FingerprintJS Case Study

How one sales software company exceeded third-party verification standards

The company was able to greatly increase their identity verification accuracy, prevent fraud committed by sales representatives, and exceed compliance standards.

Results

Reduced Fraud by 94%

One major customer of the company reduced fraudulent sales by 94% with FingerprintJS' high accuracy mobile device identification.

Integrated seamlessly with other security systems

Using FingerprintJS Pro's secure API, the company replaced their previous browser fingerprinting solution easily without disrupting existing security processes.

No disruption to customer experience

The new visitor identification process reduced fraud without increasing 'false positives,' protecting customers without causing unnecessary hurdles in the purchasing process.

Customer Overview

FingerprintJS works with a US-based door-to-door sales platform designed for retail energy sales. The company provides both software and hardware (tablets) for face-to-face sales representatives to manage their lead list and enroll new customers. The software also performs important security and compliance functions for the energy seller by ensuring data collected is accurate, secure, and compliant with state regulations.

Sector: **Energy Sales**

Use Case: **Third Party Verification**

FingerprintJS Features

- ☑ 99.5% Accurate Identification
- ☑ Browser Fingerprinting
- ☑ GDPR and CCPA Compliant
- ☑ Incognito Mode Detection
- ☑ Geolocation

FingerprintJS

The Problem

A key feature of the company's software solution is third-party verification (TPV), which is required by law for energy sales in many US states. When sales representatives enroll a new customer, the enrollee must confirm the sale was authorized and that they understand the plain-English terms and conditions of the sale. The company's platform streamlines the TPV process by texting the enrollee a link to a smartphone-optimized verification platform - a far easier process than competing solutions that require a lengthy call with a live agent or a phone recording.

To ensure that the confirmation link is sent to a legitimate customer and is not filled out by representatives seeking to claim commissions for enrolling non-consenting customers, the company wanted a sophisticated identity verification system. Their team designed a system with three layers of security:

- **Device Verification:** Ensure that the device and phone number that submitted the confirmation form is unique and legitimate using a combination of browser fingerprinting and a VOIP phone number checking service.
- **Signature Verification / Biometric Analysis:** Look for anomalies in submitted signatures and behavior on-page.
- **Customer Positive ID:** When the AI engine detects suspicious activity, ask the customer information that only they should know and verify against major credit bureaus.

When the company approached FingerprintJS, the company was using another open source browser fingerprinting library for their device verification layer. The company was looking to increase the accuracy of their fingerprinting, particularly on mobile devices, as they believed most instances of fraud could be prevented at the device and phone number verification stage.

Why FingerprintJS

After investigation, the company found that the FingerprintJS Pro API offered significant advantages to their previous fingerprinting solution, resulting in a more secure third-party verification process.

Higher accuracy for mobile devices

Many browser fingerprinting solutions struggle to accurately identify mobile visitors, as there are not enough unique signals to differentiate between users. For the company, reducing false positives was crucial to ensuring that legitimate customers could verify their enrollment quickly and easily.

For mobile devices, FingerprintJS Pro uses a combination of specialized signals to ensure the highest possible accuracy, including:

- Mobile network IP addresses analysis
- Mobile specific APIs (e.g. accelerometer)
- Mobile payment vendor information
- Mobile specific GPU signals (e.g. WebGL)

In addition to mobile browser fingerprinting, FingerprintJS Pro utilizes several server-side techniques like TLS analysis and SSL fingerprinting to increase the accuracy of visitorIDs, further reducing false positives.

Technical and Flexible Team

The company's engineering team worked closely with FingerprintJS to validate performance and optimize their installation. As the company had built a sophisticated verification system, it was important that their developers had easy access to technical support.

FingerprintJS Pro offers chat, email, and by-appointment phone support for all paid plans. As a developer-first company, our in-house support team consists of engineers with deep knowledge of our product.

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 Free Account

FingerprintJS