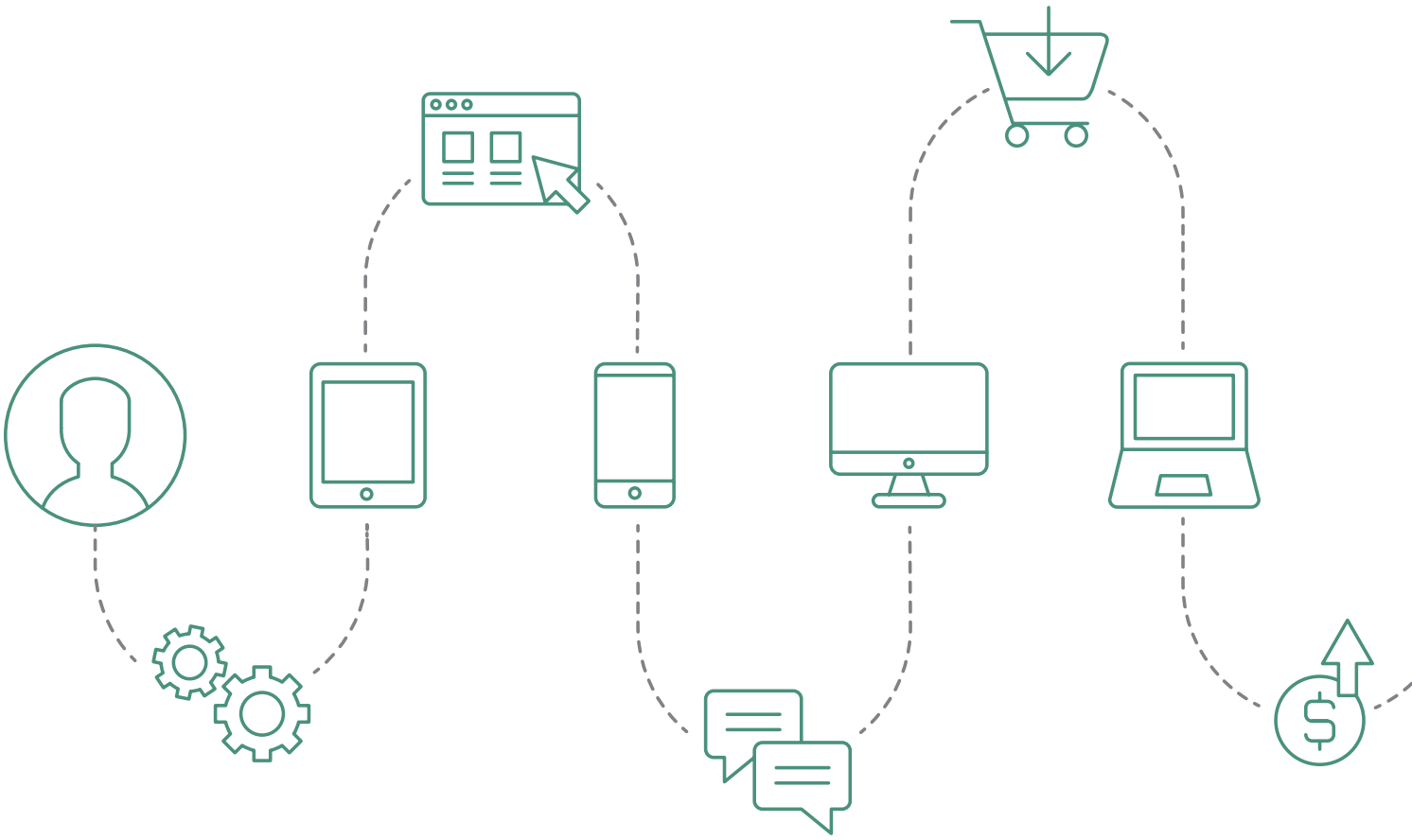
CREDIT ISSUERS

IMPROVE YOUR CUSTOMERS' EXPERIENCE AND YOUR FIGHT AGAINST CREDIT FRAUD

Reduce Fraud Losses.
Exceed Customer Expectations.

In the credit issuance industry, user experience is paramount. 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 credit issuers solutions that balance the competing demands of catching fraud, authenticating good customers, and providing outstanding user experience.



