retail TouchPoints®

SPECIAL REPORT

WHY BRANDS AND BIG TECH ARE TACKLING REVIEW FRAUD

SPONSORED BY:

AtData

THE EMAIL ADDRESS EXPERTS


Daniel - stock.adobe.com

INTRODUCTION

Checking out reviews for products and services has become an integral step in many consumers' shopping journeys — particularly for higher-priced, high-consideration purchases — with some surveys putting their influence on buying decisions at **90%** or higher. And despite the fact that allowing reviews opens up the possibility of receiving negative comments, brands and retailers have strong incentives to include them: a 2017 **study** from the Medill Spiegel Research Center at Northwestern University found that the purchase likelihood for a product with **five** reviews was **270%** greater than for one with **no** reviews.

Unfortunately, there's also a major downside to reviews: the prevalence of fakes. Whether these fraudulent reviews are written by actual people or, more worryingly, created with generative AI, they cause real-world monetary and reputational harm to companies while misleading consumers and undermining trust in reviews overall.

Quantifying the actual financial impact of this harm is difficult due to varying definitions of what constitutes a fake review, along with challenges in measuring lost sales or other impacts from fake reviews. "There's no one tool or methodology to do that," said Jason Howell, Partner and Firmwide Co-Chair of the Advertising, Marketing and Promotions Practice at law firm Perkins Coie in an interview with *Retail TouchPoints*.

Despite these challenges, it's undeniable that fraudulent reviews have "a major economic impact," Howell added, citing the Federal Trade Commission (FTC)'s rules for defining these types of unfair or deceptive practices as a strong sign that fake reviews are a "growing problem." In quantifying the scale of the problem, the FTC has cited sources like the **National Consumers League**, which said fraudulent reviews cost U.S. consumers **$28 billion** in 2021. On a global basis, the **Center for Data Innovation**, a non-partisan think tank, said fake reviews impact nearly **$152 billion** in ecommerce revenue.

But that doesn't mean that there is nothing to be done. This special report will explore:

- Tools retailers can use to **identify and weed out fake reviews**, including identifying newly created email addresses (a frequent tool of fraudsters) and invalid addresses;
- Legal and regulatory remedies being pursued by government agencies and companies, notably **Amazon**; and
- Some of the challenges presented by **deepfakes** and other methods of masking the identities and origins of reviews.

BreizhAtao - stock.adobe.com

TOOLS TO IDENTIFY FAKE REVIEWS AND REVIEWERS

One of the most basic ways to fight fake reviews is to ensure that actual consumers (who hopefully also are actual users of a product) are writing them. Identity verification, most commonly achieved through requiring an email address, is critical, but as in other areas of cybercrime, there's often an arms race between the technology used by the fakers and those trying to stop them.

Tools and tactics that merchants can use in this fight include:

- Developing an **AI-based risk score**;
- **Profiling email domain risks** in real time and **analyzing IPs** (internet protocols) as a way to get a more comprehensive profile overview;
- Using **customer behavioral insights**, developed through data points such as first activity date (a key indicator used in evaluating risk), longevity, email velocity and email popularity;
- **Email validation** to bar risky, dead or inaccurate email addresses;
- Catching fraudsters that use sequentially named email addresses or multiple variations of the same email via a **platform tumbling check**; and
- Detecting name, address and email **correlations and anomalies** by matching first name, last name and postal address fields with previously seen information, along with checking if there are an anomalous quantity of postal addresses associated with a given email address and vice versa.

Confirming that email addresses are legitimate also makes it easier for retailers to link reviews with purchases, helping increase overall credibility — and giving them a way to directly address negative reviews by contacting the purchaser.

