iovation
A TransUnion® Company

RETAIL CASE STUDY

ONLINE RETAILER REDUCES FRAUDULENT ORDERS BY 25%

CHALLENGES

With fraudsters constantly implementing new techniques to escape detection, the company had difficulty shutting down international fraud rings that were using stolen payment credentials to purchase goods.

SOLUTIONS

iovation FraudForce helped the company link previously unrelated fraudulent accounts, monitor specific device characteristics to identify fraud and high-risk transaction, and reduce manual reviews by fine-tuning business rules.

RESULTS

The company saw a 25% reduction in fraudulent online shipments, reduced reviews and gained operational efficiency, and increased fraud detection using fraud evidence from related businesses.

A GLOBAL RETAILER OF ELECTRONICS, SOFTWARE AND SERVICES PROCESSING MORE THAN FOUR MILLION ONLINE TRANSACTIONS, FIGHTS FRAUD EVERY DAY.

With an average order amount of $700, this retailer finds itself targeted by international fraud rings on an ongoing basis.

Device Intelligence Provides Critical Layer of Protection

This online retailer chose to incorporate iovation's device reputation technology into its own risk scoring system as another layer of protection. It provides insight into customer behavior and risk from a device perspective that was previously unseen.

Many of iovation's clients already have some type of fraud protection in place. Their current tools often rely on personally identifiable information to evaluate the risk of a transaction. At iovation, we evaluate risk based on what we know about the device being used to initiate an action like login, register or checkout. This gives online businesses insight into fraud they often can't identify with their current tools. Device intelligence provides significant uplift in fraud reduction both as a stand-alone solution and as a facet of a larger fraud detection system or platform.

"We had other fraud prevention technologies in place, but before iovation we didn't have the ability to look at the reputation of the device itself. We felt this was critical to identifying where fraud was coming from and stopping it," said the Fraud Manager.

Device and Account Links

iovation currently recognizes 5 billion global devices across our client base and that number grows every day. This means when an Internet-enabled device accesses the online retailer's site, there's a good chance it already has a known history and an associated risk assessment. Our data shows whether a device has a previous history of credit card fraud, identity theft, account takeover or other suspicious behavior.

After we identify a device, we find the links between other devices and associated accounts in real-time. Our comprehensive network contains over 55 million records

of fraud. This in-depth insight into previous fraud activity is extremely useful in weighing the risk of a transaction and reveals associations between devices and accounts that this retailer wasn't able to connect before. This insight allowed them to confidently stop orders knowing they wouldn't impact legitimate, good customers.

I'VE BEEN WITH THE COMPANY FOR 17 YEARS AND WHEN IT COMES TO FRAUD, IT'S ABOUT STAYING ONE STEP AHEAD OF THE BAD GUYS. THEY WILL TRY EVERY POSSIBLE WAY TO COST US REVENUE THROUGH FRAUDULENT ACTIVITY. WE NEED TO BE READY. IOVATION'S DEVICE REPUTATION TECHNOLOGY ADDS AN INCREDIBLY IMPORTANT LAYER OF PROTECTION TO OUR FRAUD EFFORTS.

Fraud Manager

"Once we implemented iovation we saw a 25 percent reduction in fraudulent online shipments. Our review volumes went down based on the business rules we added, and our fraud analysts perform manual reviews faster and with more data than before. We haven't had to add additional personnel to the fraud team. In fact, the efficiencies gained have allowed us to refocus some members on higher priority research projects," said the Fraud Manager.

The Value of a Business Partnership

iovation client managers are not only well-versed in all the capabilities of our device technology, but they immerse themselves in a client's business model as well. They understand where the pain points are and how to thoroughly apply iovation's capabilities to be the most effective as possible.

"I've been pleased by how proactive the client managers are in working with us. They keep an eye on our transactions, run reports and send a note when they notice a trend or want to suggest a business rule modification in response to a current situation. It's very helpful to have a partner that's invested in stopping fraud with us," said the Fraud Manager.

Device intelligence is a powerful tool that provides considerable information about every device and transaction. Our client managers understand that fighting fraud is not a static process. They constantly look for ways to improve, update and change the business rules clients use to fend off fraud.

"Our client manager helps us focus our business rules and locate incremental fraud. That working relationship provides a tangible, additional level of value to iovation FraudForce," said the Fraud Manager.

One Instance of Fraud

A 25 percent reduction in fraudulent online shipments comes with many stories of scams and fraud rings. This particular story involves a device, one transaction, three different locations and a time zone mismatch. It illustrates one of the many ways that iovation's device reputation technology, and consortium of over 4000 fraud professionals, can reveal and stop fraud.

The fraud team at this online retailer used iovation's technology to set up a rule to detect activity from risky ISPs. They found that this was the only rule that flagged some transactions as possible fraud. This single rule flagged ISPs with fraud rates well in excess of 50 percent.

At one point, the fraud manager noticed a particularly odd ISP and shared that information with the Fraud Force Community—a private web portal for iovation's clients to interact directly. They posted a message letting other members know that they had run across an odd ISP named Web Africa Proxy. Its location showed as the United States and not Africa but was also not getting flagged as a known proxy.

"Since we'd seen two in the past week, one showing Los Angeles, California and the other Dallas, Texas, it made sense to review these ISPs to see if they belong on a proxy list and determine whether the geolocation is accurate," noted the Fraud Manager.

An iovation client manager saw the retailer's Fraud Force Community post and proactively began to investigate the issue on behalf of the client. She found three more devices and accounts related to Web Africa Proxy and shared that information with the computer retailer. At the same time the retailer was able to determine a very strong likelihood of credit card fraud on one of the devices coming through the Web Africa Proxy.

The retailer placed “credit card fraud” evidence on an account that showed one transaction coming from a device that had:

- A billing address in Massachusetts
- Shipping address going to New York
- An ISP based in Dallas, Texas
- An 8-hour time zone mismatch with the device’s set time

All these factors together indicated a high risk of fraud. Within 24 hours of flagging the device with this evidence, four other iovation clients saw the same device hit their sites. By sharing the anomalous order information the computer retailer encountered, they gave others crucial information about the risk involved with doing business with that one device and potentially any other devices and accounts associated with it. When the computer retailer flagged the device, they also armed all of iovation’s other clients with extremely important fraud intelligence. Since iovation is able to identify and then subsequently recognize the same device, including mobile phones and tablets, clients are able to help each other by sharing their fraud experiences.

The addition of iovation FraudForce provided a more robust fraud prevention approach for this online retailer. Fraudsters constantly look for new ways to cheat the system. They purchase and phish for personal information, find out answers to knowledge-based questions, and eventually uncover passwords. “iovation’s device intelligence lets us quickly link fraudulent activity, accounts and devices together—bringing to light relationships that we would not have known about otherwise,” said the Fraud Manager.

By taking advantage of FraudForce’s sophisticated rules engine, this company quickly accumulates and evaluates data in order to fine-tune business rules. This allows them to react swiftly against new attacks and be agile in their fight against ongoing fraud.

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