Our Experience

Preventing Fraud and Protecting Credit Issuers

Transactions Protected by iovation OVER THE PAST 12 MONTHS	Credit Issuers	Customers
TOTAL NUMBER OF TRANSACTIONS PROTECTED	3.3B	8.2B
NUMBER OF RISKY TRANSACTIONS STOPPED	22M	514M
REPUTATION REPORTS SUBMITTED BY ANALYSTS	418K	13M
DEVICES PREVIOUSLY SEEN BY IOVATION	77%	74%

Types of Credit Issuers that use iovation

- Credit Card Issuers
- Retail Banks
- Commercial Banks
- Short-Term Lending
- Payment Processors
- Money Services

Create An Outstanding Experience and Shut Down Fraud

Customer authentication and fraud prevention solutions for credit issuers

The Financial Services market has seen a massive digital disruption in the last decade that has been especially impactful for online credit issuers. Over 5,000 FinTechs have emerged in the last decade, elevating market competition. Customer expectations are higher than ever, particularly in regards to accessibility and speed of service. Compressed timeframes for processing transactions and applications mean credit issuers often only have seconds to detect and stop cybercriminals.

According to the 2017 Nilson Report:

- Total card fraud losses reached $22.8B in 2016
- The U.S. accounts for $9 billion or 39.5% of worldwide card fraud losses
- Card issuers worldwide experienced $16.13 billion or 70.7% of gross fraud losses.
- Merchants, their acquirers, and ATM acquirers suffered the remaining $6.67 billion in fraud losses

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?

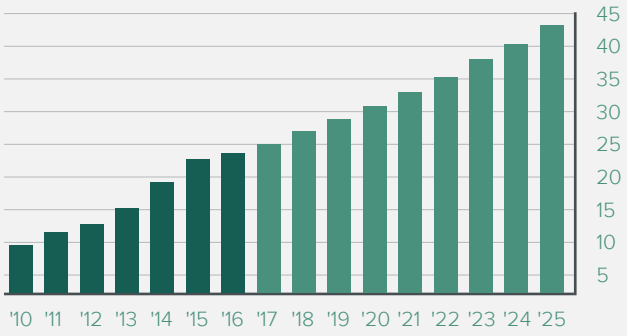
Secure, easy, instant access to services across all channels at all time. Credit application. Account login. Payment processing. Too much friction at any point and customers could click over to a competitor offering a smoother experience. Your job is to make it easier for customers and harder for fraudsters.

Your challenges:

- Improve the login experience without sacrificing security
- Stop CNP fraud without hurting your good customers
- Authenticate customers while stopping account takeover
- Fight fraud and abuse across ever-changing vectors
- New accounts are your lifeblood, but a doorway to fraud
- Different risks exist at each part of customer journey

Card Fraud Worldwide Projected ($bil.)

Source: 2017 Nilson Report



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.

How iovation Stops Credit 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 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
- Counterfeit Cards
- Account Takeover (ATO)
- Call Center Fraud
- Synthetic Fraud

Your Problem	Our Solution
CNP Fraud has Drastically Increased Adoption of EMV chip cards has significantly reduced POS fraud, but had the unintended consequence of driving up CNP fraud which now accounts for approximately 45% of total fraud losses in the US.[1]	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.
You Have No Shared Fraud Intelligence Source 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 this?	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 comprehensive database stops fraudsters as they move from business to business.
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 or apply for new lines of credit.	Multifactor authentication methods in LaunchKey strengthen security both online and offline, without slowing down service by empowering call center agents to quickly validate callers' devices before providing service.
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 programs. Good users receive the best user experience and the fraudsters are stopped cold.

[1] Nilson (2016, Oct). The Nilson Report, Issue 1096. Retrieved from https://www.nilsonreport.com/upload/content_promo/The_Nilson_Report_10-17-2016.pdf.

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 credit issuers 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 as well.	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 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.
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 view their statement? What if they want to make a payment or change their account setting? And if they want to do a cash advance? 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 "Approve this $500 purchase?" Or even, "Do you grant permission for Joe Smith to use your card?" 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, 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:

- **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.
- **Omnichannel flexibility:** Today, authentication varies by the channel. In a web browser, customers enter their username and password, and possibly a one-time password. When contacting your call center, they have to answer KBA questions. In person, they use a card and a PIN. Imagine a time in the near future when every channel will use the same simple authentication method: the user's device.

To remain competitive, credit issuers 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®