UNDERSTANDING REVIEW FRAUD AND THE ROLE OF EMAIL ADDRESS INTELLIGENCE IN MITIGATING RISKS

By Diarmuid Thoma, VP of Fraud and Data Strategy, AtData

The digital marketplace has transformed the way we shop, offering unmatched convenience and choice. However, this evolution also has introduced new challenges, notably review fraud, which threatens the trust upon which ecommerce heavily relies. Review fraud can manifest in various forms, from fake positive reviews boosting a product's apparent value to negative campaigns aimed at tarnishing competitors. The impact on businesses is deeply felt, affecting brand reputation, consumer trust and, ultimately, financial performance.

At the crux of this issue is the ease with which fraudulent accounts can create or manipulate online identities, particularly through email addresses. Email addresses serve as a primary identifier online, yet their verification has often been overlooked, providing a loophole for malicious actors. Recognizing this vulnerability, AtData focuses on enhancing email address intelligence as a central strategy in combating review fraud.

Email address intelligence analyzes email domains, longevity and behavioral patterns to assess the legitimacy of an email address. For instance, a newly created email domain submitting multiple reviews may indicate fraudulent activity. So, by flagging such anomalies, businesses can prevent these reviews from influencing consumer perception.

Moreover, linking email addresses to verified customer transactions further confirms user legitimacy. This connection allows businesses to determine whether a review comes from a genuine customer experience — it's a straightforward yet effective way to filter out inauthentic feedback, so reviews displayed represent real user experiences.

AtData
THE EMAIL ADDRESS EXPERTS

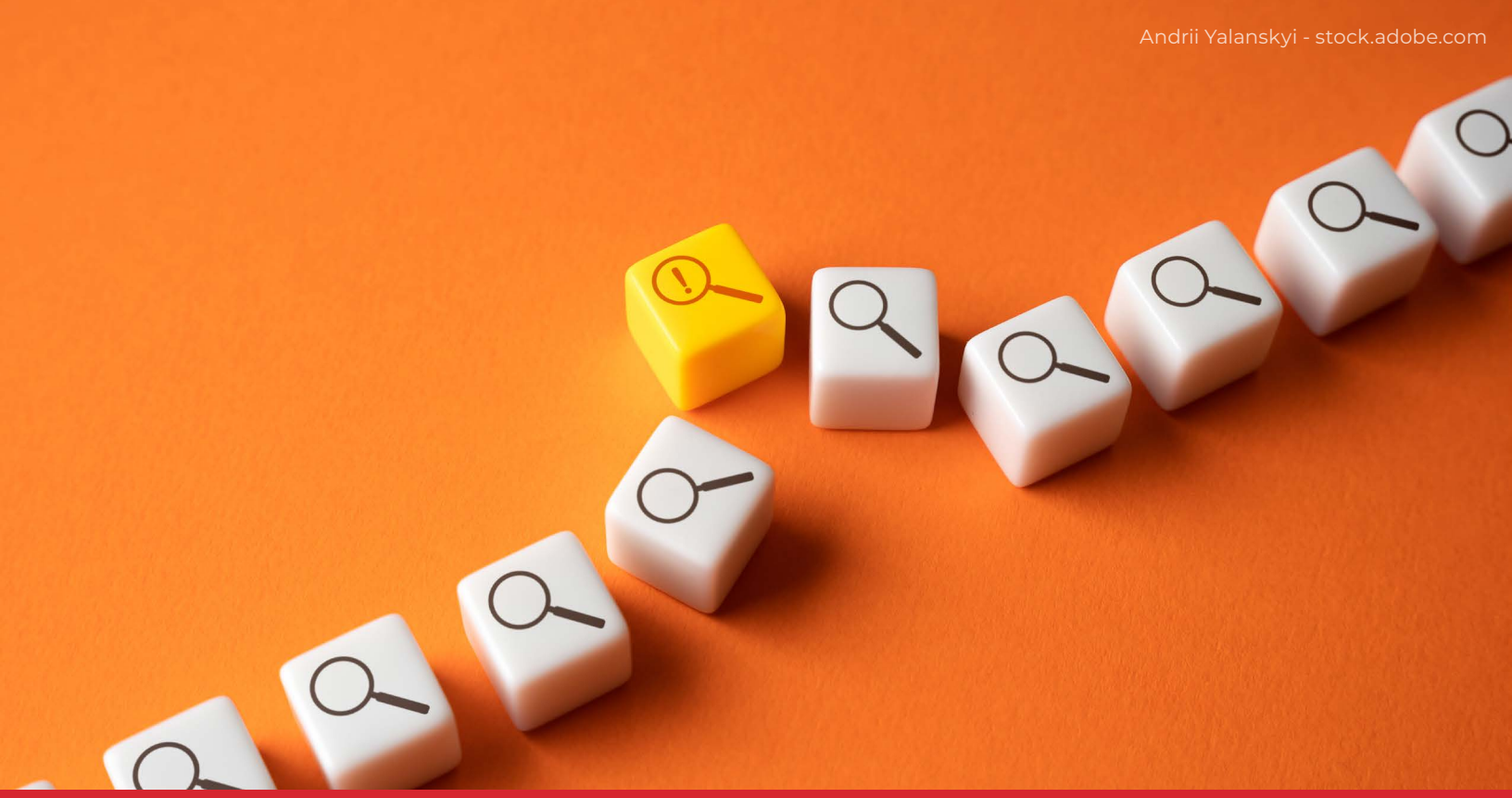
The backbone of this approach is a sophisticated mix of AI-driven risk analysis and machine-learning algorithms. These technologies continuously learn from patterns of fraud, adapting to new tactics employed by fraudsters. Backed by AtData's global email network processing billions of signals, the result is a dynamic system capable of identifying and mitigating risks in real time to protect the integrity of online reviews.

