Case study

Using device intelligence to prevent fraudulent account openings

The intrinsic value of device data in your fraud and identity strategy

Client

A leading financial services company offering end-to-end online banking solutions that enable clients to remotely create an account, apply for loans, create investment accounts and contribute to savings accounts.

Since this company doesn't have any in-person branches, maintaining a safe and convenient platform for clients to transact every day is crucial. That's why this company integrated our FraudNet solution in their fraud prevention strategy.

Challenge/Objective

This company's fraud team was extremely understaffed and was just beginning to build out their fraud strategy when they experienced unforeseen, high volumes of unusual account opening activity — the perfect storm for a large-scale fraud attack.

Since the financial services company recently implemented FraudNet, all new account openings on their platform were being monitored. FraudNet, our proprietary rules engine with device intelligence capabilities, inconspicuously collects hundreds of unique device attributes not easily spoofed by fraudsters. So FraudNet was able to identify suspicious applications and push alerts to the client's fraud team and our risk analyst. In this scenario, FraudNet flagged numerous applications that had high-risk ISPs and email domains. Since the fraud team was understaffed at the time, our risk analyst worked with the client to quickly identify the highest-risk applications.

Resolution

After some analysis, we identified the attack as a scripted attack — one in which fraudsters write a script to automatically generate thousands of new accounts. These attacks are common across not only financial services companies, but e-commerce and travel companies as well.

We also discovered that the fraudsters in this case may have been using a tool on the dark web to autogenerate names, addresses, emails, phone numbers, browser user strings and more. This gave the fraudsters an efficient and automated method to create synthetic identities. Synthetic identity fraud involves the combination of real and fake information to create a new identity, which is subsequently used to open fraudulent accounts and create fraudulent transactions.

Because the fraudsters used a script to create fictitious accounts, application volumes increased dramatically in a short time:

- Application volumes prior to the attack averaged around 19,000 per month. During the attack, the average increased 26 percent, to 24,000 applications per month.
- The attack rates prior to the scripted attack averaged 3.5 percent per month. During the attack, the average increased to 13 percent per month.

For a small fraud team, these numbers were daunting. Although the fraudsters created thousands of new accounts, they were unsuccessful in monetizing them.

Results

Thanks to our risk analyst's quick mitigation response, we were able to queue 23,800 suspicious applications for review. With an average loss of $1,500 across each new account opening in the banking industry, this client prevented an estimated $35.7 million in fraudulent funding. Any successful applications that may have turned into real accounts also were swept up by the same measures put in place for their FraudNet for Account Takeover use case, where all account logins are monitored. Through our risk analyst's vigilance and expertise in known bad device characteristics, the financial services company was able to act on this threat and execute an effective fraud strategy that gave them the time to work through the attack while understaffed.

However, the fight against fraud is ongoing. Our risk analyst continues to work closely with the fraud team to develop a layered fraud strategy to prepare against future attacks. The massive digital wave requires an integrated solution that recognizes consumers and detects fraud with every interaction — regardless of mobile, web, call center or offline channels. Device intelligence plays a fundamental role in protecting these channels and getting a holistic view of consumers.

Creating an effective fraud strategy requires the right combination across device intelligence, identity verification, alternative data and analytics.

Wondering what you should include in your fraud strategy?

Let's talk

Experian
475 Anton Blvd.
Costa Mesa, CA 92626
T: 1 888 414 1120
www.experian.com