TransUnion

CASE STUDY

Telecom Provider

One of the largest telecom providers in the US

83M

This telecom provider is protected by TruValidate and its cybercrime intelligence network of 83 million fraud and abuse reports.

"I call it a golden age of fraud. As far as account takeover is concerned, I don't think we've been in this good of a position for a year and a half. Whether customers place an order or change their contact information, we can protect and analyze the entire journey."
– Toby Ceselski

SCENARIO

The telecom company's previous authentication solution produced a flow of false positives with no rhyme or reason; at times it would challenge a customer from a familiar, unique IP address; other times it would fail to stop logins from foreign IP addresses. Some users would encounter not one but two two-factor authentication challenges on certain portions of its website. Customer complaints increased, but there was no way to investigate the root cause of the issue because the authentication solution provided so little detail.

STRATEGY

The telecom provider implemented TruValidate™ Device-based Authentication for seamless two-factor authentication. Device-based Authentication added the critical ingredients of context and risk to the telecom provider's customer-facing authentication solution. The TruValidate patented recognition technology uses hundreds of device attributes and their unique orientation with each other to instantly identify each device without needing any of the customer's directly identifiable personal information.

RESULTS

Device-based Authentication provides the information needed for the company to recognize devices and act accordingly. Along with richer detail have come more nuanced and configurable rules; now the telecom provider can use TruValidate's powerful rules engine and risk policies to determine exactly how Device-based Authentication responds to trusted customers, specific threats and detected anomalies. Customer complaints about the login experience dropped, and password-based attacks and account takeover are no longer a problem.

"Password-based attacks such as credential stuffing aren't much of a concern. We know fraudsters aren't getting around Device-based Authentication at login."

– Toby Ceselski

Device-based Authentication's highly configurable key capabilities include:

- Device registration to affirm user identity by matching device fingerprints with a high degree of accuracy
- Device Change Tolerance to account for natural drift caused by updates, new apps or even new fonts
- Passwordless Authentication to enable the user's device to serve as the primary authentication factor. Passwords or other secondary authentication factors can be reserved for cases where a customer logs in from a device for the first time or presents an elevated-risk profile
- Evasion Detection to pierce proxies and detects proxy servers often employed by fraudsters and scammers while leveraging advanced techniques to unmask TOR networks, mobile VMs, emulators and other anonymizing activity

Providing smoother transactions while protecting against fraud

With Device-based Authentication protecting the login experience, the telecom's fraud team is helping to make transactions easier. "With the amount of data available to us in real time, we will be able to create more granular rules and logic to keep fraudsters at bay while reducing customer friction," says Toby Ceselski, Business Data Analyst III with the telecom's Fraud Department. "Our customers are going to love it."

Learn more at:

transunion.com/truvalidate