Beyond the immediate benefits of fraud prevention, email address intelligence also fosters a healthier digital ecosystem. With confirmation that reviews are genuine, businesses can confidently maintain a trustworthy relationship with their consumers. This trust has become indispensable, not just for individual businesses, but for the online marketplace as a whole.

Review fraud poses a significant threat to the digital economy, undermining the trust that connects consumer engagement and business success. However, AtData is at the forefront of efforts to mitigate these risks through the strategic use of email address intelligence. By validating the authenticity of online identities, we can preserve the integrity of online reviews, fostering a more transparent and reliable ecommerce environment for businesses and consumers alike.

AtData
THE EMAIL ADDRESS EXPERTS

Feodora - stock.adobe.com


Andrii Yalanskyi - stock.adobe.com

AMAZON JOINS HOSPITALITY SITES TO RESTORE TRUST IN REVIEWS

Sites that depend heavily on reviews to guide customers, such as those in the travel and hospitality industries, partnered with Amazon to launch the Coalition for Trusted Reviews in **October 2023**. Other founding coalition members are **Booking.com, Expedia Group, Glassdoor, Tripadvisor** and **Trustpilot**. The coalition's goals include developing common standards and definitions for use throughout the industry, along with sharing information and best practices and engaging in advocacy efforts.

Even before the organization was formed, Amazon had been using its own considerable resources to fight fake reviews. In **June 2022** Amazon filed a lawsuit against the administrators of over **10,000 Facebook** groups that try to orchestrate fake reviews in exchange for money or free products, and by **October 2022** Amazon had filed a criminal complaint in Italy, a civil lawsuit in Spain and **10** U.S. lawsuits against alleged fraudsters.

A statement from Dharmesh Mehta, VP of Worldwide Selling Partner Services at Amazon, identified the challenges involved in battling a worldwide problem: "Customer reviews are an important part of the shopping experience, and the goal of this coalition is to ensure every review reflects customers' actual experiences. Amazon is aggressively fighting fake review brokers to protect our customers and selling partners, but these fraudsters are a global problem, impacting multiple industry sectors. Through greater collaboration and sharing across industries, including information on fraudsters' tactics and how they operate, we can more effectively shut down fraudulent review activity, deter other bad actors from attempting to game our systems and protect more consumers."

terovesalainen - stock.adobe.com

GENERATIVE AI, DEEPFAKES RAISE THE STAKES FOR DETECTING FAKE REVIEWS

The technology “arms race” between fraudulent reviewers and merchants is on the verge of going nuclear, as generative AI and “deepfakes” become increasingly available and realistic.

