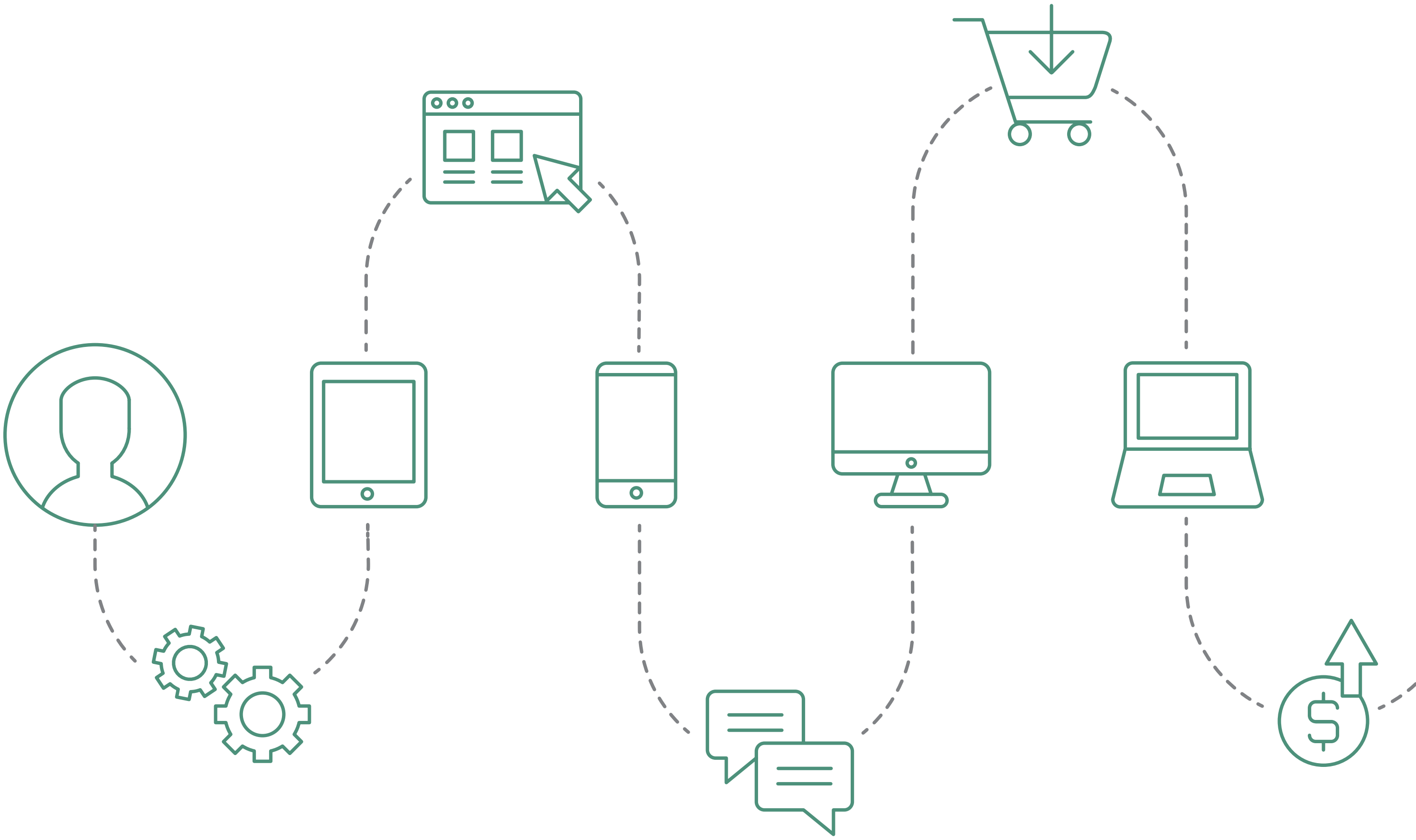
iovation®
A TransUnion® Company

CREDIT ISSUERS INDUSTRY BRIEF

GROW NEW CREDIT ACCOUNTS. SHRINK APPLICATION FRAUD.

Reduce Fraud Losses.
Exceed Customer Expectations.

Customer experience is paramount in the credit card issuance industry. 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 credit issuers the solutions that satisfy the competing demands of catching fraud, authenticating good customers and providing an outstanding user experience.



Our Experience

Preventing fraud and protecting credit issuers

Transactions protected by iovation OVER THE PAST 12 MONTHS	**Credit issuer customers**	**All customers**
NUMBER OF TRANSACTIONS PROTECTED	3.3 billion	8.2 billion
NUMBER OF RISKY TRANSACTIONS STOPPED	22 million	514 million
NUMBER OF REPUTATION REPORTS SUBMITTED BY ANALYSTS	418,000	13 million
PERCENT OF 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 new financial technology companies have elevated market competition. [1] Compressed timeframes for processing transactions and applications mean that credit issuers only have seconds to detect and stop cybercriminals.

According to the 2017 Nilson Report: [1]

- Total card fraud losses reached $22.8 billion 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
- Enhancing usability, even as prices and margins decline

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.

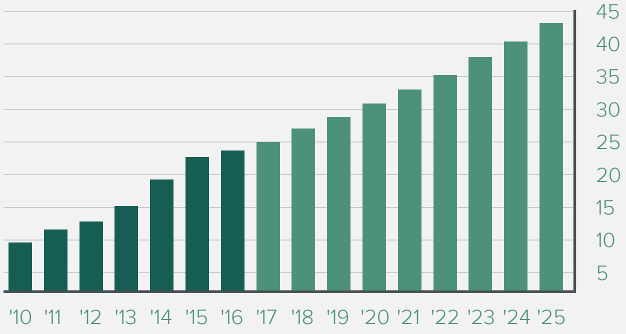
And what do your customers want?

They want secure, easy access to services across all channels at all times. 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 team's job is to make it easier for customers and harder for fraudsters.

Your challenges:

- Combating growing identity theft and synthetic fraud, which is fueling new account fraud
- Fighting fraud and abuse in ever-changing vectors
- Improving login experience without sacrificing security or adding friction
- Authenticating customers on any device while stopping account takeover (ATO)

Card Fraud Worldwide Projected ($bil.) [1]



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] 2017 Nilson Report.

How iovation Stops Credit Card 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 for 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:

- New account fraud
- Chargebacks
- Counterfeit cards
- ATO
- Call center fraud
- Synthetic fraud

Your challenges	Our solutions
New account fraud is rising New account fraud hit $1.7 billion in 2017.[1] Criminals use stolen or synthetic identities to create new accounts, bypassing IAM defenses. Once they earn trust with a series of small transactions, they apply for – and then max out – new cards before disappearing.	Our 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.
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 these guys?	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 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.	Multifactor authentication methods in LaunchKey strengthen security both online and offline, without slowing down service. Call center agents can quickly validate callers’ devices before providing service.
Your fraud solutions add customer friction You are constantly pressured to reduce friction, 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 customers from repeat abusers of your promotions programs. Good users receive the best user experience. Fraudsters are stopped cold.

[1] Javelin Strategy & Research – From Application to Transaction: Card Fraud Trends, Threats, and Tactics

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 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 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 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:

- **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.
- **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 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 **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