iovation
A TransUnion® Company

Financial Services

Case Study

How CashPlus and iovation teamed up to win a battle against bot attacks

Device Recognition Plays Essential Role in Isolating and Blocking 9,500 Fraudulent Applications

Challenge

9,500 fraudulent debit card applications flooded Cashplus in a few days. Applicants' personal data passed KYC inspection. Attacking scripts varied IP addresses through VPNs and countries. Blacklisting them all was infeasible.

Solution

iovation FraudForce revealed a gap in the attacking script's efforts; all applications came from the same device type. This insight led to a change in the FinTech's application process that stopped the attack permanently.

Results

Assuming 1 £2 per check, Cashplus saved £19,000 in KYC service fees, and prevented fraudulent accounts from opening lines of credit worth £2,000 each. The FinTech alerted victims whose personal information was used in the applications, potentially preventing millions of pounds worth of identity theft.

Device recognition plays essential role in isolating and blocking 9,500 fraudulent applications.

The first 2,000 fraudulent debit card applications appeared overnight. The applicants' names, addresses and dates of birth were correct, but the email addresses followed a pattern, and none of the phone numbers were in service. Clearly, the referring IP address needed to be blacklisted.

By next morning, another wave of thousands of fraudulent applications had arrived. This time, the applications had come in through a range of IP addresses, via multiple VPNs and countries.

For Cashplus – one of the UK's most innovative FinTech companies, and no stranger to fraudsters' efforts – the current spike in activity was unusual.

"We had a bot just looping through details to randomize the attack," explains James Coveney, Fraud and Credit Manager at Cashplus. "Thanks to data from iovation FraudForce, we could see a distinct device type across all of the applications. We combined iovation's data with ours so we could prevent any of the applications from converting into debit accounts."

By the time Cashplus stopped the attack the bots had submitted 9,500 fraudulent debit card applications.

First move in sophisticated identity-theft campaign

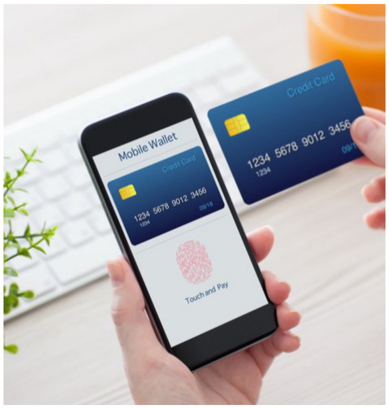
“We concluded that the attackers didn’t actually want debit card accounts,” says James. “They just wanted to use our Know Your Customer (KYC) service to validate a dataset. If we were to approve one of the applications, then ultimately, the attackers would know that they had a correct combination of name, date of birth, address and other personal information. It was a cleansing exercise.”

And a costly one at that. If James and his team hadn’t caught the applications, Cashplus would have had a big bill from its KYC service. At an assumed £2 per use, the attack could have cost upwards of £19,000.

Even more worrisome, those debit card accounts could be used in a popular scam in the United Kingdom.

“There’s quite a lot of regulatory discussion at the moment around payments into accounts,” James shares. “We might be held responsible for validating that payments into an account are from known sources. That’s quite a big topic for us at the moment.”

If the fraudulent debit accounts were opened successfully, they could be used to trick victims to transfer funds into the debit accounts. That would likely lead to consumer complaints against Cashplus, along with unwarranted attention from regulators. Preventing those fraudulent applications from converting into accounts was in the best interests of Cashplus, its customers, and the general public.



iovation’s device recognition technology uses thousands of permutations of device attributes to identify every visiting device instantly.

Device recognition underpins Cashplus’s successful defense

The device type used to submit the fraudulent applications represented an important clue. iovation’s device recognition technology uses thousands of permutations of device attributes to identify every visiting device instantly and continue to recognize it over time, including those coming through VPNs, proxies and Tor nodes.

“Due to the attack’s complex nature and the speed at which it took place, I assume that this was executed by more than one person,” James reflects. “Although they changed their approach and personal information, they didn’t have enough control over their

£19k

Saved in KYC service fees[1]

The attackers changed every detail on their applications, but the device type remained the same all the way through the attack. That gave us a way to identify their applications pretty easily.

**Paul Schooley,
Chief Operating Officer,
Cashplus**

script to modify the device type. That was the one continuous data point that we were able to track throughout the entire event. iovation's data has the device type; we had no problem there."

This was the kind of use case that originally convinced Cashplus to choose iovation over other providers. Paul Schooley, Cashplus's Chief Operating Officer, elaborates "When we reviewed the marketplace for a device recognition partner, we decided to use iovation because of the variety of benefits their solution offered on top of others in the market. We wanted something that not only gave unique device IDs but also enabled us to ingest new data about the devices our customers were using and to create rules based on this new data. During the proof-of-concept phase, it was clear that iovation met all these requirements."

Once James and his team confirmed that the applications were fraudulent – James personally visited some of the closest addresses on the applications – he uploaded evidence of the fraud into the iovation Intelligence Center.

When any iovation user confirms fraud from a device, they place specific evidence of that fraud against the device in iovation's database, which is the world's most comprehensive collection of device data built from experience with over 6 billion known devices.

[1] Cashplus' contract with its KYC provider expressly prohibits sharing the actual cost for its KYC service

Since integrating iovation we have used its various data points to enrich our existing internal data and enhance our fraud-detection capabilities.

Paul Schooley,
Chief Operating Officer,
Cashplus

Every anti-fraud professional involved in iovation’s 4,000-plus community of users is intrinsically motivated to add the highest quality of evidence to iovation’s 55 million reports of fraud and abuse.

“We make sure that we only load evidence of confirmed fraud,” James asserts. “It’s not in anyone’s interests – ours, other iovation users, or iovation’s algorithms – to do otherwise. By keeping evidence quality high, we’re better able to keep bad devices from returning without impacting honest customers.”

Cashplus uses iovation for more than device recognition

Cashplus’s algorithm had a good capture rate before it began drawing data from iovation. After James rebuilt the algorithm to ingest iovation data, he has noticed a number of iovation’s data sources have become the most valuable risk indicators: the black box age, some of the risk scores, the presence of a proxy or a Tor exit node, for example.

“We couldn’t identify those without using iovation. They’re very useful,” James shares. “We use our application algorithm as a starting point for tracking each customer’s risk over the course of their lifecycle with us. Even when we accept some applications, the attached account may be in a higher risk category than it would be otherwise, as a result of our internal algorithms using iovation’s data. That helps us to detect and stop fraudulent efforts faster.”

—

For more case studies visit **iovation.com/resources**

Get in Touch

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

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 multifactor authentication methods, iovation safeguards tens of millions of digital transactions each day.

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