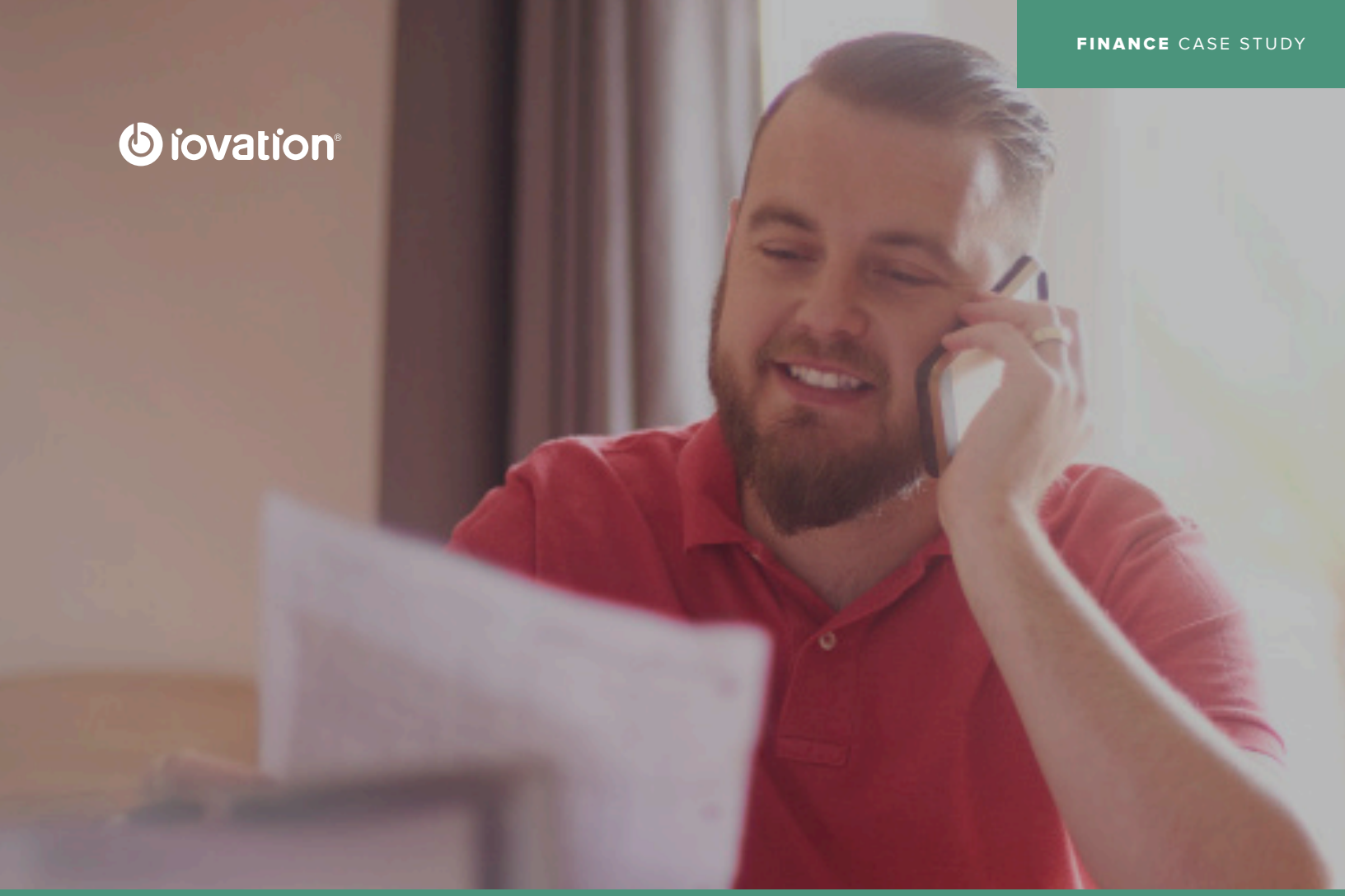
iovation®



IKANO BANK CASE STUDY

IKANO BANK UK SIGNIFICANTLY REDUCES IMPERSONATION FRAUD WITH IOVATION DEVICE INTELLIGENCE

CHALLENGES

Ikano Bank sought to protect their customers from romance fraudsters without having to sacrifice the simplicity of their service offering, a major value proposition and point of differentiation.

SOLUTIONS

Ikano Bank implemented iovation's online fraud prevention and detection solution. By identifying every device visiting their loan application page, Ikano can assess each device's reputation and association with other devices.

RESULTS

Within six months of implementation, iovation stopped almost every instance of the impersonation-based fraud Ikano Bank was suffering, yielding an 850% ROI over that timeframe.

IKANO BANK

Born out of IKEA, Ikano Bank was founded on the principles of value and simplicity. Fraudsters have taken notice, making it even more important for Ikano's fraud department to identify potential scams before approving and fulfilling loan applications.

"One customer was so deep into the scam that we called the police to intercede," recounts Eddie Vaughan, UK Fraud & Financial Crime Manager at Ikano Bank. "Banks and their customers are increasingly prone to a variety of scams in which fraudsters prey upon individuals who are particularly vulnerable. Romance scams have been effective for decades now but have been updated to the Internet age – we've seen some people who have been close to selling their homes to raise money to pay an online boyfriend or girlfriend they've never actually met."

