FingerprintJS Case Study

How a grocery delivery service prevented credit card fraud with FingerprintJS Pro

A grocery delivery service needed to prevent stolen credit cards from being used by new accounts without impacting legitimate users. FingerprintJS Pro's browser identifier increased fraud identification accuracy over their existing solution, reducing stolen card purchases and saving time on manual checks.

Results

Prevented stolen credit card purchases from fraudsters

The company was able to identify suspicious purchases before they happened by flagging visitors with multiple accounts or a history of fraudulent transactions.

Saved time spent on manual payment review

FingerprintJS Pro reduced false positives that would otherwise have to be reviewed by the company's internal fraud team.

Simplified rule management from previous solutions

FingerprintJS Pro's API and webhooks integrated easily into the company's existing anti-fraud system, with the increased accuracy allowing them to simplify previously complicated rulesets for flagging suspicious transactions.

Customer Overview

FingerprintJS began working with a fast-growing online grocery delivery service looking to prevent multiple forms of fraud. This multi-national company has both a web portal and a native app where customers can order items from local businesses to be delivered same-day to their door.

Sector: Online Delivery
Use Case: Payment Fraud
Employees: 1,000

FingerprintJS Features

- [x] 99.5% Accurate Identification
- [x] Browser Fingerprinting
- [x] GDPR and CCPA Compliant
- [x] Incognito Mode Detection
- [x] Geolocation

FingerprintJS

The Problem

Stopping credit card fraud

The company wanted to reduce fraudulent purchases from stolen credit cards. Typically, stolen credit cards were being used by new accounts created via the browser. The new user would make 1-3 fraudulent purchases and abandon the account. From analysing IP data and other browser signals, the company determined that much of the fraud was being done by users who already had multiple accounts with their service, and often had made fraudulent purchases in the past.

The company had built a sophisticated anti-fraud system that took into account a visitor's device, IP address, and browser fingerprint to flag suspicious purchases, however some fraudulent purchases were still falling through the cracks. The company found that the accuracy of their current fingerprinting solution was too low to catch all fraudulent activity, resulting in chargebacks, lost revenue, and a threat to their seller reputation.

Their anti-fraud system was also causing a number of false positives - transactions that were flagged as suspicious but were later found to be legitimate. Flagged transactions were blocked automatically within the web application only in extreme circumstances - typically flagged purchases were sent to an internal fraud analysis team to review. These false positives were taking up valuable time for the fraud department to review and dismiss.

Cleaning up legacy anti-fraud rulesets

From using multiple anti-fraud vendors, the logic to determine which purchases were suspicious and required review had become very complicated. The level of complexity made it difficult for the risk team to troubleshoot their own system and make changes.

The company started an internal rule management project to map out all of their individual rule triggers, and simplify the logic based on historical fraud data. If they were going to add an additional service to their anti-fraud tech stack, it needed to be easily integrated and unopinionated, allowing them to use their own rules logic and avoid introducing additional complexity.

Why FingerprintJS

As the company had already been working with several vendors for device identification, FingerprintJS had come up in their research into an additional accurate identifier that could be incorporated into their existing solution.

Successful pilot that improved accuracy of existing solution

After comparing FingerprintJS Pro with their existing browser identifiers, the company found that FingerprintJS Pro's visitorIDs were more accurate and made fewer false positives, which allowed them to improve their credit card anti-fraud workflows significantly.

Incorporation into existing workflows

Due to the company's philosophy of putting its customers first, it was essential to maintain users' rights to online privacy. FingerprintJS Pro is compliant with GDPR and CCPA for fraud detection. All customers of FingerprintJS can choose between US and EU hosted data centers to comply with their specific data localization and residency requirements.

FingerprintJS Pro's Javascript snippet also had minimal impact to browser performance, keeping the customer experience speedy and unhindered by new anti-fraud measures.

Get in Touch

Learn how FingerprintJS Pro can help your business build a custom solution to prevent online fraud.

Contact Sales

sales@fingerprintjs.com

Get Started Today

Create Account

FingerprintJS