TruValidate

Telecom

Case Study

Major US Telecom Provider Improves Customer Login Experience With Device-Based Authentication

Challenge

Previous authentication solution produced a flow of false positives but starved the Fraud department of data. Customer complaints increased. There was no way to investigate the root cause of the cases.

Solution

The telecom provider – already succeeding with TruValidate Device Risk – decided to transition to TruValidate Device-Based Authentication for seamless two-factor authentication. The switch unlocked significantly more data for the Fraud team.

Results

The Fraud team works closely with the Customer Care team to streamline the login experience for website users. Customer complaints about the login experience dropped. Password-based attacks and account takeover (ATO) are no longer a problem.

Transition to TruValidate Device-Based Authentication prevents account takeover attempts while reducing complaints to customer care

It's a modern love story. Customer meets fraudster on a dating site. Fraudster earns customer's trust and requests login credentials to account at major telecommunications provider.

Fraudster orders four new iPhones by opening four new lines on customer's account. Payment becomes a chargeback.

Fraudster disappears. Customer cancels the four new lines. Telecom provider loses thousands of dollars in product and service revenue.

"Because of the fraud levels we used to see, our IT department put up a digital wall," explains Toby Ceselski, Business Data Analyst III at this telecom provider. "Some users would encounter not one but two two-factor authentication challenges on certain portions of the website. Compared to our position now, we were putting these customers through a needless hassle."

The telecom provider had been using an authentication solution for several years. They were ready for a change.

"We weren't driven away from the previous authentication vendor by a fear of password-based attacks," Ceselski explains. "It was more about our customers' experience. In the last six months of that contract, we were impacting many more visitors than we should have been."

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.

Toby Ceselski,
Business Data Analyst III,
Fraud Department

Whether customers place an order or change their contact information, we can protect and analyze the entire journey.

The previous authentication vendor was flagging too many false positives. Legitimate customers called to complain about step-up authentication challenges at every login. Toby and his team had to correct the authentication vendor's mistakes manually.

"There was no rhyme or reason to the false positives," says Toby. "For example, the vendors product would challenge a customer from a familiar, unique IP address. At other times, it failed to stop login events from foreign IP addresses."

The underlying problem: limited data. The previous authentication solution was supposed to work as a learning system. Feedback from Toby and his team was supposed to teach the solution how to weight subsequent events.

"The previous solution was sold as a 'device-fingerprint solution,' but we couldn't get more than a username, the IP address, and the score assigned to the event," Toby remembers. "When we had an issue, we didn't have any detail with which to conduct a root-cause analysis. When we approached the vendor and got a preview of the upcoming version, we could see that we wouldn't get what we needed."

Need for greater volume and quality of data drove switch to TruValidate Device-Based Authentication

The Fraud team drove the change in authentication solutions. They could have their choice as long as it didn't impact customers. Preferably, the Customer Care team would receive fewer complaints about the login experience.

Toby knew he wanted to replace the authentication solution with Device-Based Authentication. "We'd been happy with [Device Risk] for several years by that time. We expected end-to-end visibility from login to checkout. Whether customers place an order or change their contact information, we can protect and analyze the entire journey."

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,
Business Data Analyst III,
Fraud Department

How Device-Based Authentication adds seamless two-factor authentication

Device-Based Authentication adds the critical ingredients of context and risk to the telecom provider's customer-facing authentication solution. TruValidate's 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.

Customers get an invisible, frictionless web experience by using their device as an additional factor of risk-based authentication. They can choose the devices they want associated with their accounts and used for authentication, or the telecom provider can register accounts and devices automatically on behalf of its customers.

Powerful risk insights allow the telecom provider to guard against indicators of ATO attacks, including device anomalies, spoofing, and evasion. New or suspicious devices attempting to authenticate may receive step-up challenges, enhancing existing authentication procedures without heavy lifting or intense coding.

"Our IT and Security teams supported our request to switch to [Device-Based Authentication]. Customer Care loved the prospect of fewer frustrated customers calling about their login experiences," Toby recalls. "My team craved the greater volume and quality of data that [Device-Based Authentication] would deliver."

All stakeholders benefit from Device-Based Authentication

"When we switched to [Device-Based Authentication], we got the information that we needed to automate more analysis and re-secure of compromised accounts," Toby shares. "Now, we recognize devices and act accordingly. No more vague scores to base our decisions on."

Along with richer detail have come more nuanced and configurable rules. With the previous authentication solution, Toby and his team could blacklist countries and whitelist known test accounts, but nothing else. Now, they can use TransUnion's powerful rules engine

[Device-Based Authentication] is definitely a viable and working solution for preventing account takeover at login. You will see improvement with it.

Toby Ceselski,
Business Data Analyst III,
Fraud Department

and risk policies to determine exactly how Device-Based Authentication responds to trusted customers, specific threats, and detected anomalies.

The transition to Device-Based Authentication has brought tangible results, according to Toby. "We're saving the company money. Along with helping to automate our efforts, [TransUnion's] TruValidate data has been effective at reducing our manual review queue. Many of our checks use logic based upon the data that we pull from TruValidate, data that we didn't get from the previous authentication vendor."

Toby's weekly reporting shows that Device-Based Authentication has improved the customer experience. In fact, Device-Based Authentication has increased collaboration between the Fraud and Customer Care teams.

"We've become more attuned to the customer experience," says Toby. "When we launched [Device Risk], we made a lot of hard denies to stem a wave of fraud. Now that [Device-Based Authentication] gives us a cleaner picture of the devices logging into our site, we've become more accommodating."

Looking ahead

With Device-Based Authentication protecting the login experience, Toby and his team are helping to make transactions easier. Instead of a blanket two-factor authentication experience for all customers, those using a trusted device will have a smoother risk-based authentication experience.

"We're re-thinking and re-architecting the way many of our customer flows work," says Toby. "In the future, 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. Our customers are going to love it."

—

For more case studies visit **transunion.com/truvalidate**.

Learn more about our identity proofing, risk-based authentication and fraud analytics solutions. Contact your TransUnion representative or visit **transunion.com/truvalidate**.

TransUnion

About TransUnion Global Fraud Solutions

TransUnion is a global information and insights company that makes trust possible in the modern economy. We do this by providing a comprehensive picture of each person so they can be reliably and safely represented in the marketplace. As a result, businesses and consumers can transact with confidence and achieve great things. We call this Information for Good.®

TransUnion Global Fraud Solutions unite both consumer and device identities to detect threats across markets while ensuring friction-right user experiences. The solutions, all part of the TruValidate suite, fuse traditional data science with machine learning to provide businesses unique insights about consumer transactions, safeguarding tens of millions of transactions each day.

transunion.com/business