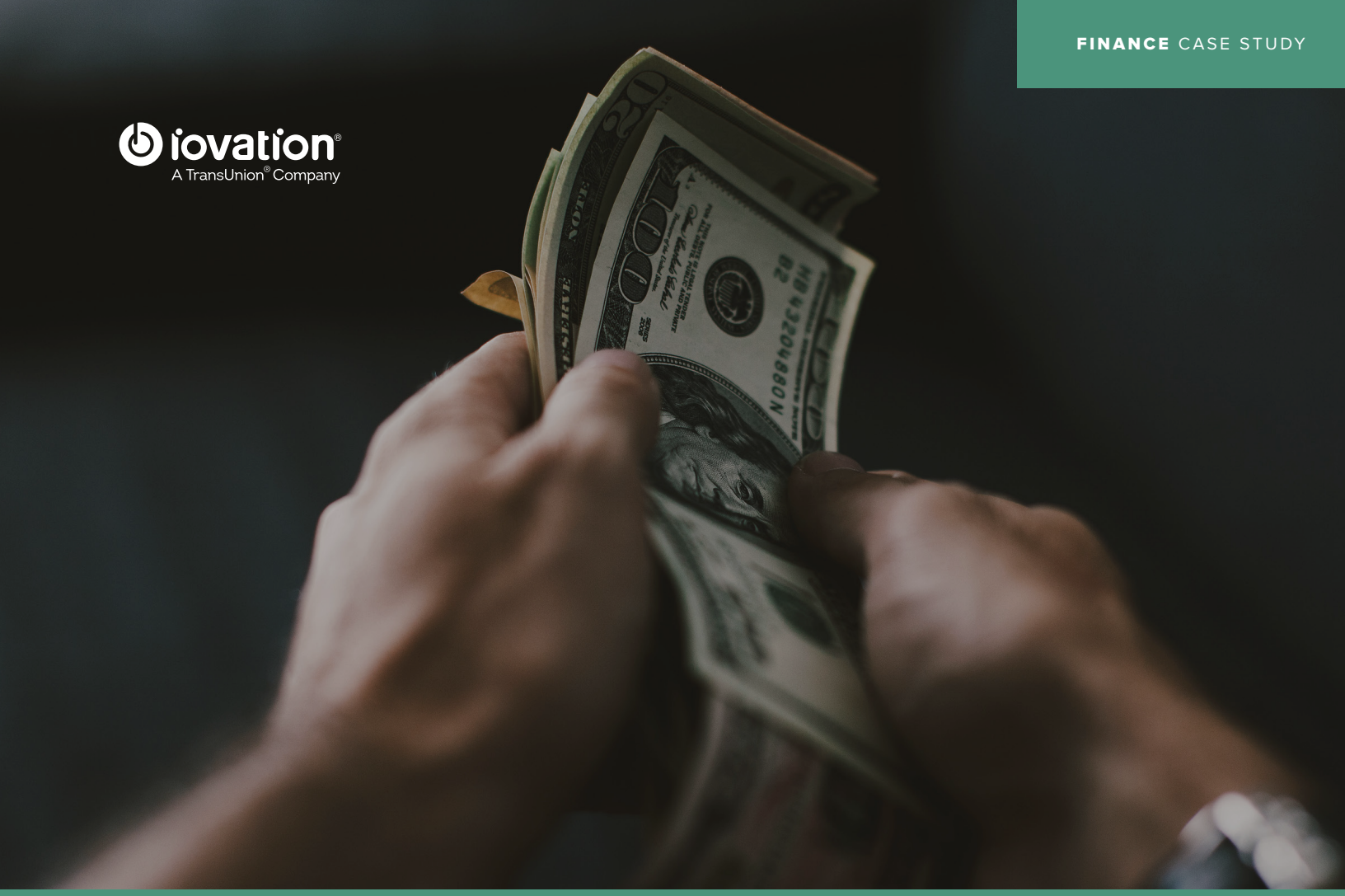
iovation®
A TransUnion® Company



CASE STUDY

CREDIT UNION ENJOYS ROI FROM FIRST PREVENTED FRAUD APPLICATION

CHALLENGES

With fraudsters using clean fake identities to create new accounts, the credit union had difficulty knowing which customer applications to trust, resulting in deepening manual review queues.

SOLUTIONS

iovation helped streamline the manual review process by fine-tuning automated business rules, and identifying fraud and high-risk transactions showing specific device characteristics.

RESULTS

The credit union saw immediate ROI by stopping more than $1M in fraudulent applications a month and reducing review processes from hours to minutes.

DELUGE OF FRAUDULENT APPLICATIONS THREATENED TO OVERWHELM REVIEW QUEUE AND FRAUD TEAM, UNTIL IMPLEMENTING IOVATION.

Fraud analysts' work at credit unions was never easy. Unfortunately, the steady cascade of data breaches have amplified the torrent of fraudulent consumer loan applications. Because fraudsters can easily buy their victims' personal identifying information, they can submit squeaky-clean loan applications.

This credit union's fraud review process had grown organically over the years in response to the changing threat landscape. Although they noticed suspicious similarities between some applications, they had no way of verifying connections.