"Our online personal loan product makes it easy to quickly pay a sum of money into the bank account of someone whom we've never met," Eddie explains. "While our customers love the simplicity and speed of this product, scammers can also benefit. It was imperative for us to do everything we could to prevent fraudsters from taking out loans using honest people's personally identifiable information."

A new take on an old scam

Many of the most common Internet scams actually pre-date the Internet. For instance, romance scams have been around in some form since the dawn of pen pals. But the ease in which the Internet connects people, combined with sophisticated social engineering skills, has made it that much easier for fraudsters to separate their marks from their money.

Online dating sites have become an especially rich source for these types scams. Fraudsters trick their victims into divulging their Personally Identifiable Information (PII), which the fraudsters then use to take out loans from lenders.

Other solutions couldn't help.

Initially, Eddie and his team fought back with cookie matching and a private fraud aggregation network for UK lenders.

"Once we realized we were dealing with a sophisticated fraud ring, we had quite a bit of difficulty in finding the data that would establish the size of the problem," recalls Eddie.

The Ikano Bank fraud team built a database of the browser cookies associated with the fraudulent loan applications; an extremely time-consuming and fragile process. Any device used to submit the applications could clear its browser cache at any moment. The next time it submitted a loan application, that 'new' device would carry an innocuous cookie.

The private fraud aggregation network for UK lenders wasn't much better as the fraudsters were using advanced tactics that successfully circumnavigated traditional methods of identifying fraud. Due to these limitations, Eddie's team received an unacceptable number of false positives, consuming too much time and frustrating legitimate customers.

AS SOON AS WE BEGAN TO CONSIDER DEVICE RECOGNITION TECHNOLOGY TO STOP THIS FRAUD RING, IOVATION WAS AT THE TOP OF OUR LIST. AMONG LENDERS, IOVATION HAS A REPUTATION AS A MARKET LEADER. I KNEW I NEEDED IOVATION'S HELP.

Eddie Vaughan, UK Fraud & Financial Crime Manager, Ikano Bank

Ikano Bank turns to iovation for help.

iovation's device recognition technology uses thousands of permutations of device attributes to identify every phone, tablet and computer visiting Ikano Bank's loan application page instantly, and recognize them over time with persistent device IDs. With real-time access to more than four billion device IDs in iovation's global database, Ikano Bank gained instant visibility into the reputations and associations of the devices accessing its digital properties.

Once Ikano Bank had iovation's FraudForce solution implemented, Eddie and his team began to place evidence of fraud against the offending devices in iovation's Intelligence Center, the world's richest device reputation database. From then on, devices used to submit fraudulent applications could be flagged for review automatically. No combination of cookie clearing, IP spoofing, use of Tor or proxies, or other tricks can fool iovation.

Immediate and decisive results.

"We implemented iovation in the fourth quarter of 2016. Results appeared immediately. It was huge," says Eddie. "By the end of the quarter, we'd reduced our fraud losses from impersonation by 72%. By the end of Q1 2017, we stopped almost all impersonation attempts."

AS LONG AS PEOPLE CAN BE TRICKED INTO DIVULGING THEIR PRIVATE INFORMATION TO FRAUDSTERS, WE WILL BE AT RISK FOR IMPERSONATION FRAUD. THE VICTIMS' APPLICATIONS AND BANK ACCOUNTS WILL CHECK OUT. WE ARE NOT IMMUNE, BUT IOVATION CERTAINLY HELPS US TO MANAGE THAT RISK TO THE GREATEST EXTENT POSSIBLE.

Eddie Vaughan, UK Fraud & Financial Crime Manager, Ikano Bank

As a result of the savings from stopping that impersonation fraud, Eddie estimates that iovation yielded an ROI of 850% over those first two quarters alone. Now that the fraud ring has been stopped, this impressive ratio has corrected, but Ikano Bank definitely intends to keep iovation in its set of fraud-fighting tools.

Since implementation, Eddie says iovation has:

- helped Ikano Bank to identify more fraud every day;
- increased the amount of time his fraud team has to decide how to treat new, questionable applications;
- cut through the 'noise' of conflicting data provided on applications;
- slashed false positives; and
- supported a more data-driven approach to their investigation of suspected fraudsters.

"Looking ahead, we're asking ourselves how we can use iovation's data in other ways," says Eddie. "We're learning to integrate evidence from other iovation users into our decisioning process. We expect it will help us uphold our responsibilities for Anti-Money Laundering and Countering Terrorism Financing. And we are beginning to explore how iovation's data can help us understand our customers better, and identify bad debt behavior faster."

ABOUT IOVATION

iovation protects online businesses and their end users against fraud and abuse, and identifies trustworthy customers through a combination of advanced device identification, shared device reputation, customer authentication and real-time risk evaluation.

More than 4,000 fraud managers representing global retail, financial services, insurance, social network, gaming and other companies leverage iovation's database of more than 3 billion Internet devices and the relationships between them to determine the level of risk associated with online transactions.

The company's device reputation database is the world's largest, used to protect 23 million transactions and stop an average of 300,000 fraudulent activities every day.

The world's foremost fraud experts share intelligence, cybercrime tips and onlinefraud prevention techniques in iovation's Fraud Force Community, an exclusive virtual crime-fighting network.

Global Headquarters

iovation Inc
111 SW 5th Avenue, Suite 3200
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

www.iovation.com

iovation®