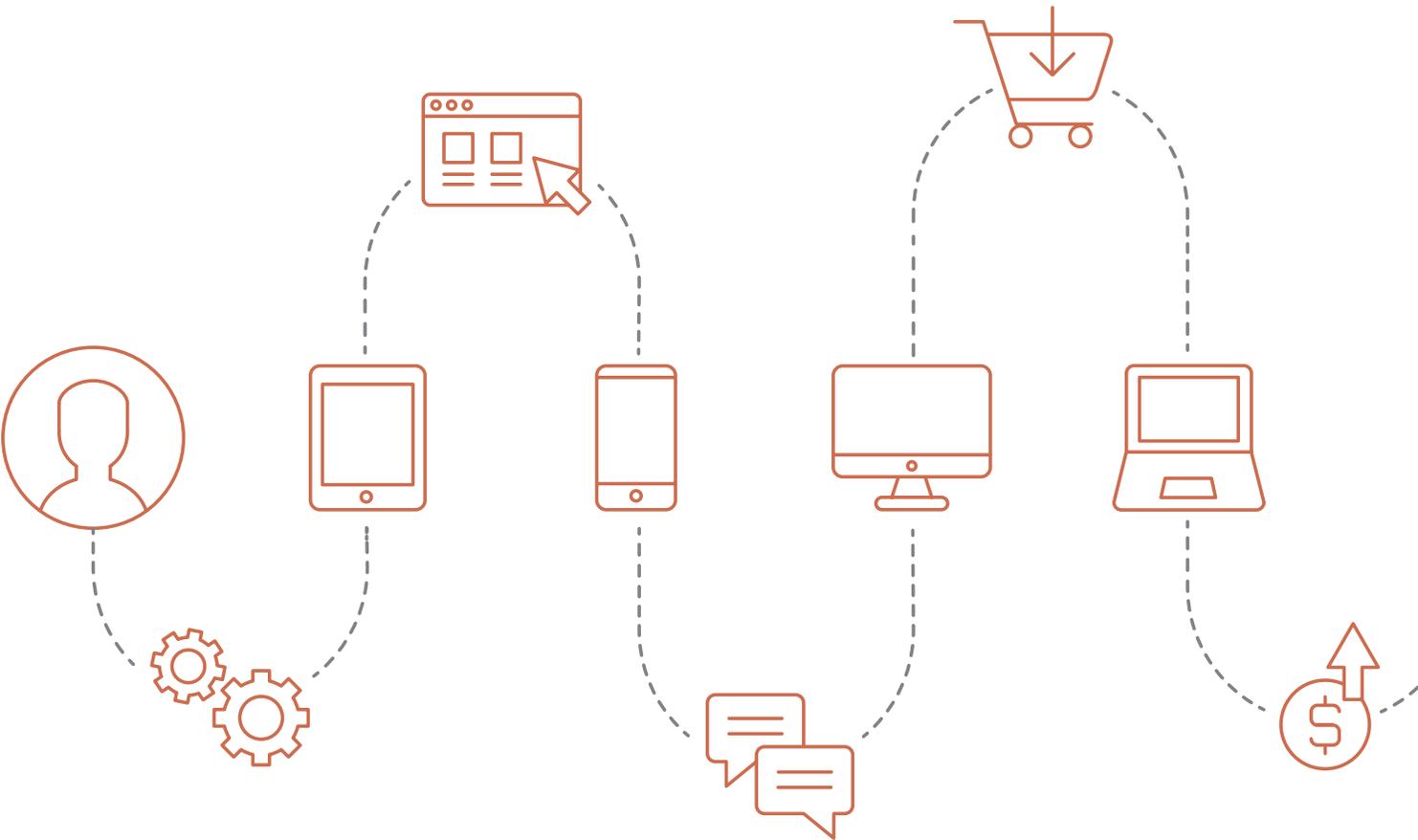
Our Experience

Preventing fraud and protecting e-commerce businesses

Transactions protected by iovation OVER THE PAST 12 MONTHS	E-commerce customers	All customers
NUMBER OF TRANSACTIONS PROTECTED	1.6 billion	8.2 billion
NUMBER OF RISKY TRANSACTIONS STOPPED	200 million	514 million
NUMBER OF REPUTATION REPORTS SUBMITTED BY ANALYSTS	1.8 million	13 million
PERCENT OF DEVICES PREVIOUSLY SEEN BY IOVATION	67%	74%

E-commerce companies that use iovation:

- Computers and electronics
- Lifestyle and home
- Automotive and industrial
- Wholesale
- Outdoors and health
- Fashion, beauty and bridal
- Hobbies and travel
- Business and education
- Entertainment and 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. [1] 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 checkout. 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:

- Improving the login experience without sacrificing security
- Authenticating shoppers while stopping account takeover (ATO)
- Fighting fraud and abuse across ever-changing vectors
- Enhancing usability, even as prices and margins decline

E-commerce fraud is up 5.5% year-over-year across all industries but rose significantly higher in several sub-segments. [2]
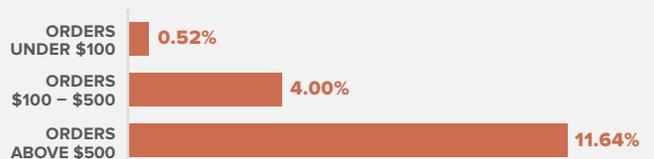
11.9%
CONSUMER ELECTRONICS

36.7%
JEWELRY

172%
COSMETICS & PERFUMES

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

FRAUD PERCENTAGE INCREASE BY ORDER AMOUNT:

ORDERS UNDER $100 — 0.52%

ORDERS $100 – $500 — 4.00%

ORDERS ABOVE $500 — 11.64%

The solution: Focus on your customer's device
Every purchase. 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] Statista 2017.
[2] 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 the need of directly identifiable 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:

- Identity theft
- Triangulation fraud
- Shipping Fraud

- Credit card fraud
- Promotions abuse

- Friendly fraud
- Policy and license violations

Your challenges

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.

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?

Synthetic identities are hard to spot
Fraudsters are outmaneuvering you using techniques such as synthetic, forged, or hybrid identities, automated attacks, device spoofing, and proxies.

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.

Our solutions

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.

Over 4,000 global fraud professionals use our unique device reputation database to share confirmed fraud and abuse reports. With over 5 billion devices and 55 million incidents reported, this real-time intelligence stops fraudsters as they move from business to business.

With patented device recognition technology, we help you spot risks from device behavior and characteristics. We use advanced machine learning analytics, uncover false IP addresses and geolocations, and detect other techniques that fraudsters commonly use.

Through a combination of machine learning, device behavior, and device reputation, you can separate good customers from repeat abusers of your promotions programs. Thus, good users receive the best user experience and the fraudsters are stopped.

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 challenges

ATO is rising
The risk of ATO drops as you introduce more authentication factors, but the quality of the user's experience drops, too.

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 (KBA) 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 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.

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 solutions

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.

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.

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.

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.

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, KBA 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' 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.

- **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 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 point of sale, 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 **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