Case study

E-commerce client reduces fake accounts with fraud prevention

A noted e-commerce company discovered, after testing, that it could significantly increase fraud capture by running the AtData, an Experian company, Fraud Application Programming Interface (API), when users attempt to create an account during its sales process. Not only did they reduce the number of fake accounts being created, but they also used that data for future monitoring across the company.

The challenge

This company was experiencing high rates of fraud in its online sales, which invariably led to high chargebacks, account takeovers, identity theft and a massive increase in fake accounts. Because their fraud-detection processes were overwhelmed, their losses doubled as fraudsters deemed this site an easy target.

The solution

Vendor selection

In selecting their vendor and talking with our fraud experts, they had to determine the right solution to meet their needs and scale. The AtData team, an Experian Company, offered a comprehensive test solution, enabling the client to quickly see the product's benefits and accuracy prior to full integration.

Our solution was a natural fit because email was a critical data point in both account opening and guest checkout. By evaluating email addresses at these key customer touchpoints, the company was able to identify risk earlier and make more informed decisions without adding friction to the user experience.

How it works

Email fraud prevention services are designed to give you a holistic view of the email and automatically assess its risk.

Key to that process are the following factors:

- Fraud risk score: a machine learning model that assesses global metadata to determine email risk
- Date first seen: the date the email address first became active
- Longevity: a score indicating when the email address was first encountered
- Velocity: a score describing the level of activity of the email address over the past six months
- Popularity: a score reflecting the popularity of email across sources in the past 12 months
- Validation: flags invalid and risky email addresses through proprietary methods
- Domain check: blocks toxic or known high-risk domains
- Tumbling check: catches fraudsters using multiple variations of the same email address
- Fraud consortium: identifies fraudulent emails reported by our network

Case study

Anonymous e-commerce client

Email age, velocity, and popularity each provide valuable signals for evaluating risk and legitimacy. Combined with first-party customer data, these attributes help organizations distinguish trusted customers from potentially fraudulent activity. An AtData study published in 2025 found that high-risk email addresses were 25 times more likely to be associated with fraud, underscoring the value of email intelligence in risk assessment and fraud prevention.



Results

Most fraud prevention solutions are custom-fit based on the client requirements and the requirements of their customers. This e-commerce company emphasized its need to say yes with confidence and to quickly stop the surge in fraud it was experiencing. The client fully implemented the AtData Fraud API in their frontend registration page within two weeks and was immediately able to identify the bad actors creating the fake accounts, as well as the subsequent credit card transactions.

Outcome

Within weeks of using the AtData Fraud API, the customer reported dramatically lower fraud rates, and the attempt rate had decreased because fraudsters could no longer create accounts.

This, in turn, reduced the chargeback rate, and the client was delighted to see a significant increase in sales conversions and reduced friction in the experience of their not-at-risk customers.

For more information about our suite of e-commerce fraud and identity solutions, visit us online at:
https://www.experian.com/ecommerce-retail/fraud-prevention

Experian
475 Anton Blvd.
Costa Mesa, CA 92626
T: 1 855 339 3990
experian.com

© 2026 Experian • All rights reserved
Experian and the Experian marks used herein are trademarks or registered trademarks of Experian.
Other product and company names mentioned herein are the property of their respective owners.
(10/26)