TransUnion

CASE STUDY

UMB Bank

A diversified financial services holding company with multibillion-dollar assets.

100%

UMB Bank realized a 100% reduction in fraudulent credit card applications.

"We have not experienced fraud losses resulting from a credit card application since we deployed TruValidate™ Device Risk. Stopping fraud is why I come to work every day. The success we've had from using TruValidate is very rewarding." – Cristina Koder, Check Fraud Operations Supervisor, UMB

SCENARIO

UMB 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. Fraudsters and fraud rings were applying for credit cards using stolen identities, and risky transactions were coming in from a range of geographies. UMB knew they needed a strong, multilayered strategy to protect their customers while reducing fraud.

STRATEGY

After evaluating best-in-class fraud prevention solutions at major financial institutions, UMB chose TransUnion's TruValidate. Implementing TruValidate Device Risk, UMB tapped into its cybercrime intelligence network of more than 9 billion Internet-enabled devices and 83 million fraud and abuse reports. They also gained insight from nearly 5,000 global fraud professionals sharing intelligence to prevent online fraud. The Real IP and geolocation feature of Device Risk enabled UMB to identify location anomalies that indicate potential fraud. Knowing that criminals quickly move from business to business, UMB implemented TruValidate to get immediate knowledge of when bad actors began interacting with their website or banking app.

RESULTS

Using TruValidate to proactively monitor transactions, UMB was able to stop bad actors at the front door. Devices with questionable reputations are immediately stopped from creating a new account enabling UMB to realize a 100% reduction in fraudulent credit card applications. In addition, UMB was able to utilize geolocation intelligence to expose and stop a Florida-based identity theft ring.

"While people continue to try and commit fraud, there's no question that [Device Risk] is a fantastic tool in stopping them from getting through both the online and mobile application process." –Cristina Koder, Check Fraud Operations Supervisor, UMB

TruValidate provided insight to potential fraud based on the risk profiles of the devices being used to submit credit card applications, including:

- Real-time risk uncovered – such as velocity thresholds exceeded, a risky profile match, evasion techniques uncovered, and client reports of specific types of fraud and abuse.
- Up to 45 specific types of fraud in the TruValidate service, such as credit card fraud, identity theft and account takeovers.
- Geo/IP checks indicating where the site visitor is coming from including country, the stated and "real" IP address, and latitude and longitude.

Protection for their customers and their business.

"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," says Cristina Koder, Check Fraud Operations Supervisor at UMB. "Those are the most dangerous applications that we see. Since we have deployed Device Risk, we have not experienced fraud losses resulting from a credit card application flagged by TruValidate."

Learn more about our identity insights, digital insights, omnichannel authentication and fraud analytics. Contact your TransUnion representative or visit:

transunion.com/truvalidate