“We’re now at a junction enabled by the inevitability of [people using] tools based on generative AI and deepfakes, which are just starting to be mature enough to enable fraudsters to play with your senses,” said Ofer Friedman, Chief Business Development Officer at **AU10TIX**, warning that “what you see and hear is not necessarily true.”

Perkins Coie’s Howell agreed that the merging of generative AI and consumer reviews could be “used to create more fake reviews and increase the problem.”

The challenge is particularly acute given the resources that organized criminals and other fraudsters can gain access to. “The dangerous guys have professional tools and the know-how to use them,” said Friedman. In contrast, the fraudsters Friedman classifies as “amateurs” are more likely to use off-the-shelf tools to generate fake identities and email addresses, “and we can already see and detect them,” he noted.

Friedman recommended that brands use multi-layered security defenses to improve their overall security profile, including the use of two-factor authentication and biometrics along with traditional firewalls and encryption for sensitive personal and transaction data. “The more hurdles you put [in the way of fraudsters], the more likely you are to stop them,” said Friedman.

terovesalainen - stock.adobe.com

THE MANY VARIETIES OF FAKE REVIEWS

The FTC is in the process of instituting new, **more specific rules** against fraudulent reviews, and although these rules have not yet gone into effect, they have gotten through the public comment period. The agency's Advance Notice of Proposed Rulemaking (ANPR), published in November 2022, identified the multiple kinds of fakes its new rules are designed to fight:

- The use of reviews or endorsements by **people who do not exist, who did not actually use or test the product or service or who were misrepresenting their experience with it**;
- **Review hijacking**, where a seller steals or repurposes reviews of another product;
- Marketers **offering compensation** or other incentives in exchange for, or conditioned on, the writing of positive or negative consumer reviews;
- Owners, officers or managers of a company **writing reviews or testimonials of their own products or services**, or publishing testimonials by their employees or family members that fail to provide clear and conspicuous disclosures of those relationships, or soliciting reviews from employees or relatives without instructing them to disclose their relationships;
- The creation or operation of websites, organizations or entities that purportedly provide independent reviews or opinions of products or services but are, in fact, **created and controlled by the companies offering the products or services**;
- Misrepresenting that the consumer reviews displayed represent most or all of the reviews submitted when, in fact, **reviews are being suppressed** based upon their negativity;
- The suppression of customer reviews by **physical threat or unjustified legal threat**; and
- Selling, distributing or buying followers, subscribers, views and other indicators of **social media influence**.

LEARN MORE...

AtData
THE EMAIL ADDRESS EXPERTS

AtData is the leader in email address intelligence. Powered by accurate, comprehensive and privacy-compliant data, including 20+ years of historical email and postal addresses and billions of monthly activity signals, AtData's email-centric data solutions help organizations recognize, know, and target the person associated with the email address. AtData validates and verifies its customers' first party data enabling them to develop actionable customer profiles and assess risk, resulting in an increase in customer engagement, sales, and retention.

retail TouchPoints®

Retail TouchPoints and Design:Retail give all members of the retail world access to a vibrant community that combines insights, inspiration and opportunities to interact with their peers. We sit at the intersection of the art and science of retail strategy, providing granular data, high-value commentary, and aspirational success stories to help readers optimize customer experiences across all channels. Touching all facets of the retail ecosystem, including store experience and design, workforce management, digital marketing and engagement, and omnichannel optimization, our editorial content, multi-media resources and events take timely news and trends and transform them into tactical takeaways that meet the unique needs and priorities of our executive readers.

info@retailtouchpoints.com

ABOUT THE AUTHOR

Adam Blair, Editor

Avid theater-goer, intrepid journalist and grammar nag. There's always something new to learn about retail technology.