



NTRUST CASE STUDY

PUTTING SECURITY FIRST IN PEER-TO- PEER MONEY TRANSFERS

CHALLENGES

With the rising popularity of digital cash transfers attracting cybercrooks, member accounts had to be secured to protect against account takeover and payment fraud, leading to high volumes of manual reviews that overwhelmed internal resources.



SOLUTIONS

Using a consortium model that provides deep insight into device reputation and behavior, the solution flagged risky transactions in real time, based on nTrust's custom business rules, without impacting the user experience.



RESULTS

Mobile SDKs for Android and iOS apps helped reduce fraud by 75%, and reduced customer friction to ensure a seamless user experience for good users. Plus, by stopping fraud at login, downstream damage was prevented.



NTRUST IS A CANADIAN-BASED REGULATED AND TRUSTED GLOBAL PEER-TO-PEER (P2P) MONEY TRANSFER PLATFORM DESIGNED TO FREE ITS MEMBERS' MONEY BY UPLOADING IT TO THE CLOUD.

nTrust's Cloud Money service enables money transfers around the globe as fast and seamless as sending a text. nTrust members can pay with their phone at retail shops and boutiques, food trucks, breweries, salons and other businesses that accept nTrust. Members can also use nTrust to split the bill, load money to a prepaid card, securely send money, collect payments and make bank deposits, and receive payments from anywhere in the world.

Providing a safe and secure mobile transfer service means teaming up with a trusted fraud prevention partner with a proven track record for keeping bad actors out.



WITH IOVATION'S FRAUD PREVENTION SERVICE, WE HAVE THE DEVICE-BASED INTELLIGENCE WE NEED TO QUICKLY APPROVE GOOD ACCOUNTS AND DIGITAL CASH TRANSFERS, WHILE STOPPING CYBERCRIMINALS IN THEIR TRACKS. WE HAVE GREATLY REDUCED FRAUD LOSSES AND OUR MANUAL REVIEWS ARE NOW AT A MANAGEABLE LEVEL.

Angela Biener, Chief Operating Officer

Digital Cash Adoption Sparks Fraud Concerns

nTrust lets customers send money instantly from any location using a smartphone, tablet or computer. The service works across platforms and uses both Android and iOS apps. As digital cash adoption soars, so does cybercriminal activity

in the form of identity theft, payment fraud and account takeover attempts.

Fraudsters target money transfer services to open up accounts using stolen credit cards, add money, and then quickly transfer the money out. This can also come in the form of friendly fraud with two friends or relatives work together to incur charges and then claim they are fraudulent. Since p2p accounts are generally linked directly to checking accounts and money can be moved in under a minute, account takeover protection is a necessity.



TO USE THE SERVICE, MEMBERS SIMPLY ADD FUNDS TO THEIR ACCOUNT, START THEIR PURCHASE OR ORDER, AND LET THE CASHIER KNOW THAT THEY ARE PAYING WITH NTRUST.

Shared Global Intelligence to Stop Financial Fraud

After evaluating multiple vendors in the fraud and security space, nTrust was attracted to the advanced sophistication of iovation’s device recognition technology and innovation of determining a device’s reputation. Having access to iovation’s globally-shared consortium of 5 billion devices and 55 million client-reported fraud records meant they would be armed with intelligence upfront to help evaluate risk in real-time.

“We needed a strong device recognition element in our fraud strategy. We searched for a service flexible enough to work in tandem with our in-house platform that was accurate, easy to use, and provided deep insight into device behavior and reputation,” said Biener.

A major advantage of iovation was that nTrust could integrate fraud and abuse records into their own in-house system. With some of the largest, most recognizable global brands contributing to the iovation consortium in banking, retail, shipping, telco, travel and other industries, nTrust chose to more heavily weigh fraud evidence from other financial institutions in their business rule setup, since they share similar fraud concerns.

“We trust the information shared by other iovation clients about the fraud behaviors they’ve seen across groups of devices. There’s huge value for us in having real-time access to a device’s reputation within the fraud community, and that has allowed us to greatly cut fraud losses and reduce review queues,” said Fraud Management Specialist, Darcy Berringer.

iovation has over 45 specific types of fraud and abuse that can be marked on an account to give clients specific insight into the type of fraud that has been noted. This level of granularity is important because it gives users the ability to weight fraud types differently based on their relevance to the specific business and industry.

Customize Device Recognition for Your Unique Needs

nTrust has taken a unique approach to using iovation’s shared fraud intelligence for evaluating and making decisions about the risk level of transactions. In order to mitigate manual reviews and to provide 24/7 fraud protection, nTrust’s internal system uses iovation’s business rules to flag and rate the shared evidence and then automates a response.

“iovation’s business rules editor gave me the flexibility to create rules based on nTrust’s own evidence of fraud plus the shared evidence from other iovation clients. I’ve been able to customize business rule sets for different integration points across our site and mobile apps to thwart new attacks, adjust for seasonality, or change business rule settings for other reasons,” said Darcy Berringer.

nTrust created three levels of business rules: high, medium and low based on shared fraud records. Their in-house system pulls in iovation’s business rules when they’re triggered. If hard evidence of fraud has been placed on a device by another client, it will be routed into the high business rule and the transaction will be stopped in real-time before they are completed and then reviewed.

“Since we have iovation integrated at login, their device intelligence helps us stop fraudsters before they ever get into an account and do any damage. There’s nothing we like more than shutting down a fraudster,” said Biener. “The iOS and Android SDKs for our mobile apps add even more power to helping us pinpoint bad actors and keep them out. All in all, we’ve reduced fraud by 75% and our operational efficiencies and customer experience has improved greatly.”

Cutting down on customer friction is an important part of the approach that nTrust has adopted. They are savvy about basing their decisions regarding risk on whether an account holder is brand new to them or fully verified. iovation is able to help fine-tune these assessments by providing specific information about whether a device has been directly involved with fraudulent behavior, or indirectly associated with fraud, and that precise data is taken into consideration in their automated evaluation of risk. The powerful combination of nTrust’s in-house platform and iovation’s risk service makes it possible to stop fraud before it happens. “Keeping our members’ accounts safe and secure means happy customers and happy employees,” said Biener.

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