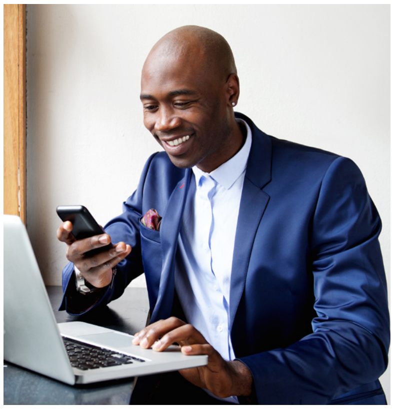
iovation
A TransUnion® Company

Product Sheet

FraudForce Device-Based Reputation



—

Providing your customers with a positive online experience is crucial, but how do you protect your business and your consumers while delivering a seamless experience – even when bad actors have perfect information?

Massive data breaches have compromised millions of usernames and passwords from major retailers, financial institutions, and social networking sites. EMV is compelling fraudsters to shift away from point-of-sale (POS) fraud to focus on card-not-present (CNP) fraud.

iovation FraudForce stops online and mobile fraud in real time. Our unique approach to device intelligence gives online businesses the tools they need to stop fraudsters and fraud rings without sacrificing customer experience. We track relationships between devices and accounts, and leverage device history and confirmed fraud reports from our global network of fraud and security analysts.

Our technology adds an independent layer of digital identity that recognizes internet-connected devices separate from personal data, which is often compromised. Our powerful fraud prevention technology can be easily integrated into any native app (iOS, Android, Windows, Mac OS) or web application, and at any customer touch-point where fraud risk is a concern, such as account creation or modification, purchase or transfer.

iovation has a comprehensive database of devices and fraud evidence, with over 6 billion devices seen, 69 million confirmed fraud reports, and a network of 5,000 fraud analysts.

Uncover Coordinated Fraud Rings

Device-based authentication easily integrates with your existing authentication flow without adding customer friction. It provides customers with an invisible, hassle-free digital experience by recognizing and using their device as an additional factor of authentication.

Onboard Good Customers and Keep Fraudsters Out

Device-based authentication provides powerful risk insight that allows you to assess risk factors indicative of ATO attacks including device anomalies, spoofing, and detection evasion. It adds a second, invisible layer of authentication that drives step-up measures when new or suspicious devices try to access an account, enhancing your existing authentication procedures without heavy lifting or intense coding.

Target the Types of Fraud That Impact You

Device-based authentication adds the critical ingredients of context and risk to your customer-facing authentication solution. Geolocation, true IP address and risk scores combine with a powerful rules engine to provide insight on access requests and step-up authentication processes.

Build associations between devices and user accounts without relying on personal data.

Key Features

Uncover Hidden Fraud Data

Our analytics, searching, and reporting capabilities help you spot transaction and device patterns that indicate fraud. Advanced fraud prevention and detection capabilities extend your protection to track the patterns that you are most concerned about.

Recognize Device Types

Using a patented multi-layered approach to device recognition, we analyze thousands of permutations of device attributes to accurately recognize a device while minimizing false positives.

Evasion Detection

Detect fraudsters hiding behind proxy servers, TOR networks, mobile virtual machines, emulators or other anonymizing technology. Gain insight into high-risk activity such as mismatches of specific time zones, regions and IP addresses.

Adapt to Changing Fraud Patterns

Our powerful and flexible business rules editor enables fraud analysts to react immediately to new threats. For example, track if a particular device has been used to access multiple accounts within a particular time period, or if several devices have been used to access a single account.

Email and Phone Verification

Gain visibility into the behaviors and attributes connected to a fraudulent email or phone number and centralize your fraud detection programs with this add-on feature for US subscribers.

Device and Account Links

Reveal hidden connections between devices and accounts, even across subscribers and industries. Through device and account associations, easily spot and stop fraud rings before they do damage to your business.

Key Advantages

With iovation's help, we reduced customers' friction in the application process by half and account bookings improved two-fold over the original process.

Jen
Vice President

Secure every point of the customer journey

Used in conjunction, iovation's solutions secure any point in the customer's online journey, from account creation to purchasing, to assure that consumers are identified correctly and fraud is stopped.

Authenticate in real time

In about 100ms, iovation recognizes a device, checks if it's authorized for an account and checks for risk signals. Identify and authenticate all device types, from phones and PCs to laptops and tablets, regardless of the platform, OS, browser or mobile apps.

99.9% uptime

iovation's distributed SaaS infrastructure supports the largest transaction volumes in the world with an average response time of 100 milliseconds. An active-active infrastructure means no service interruptions during updates or maintenance.

World-class fraud and ATO experts

Add our trusted fraud advisors to your team. Our customer success team partners with you to solve your unique business challenges and adapt to an ever-changing fraud environment.

Get in Touch

Find out more about our authentication and fraud prevention solutions. Contact us for a demo or visit iovation.com

iovation
A TransUnion® Company

Global Headquarters
iovation, a TransUnion Company
555 SW Oak Street, Suite #300
Portland, OR 97204 USA
PH +1 (503) 224 6010
EMAIL info@iovation.com

United Kingdom
PH +44 (0) 800 058 8731
EMAIL uk@iovation.com

iovation.com