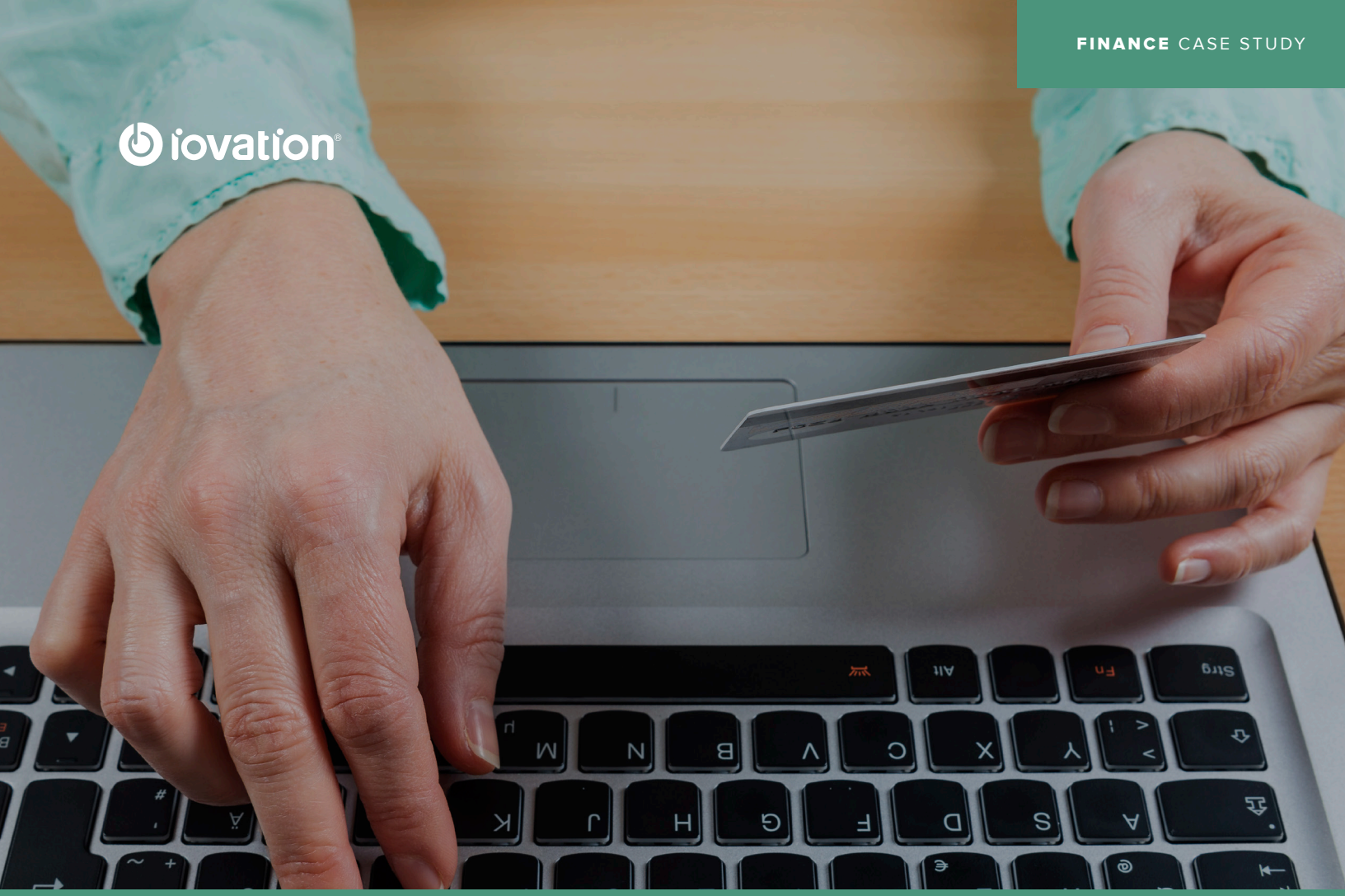
iovation®



UMB BANK CASE STUDY

UMB BANK STOPS FRAUD IN CREDIT CARD APPLICATIONS

CHALLENGES

With fraudsters applying for credit using stolen identities and risky transactions coming in from a range of geographies, it was difficult for UMB to know who to trust online.

SOLUTIONS

By leveraging device recognition, device reputation, link analysis and pre-set alerts, the bank was able to tie related accounts and devices together, and better understand each applicant's true location.

RESULTS

Using a proactive approach, UMB was able to stop bad actors at the front door, expose and stop a Florida identity theft ring, and realize a 100% reduction in fraudulent credit applications.

