CEQUENCE SECURITY

CUSTOMER CASE STUDY

Fast Growing Fintech Company Blocked Fraudulent Loans and Eliminated Burgeoning Fraud Costs

Fraud Team Leverages Cequence to Protect Their Loan Application Process

Lease-To-Own Fintech Company

An emerging fintech company that specialized in providing lease-to-own financing options to consumers had started to experience rapid growth. Consumers could use the financing to buy goods that could range from computers to furniture, enabled by an easy payment plan. The company's business model is centered around the concept that once the lease ends, the consumer owns the item outright. This fintech company partners with merchants to provide direct financing to each of their respective customers who apply for a loan.

The fintech company operates both a website and mobile app, providing consumers with multiple ways to access their service, apply for a loan, and obtain credit.

However, with the company's rapid growth and success came an increase in cybercriminal activity. Cybercriminals had discovered a perfect opportunity to commit financial fraud by exploiting this fintech company business model. The fintech company not only saw an increase in fraudulent loan applications but also an increased burden on internal fraud analysts that had to ensure that only legitimate applications reached the approval stage, in addition to denying fraudulent loan applications.

Sophisticated Phishing Campaign

More recently, cybercriminals orchestrated a phishing campaign against merchants who used the fintech company to help determine and approve loan applications from their clients. Cybercriminals were utilizing SMS phishing (Smishing) against merchants by sending them texts containing links to a fake webpage with a domain name similar to the fintech's domain. The fake webpage promised an award upon login for the merchant. The merchants would then log into the fake webpage, giving the cleartext username and password to the cybercriminals. Once the attackers authenticated to the real webpage, they were able to submit fake loan applications to their targeted merchant company that, if approved, would enable them to purchase expensive high-end items such as Apple products that were shipped to them at no cost.

What resulted was an increase in fraudulent activity, lost revenue, and a negative impact on their brand's reputation.

CUSTOMER PROFILE

A fintech company that specializes in providing consumer financing and lease-to-own purchase options to customers. Founded in 2012 in Salt Lake City, Utah, it has over 500 employees that support its operation. It has an estimated revenue of over $150 million per year.

Goals

- **Reduce Fraud Analyst Burden:** Reduce the number of hours spent by fraud analysts on each loan application.
- **Increase Accuracy:** Increase the accuracy and quality of analysis for each transaction, ensuring that mistakes were not made that delayed or blocked legitimate loan applications.
- **Loan Quality:** Ensure that only legitimate loans were submitted and processed, ensuring there were no delays due to manual fraud analysis.
- **Reduce Fraud Cost:** Reduce the cost of fraudulent loan processing that hit the company's expenses.

Fraud Analysts Were Exhausted

The existing process consisted of a team of fraud analysts sifting through every loan application to identify whether the application was legitimate or fraudulent. This caused an enormous burden on each analyst, which also acted as a bottleneck in getting applications processed on time. Worse, the process was less than perfect and fraught with inaccuracies, mistakes, and commitment of time. The fraud team was looking for another way to help them to eliminate fraudulent transactions and reduce the burden on internal analyses.

THE RESULTS

Streamlined Approval Process

The Cequence Unified API Protection (UAP) solution was introduced to the fraud team at the fintech company. Working together, Cequence helped the fintech company configure security policies through API Spartan, a UAP module that blocked all fraud traffic in days. After implementing API Spartan, the fintech company saw an immediate decrease in fraudulent loan applications. They were able to achieve the following results:

- **Fraud Analysts Productivity:** A reduction in the number of hours spent by each analyst on processing each application.
- **Decrease Loan Processing Time:** The amount of time spent on processing each loan application decreased, enabling customers to receive a response on loan approval much sooner.
- **Fraud Cost Reduced:** Due to blocking fraudulent bot activity, the fintech company saw an immediate reduction in the fraud costs impacting their bottom line.

What They Achieved

- 100% of fake applications were blocked.
- Blocked over 3,150 fake applications in a single attack.
- Saved over $3,150,000[1] in potential account losses.

1 Based on a $1,000 account loss per account based on the average cost of a single Apple iPhone value.