When reviewing suspicious applications, a fraud analyst would send a letter to the applicant requesting some mix of: a phone call, a notarized copy of identification, pay stubs, proof of residence, etc. Each of those earnest requests served the fraudsters' dishonest objectives; they would discover what documents they would need to counterfeit for the next batch of applications.

"Some documents were easily detectable," says 'Jane,' a fraud leader at the credit union. "But some were very well done, leaving us wondering whether to approve the loan. And if the applicant didn't return the requested information, we would be left wondering if we'd turned away good business, or if we'd inadvertently helped fraudsters to apply to other institutions."

Fraud review process ate into operational efficiency

Before iovation, up to three departments would review the same application for signs of fraud. First, the receiving call center or loan center would put questionable applications through a third-party tool. If the application advanced to the lending department, but raised suspicions there, that group would examine the application with similar tools.

If the application still raised red flags, it'd go to the Fraud department, which would take a closer look, says Jane. "The most suspicious applications could take more than eight hours

of review by multiple staff members. Even worse, we still might not put our fingers on definitive indicators of fraud."

Jane knew there had to be a better way. By tracking averted losses, she wanted to show that the fraud department could be more than the traditional cost center, that it could save the credit union money.

IF THE APPLICANT DIDN'T RETURN THE REQUESTED INFORMATION, WE WOULD BE LEFT WONDERING IF WE'D TURNED AWAY GOOD BUSINESS, OR IF WE'D INADVERTENTLY HELPED FRAUDSTERS TO APPLY TO OTHER INSTITUTIONS.

Reputation for excellence attracts fraudsters

Founded several decades ago, with numerous locations in the United States, this credit union employs hundreds, and manages over US$1bn in assets. "Credit unions are not-for-profit financial cooperatives," says Jane. "We exist to serve our members, not to make a profit. We can't afford to risk their money. The more fraud we can prevent, the more our customers benefit."

Before iovation, the credit union didn't know with certainty the geographic nor IP origins of its loan applications, nor the number of computer applications each loan was connected to. In many cases, there was no clear relationship between true IP, geographical area and application velocity.
If they could gain this insight, they could avert more fraud and streamline their review process: two monumental wins.

Why they added iovation to their anti-fraud stack

iovation's FraudForce collects numerous details about the devices used to complete loan applications, including app information, device attributes, geolocation, system information, and much more. Once a device is identified, iovation checks for prior evidence of fraud (on the current device and any associated devices), and seeks out anomalies (e.g. an unusually high velocity of transactions).

Following configurable business rules set by the user, iovation returns in real time an Allow, Review or Deny recommendation, a weighted risk score, and a detailed report of the device's details that can be useful for forensic investigations.

By integrating device intelligence with another platform such as an identity authentication solution, iovation partners can provide a multi-tier strategy for fighting online and mobile fraud. When the behind-the-scenes device reputation check occurs early in the process, there's less need for step-up authentication challenges. This improves the customer experience and frees fraud teams to focus on the riskiest transactions, shortening review queues and improving operational efficiency.

"We started seeing results immediately"

The credit union's multi-stage implementation of iovation finished in March, 2015. As they progressively added iovation to the application process for credit cards, auto loans, and other consumer products, they gained the insight they'd been missing. Upon completing integration, the credit union identified numerous illegal third-party brokers, fraudulent applications using personal information acquired from data breaches, and much more.

Between April and June, 2015, the credit union has averted more than one million dollars' worth of fraudulent applications each month.

"This is strictly related to iovation's service," says Jane. "Usually 10% of our online consumer loan applications get kicked out for review by iovation. Of that 10%, 40% are revealed as fraudulent. That's the basis for how I calculate iovation's results, and for my argument that the fraud department isn't a cost-center.

Review queue shrinks to manageable size

Before, the fraud department could only pick up an application's stated IP address, which can be spoofed easily. With iovation, they can compare the stated and actual IP address, and the distance between the two: from devices hundreds of miles apart, to the exact same device. Armed with these and dozens of other risky device characteristics, automated decisioning in the lending and fraud departments has made the review process much more efficient.

IF WE HAD ONLY EVER CAUGHT ONE LOAN, IOVATION WOULD HAVE PAID FOR ITSELF.

As the credit union finds applicant- and device-connections on fraudulent loans, they add evidence to iovation's industry-leading database. They also selectively use evidence supplied by other financial institutions. With this selectivity, they can deny the worst applications automatically.

"We have been able to identify many more fraudulent applications using iovation and with less second-guessing," says Jane. "Now, each application that makes it to review takes about five minutes for one department, down from hours for three departments. It's a lot more streamlined.

We only request additional information from applicants that make it to our review queue. We don't waste time on applications that iovation denies."

"All credit unions need iovation"

Though Jane was an advocate of iovation from the moment she first heard about it, the fraud department -hampered by the old review process- worried that the solution would just add one more level of complexity to its workflow. Today, they're the ones who've found more value from iovation than anyone else. They've become such big proponents that they're exploring how they can add iovation to new membership applications and account logins.

Over the summer of 2015, the credit union's fraud department hosted a roundtable event for other fraud departments from regional credit unions. They invited iovation to present to get more institutions signed up, says Jane.

WE WOULD LOVE FOR MORE CREDIT UNIONS TO JOIN THE PLATFORM, SO WE'D ALL HAVE A LARGER POOL OF EVIDENCE AND MORE EFFECTIVELY DENY FRAUDSTERS.

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