IOVATION DEVICE INTELLIGENCE STOPS CRIMINALS AT THE FRONT DOOR AND LEADS TO 100% REDUCTION IN FRAUDULENT CREDIT APPLICATIONS.

From a storefront bank in Kansas City, Mo., with first-day deposits of $1,100 in 1913, UMB Financial Corporation has grown to become a diversified financial services holding company with multi-billion dollar assets. The company has a long tradition of providing outstanding customer service and its associates shared mission includes knowing their customers, anticipating their needs and acting as their advocate. This commitment to service also means keeping customers safe from cybercriminals with advanced fraud protection that works behind the scenes and providing a seamless user experience.

SINCE WE DEPLOYED IOVATION, WE HAVE NOT EXPERIENCED FRAUD LOSSES RESULTING FROM A CREDIT CARD APPLICATION FLAGGED BY IOVATION.

Cristina Koder
Check Fraud Operations Supervisor

Financial institutions are obvious targets for cybercriminals, especially when they offer consumer credit online. Organized fraud rings are out to make big profits using stolen or synthetic identities on these application platforms. UMB was no exception and they knew they needed a strong, multi-layered strategy to protect their customers and brand reputation.

After evaluating best-in-class fraud prevention solutions used at major financial institutions, UMB settled on iovation Fraud Prevention. This allowed them to tap into the shared knowledge within iovation's cybercrime intelligence network of more than 2 billion Internet-enabled devices (such as laptops, tablets and mobile phones) and 22 million fraud and abuse reports. Knowing that criminals quickly move from business to business, UMB wanted immediate knowledge of when bad actors began interacting with their website or banking app.

"The typical abuse that we see attempted over and over, is fraudsters using stolen identities to open new accounts," said Koder. "While people continue to try and commit fraud, there's no question that iovation is a fantastic tool in stopping them from getting through both the online and mobile application process. The Fraud Prevention solution provided by iovation allows UMB to prevent fraud every single day. That, in turn, helps keep our customers protected, engaged and satisfied."

Shared Intelligence to Stop Fraud Rings

UMB uses iovation to uncover cybercriminals working on their own and in fraud rings. Cybercriminals often band together in organized groups in order to defraud businesses and consumers. By the same token, iovation's risk service includes 3,000 global fraud professionals banding together and sharing intelligence to prevent online fraud from happening on their sites in the first place.

Device reputation is a combination of real-time risk uncovered (such as velocity thresholds exceeded, a risky profile match, or evasion techniques uncovered) and client-reports of specific types of fraud and abuse. UMB can choose to look at up to 45 specific types of fraud in the iovation service (such as credit card fraud, identity theft, and account takeovers). This granular level allows businesses to consider the type of evidence that is most relevant to their situation or industry. The information (along with an allow, review or deny response) is returned by iovation within a tenth of a second.

I FIND IT MOST HELPFUL TO LOOK AT THE FRAUD EXPERIENCES FROM MAJOR FINANCIAL INSTITUTIONS IN THE IOVATION NETWORK. IF OTHER FINANCIAL CLIENTS HAVE MARKED AN ACCOUNT, AND BY ASSOCIATION A DEVICE, WITH FINANCIAL FRAUD OR IDENTITY THEFT, I WEIGH THAT VERY HEAVILY IN MY REVIEW PROCESS.

Cristina Koder
Check Fraud Operations Supervisor

Identifying Location Anomalies

UMB finds iovation's Real IP and geolocation features extremely effective in fighting identity theft within their credit card applications. Real IP tells them where the site visitor is coming from and the geolocation data offers country, the stated and 'real' IP address, latitude and longitude. Transactions can be flagged appropriately based on the proxy used, or a watch list or block list can easily be set up through business rules.

"Anomalies are something we always track. An example would be a mismatch between the time zone and location or browser language and IP address," said Koder. "Being alerted to anomalies upfront, we can investigate the legitimacy of the identity. When we uncover that it's a stolen identity, we contact the real identity owner and help them get on the right path to mitigate the damage most efficiently."

The value of the Real IP and geolocation feature was underscored for UMB when they were able to use it to identify and stop a fraud ring operating out of Florida.

"Fraudsters will purchase every piece of personally identifiable information on a victim, including name, address, birth date, and social security number. It all looks perfect on paper and matches the credit bureau information exactly," said Koder. "Those are the most dangerous applications that we see. We have not experienced fraud losses resulting from a credit card application since we deployed iovation. Stopping fraud is why I come to work every day. The success we've had from using iovation is very rewarding."

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 3,500 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 16 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®