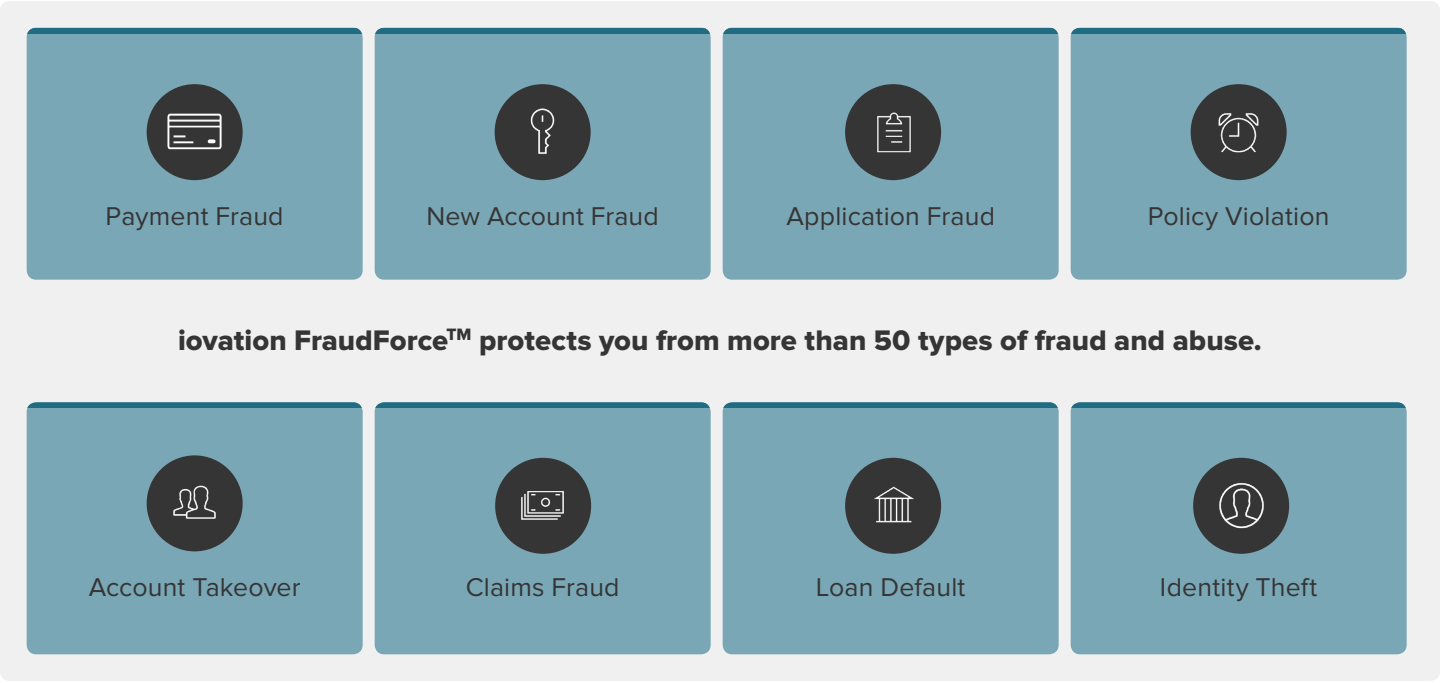
FraudForce

Using device intelligence to stop online fraud and abuse in real time



Online fraud costs businesses billions of dollars worldwide every year, and you never know where or when a fraudster will strike. That's why stopping online fraud before it happens is your best defense.

When it comes to online fraud, massive data breaches that have compromised countless user names and passwords from major retailers, financial institutions, and social networking sites have dominated the news. But that's just the beginning.

- EMV is compelling fraudsters to shift away from point of sales (POS) fraud to focus on card not present (CNP) fraud.
- Synthetic identify fraud is on the rise, even outpacing true identity theft.
- Fraudsters are now using more sophisticated techniques like device emulators, virtual machines, botnets and anonymization.

iovation FraudForce stops online and mobile fraud in real time. Utilizing powerful device recognition technology and a unique approach to device intelligence that leverages device-to-device and device-to-account associations, device history, and detailed reports of confirmed fraud from a global network of fraud and security analysts, iovation provides the tools online businesses need to stop fraudsters and fraud rings without sacrificing customer experience.

By recognizing Internet-connected devices without requiring directly identifiable personal information, our technology adds an independent layer of digital identity that's separate from personal data that may have been previously 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.

Identify fraud patterns

To help you accurately separate the fraudsters from your good customers, iovation FraudForce identifies risky device behaviors including:

Evasion Techniques:
Includes transactions originating from TOR networks, use of a proxy server, or use of mobile emulators.

Device Anomalies and Risk Indicators:
Includes location mismatches, time zone and IP address changes, and transactions that originate from known high-risk locations, IPs, or ISPs.

Device Behavior:
Device Behavior: Includes high transaction volumes, too many accounts and/or geolocations per device, and past history of fraud or abuse.

Advanced Analytics

Our advanced fraud prevention and detection capabilities extend your protection to fraud patterns that you are most concerned about. For example, iovation can inform you:

- If a particular device has been used to **access multiple accounts** within a particular time period.
- When many devices have been used to **access a single account**.
- If the device has a history of **specific types** of fraudulent activity.
- When the device is **linked to other devices** or accounts associated with fraud.
- Whether the device has **violated specific policies** that you have defined such as geolocation, chat abuse, spending limits, or cheating.

Key Features

- **Accurately recognize devices of all 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.
- **Comprehensive database of devices and fraud evidence:** Join over 6,000 fraud and security analysts who fight global fraud rings by leveraging our database informed by the experience of over 6 billion known devices and over 65 million detailed fraud reports.
- **Device and account linkages:** Reveal hidden connections between devices and accounts, even across subscribers and industries.
- **Evasion detection:** Stop fraudsters who are hiding behind proxy servers, TOR networks, VPNs, mobile VMs, emulators or other anonymizing technology.
- **Quickly adjust to changing fraud patterns:** Our powerful and flexible business rules editor enables fraud analysts to react immediately to new threats.
- **Spot new risk patterns with machine learning:** Leverage SureScore to catch more fraud by detecting and analyzing subtle as well as global risk patterns.
- **Performance and reliability:** Our service has a 99.9% uptime to ensure you're always protected.

Benefits

- ✓ **Stop fraud in real time:** In about 100ms, iovation will recognize the device, determine if it's evading detection, check to see if it's associated with past fraud or other devices/accounts linked to fraud, and run all of the transaction risk checks that you have specified.
- ✓ **Integrate device intelligence into your other systems:** Besides returning an actionable Approve/Review/Deny response, our real-time service returns detailed device attributes including hundreds of mobile fields along with detailed reasons for a Deny response.
- ✓ **Uncover coordinated fraud rings:** Discover cybercriminals working together by exposing hidden relationships.
- ✓ **Find hidden fraud through dynamic data analysis:** Our analytics, searching, and reporting capabilities help you spot transaction and device patterns that indicate fraud.
- ✓ **Enhance your fraud detection with email phone verification:** Get 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.
- ✓ **Botnet detection:** Leverage a botnet risk score - based on a history of frequency, severity and evidence placement of previous attacks - to make real time decisions on botnet threats.

iovation®
A TransUnion® Company

Find out more at **iovation.com** or (503) 224-6010.

PORTLAND • PH +1 (503) 224-6010 • EMAIL info@iovation.com **LONDON** • PH +44 (0) 800 058 8731 • EMAIL uk@iovation.com