The Fight Against Retail Fraud and Policy Abuse

Lessons in AI from Etsy, Instacart, and Gap

Co-created by **Emerj Artificial Intelligence** and **Riskified**

emerj The AI Research and Advisory Company

riskified

INTRODUCTION

In the initial wave of the COVID-19 pandemic, online retail sales grew dramatically. The United Nations Conference on Trade and Development reported in May 2021 that global eCommerce saw ***a "dramatic" increase — from 16 to 19% — in the previous year.***

While eCommerce growth returned to pre-pandemic projections, according to the International Monetary Fund, rates of fraud and online attacks on retailers did not. ***Juniper Research projected in mid 2021 that online payment fraud would grow to $206 billion by 2025.***

Post-pandemic, eCommerce has been at the forefront of artificial intelligence (AI) adoption, which has opened up dozens of new ways for consumers to interact with and order from brands. Not surprisingly you also find that fraudsters have discovered just as many new ways to commit fraud and policy abuse against retailers.

Instead of waiting on headline-grabbing corporate breach news, this moment of technological advancement offers an opportunity to increase scrutiny for privacy data and systems — and the business leaders responsible.

Retail leaders know such incidents are rare, and the super-criminal fraudsters behind them don't represent a significant fraction of the customers that make retail organizations profitable. Yet through predictive AI capabilities, retail leaders can use these data to gain deeper insight into:

- → Where and how fraud is happening across the enterprise and.
- → How to minimize its impact with the least amount of friction possible.

Insights From Top Retailers on Fighting Fraud in an AI-driven World

As part of a special series of episodes recorded for Emerj Technology Research's "AI in Business" podcast sponsored by Riskified, three influential retail executives — Instacart COO Asha Sharma, Gap Inc. Senior Vice President and Head of Asset Protection Chris Nelson, Etsy VP of Analytics and Strategic Finance Gerald van den Berg — appeared on the program to offer their analysis and suggestions for addressing these trends.

In this white paper, you'll discover insights from these distinguished retail leaders that include:

- → High-level insights on the critical retail trends around policy abuse.
- → AI use cases and anti-fraud policies in:
  - **Personalizing customer experiences:** Incentivizing legitimate consumer activity by providing higher quality customer experiences tailored to their interests.
  - **Customer fraud classification:** Using predictive methods to define, predict, and disincentivize friendly fraud and promotional abuse offenders.

Retail Fraud Trends: Three Types of Policy Abuse

Policy abuse broadly refers to consumer activity that manipulates organizational policy for consumer benefit. Consumers may not even think of it as fraud but more as a way to "work the system," i.e., abuse a retailer's policy.

Policy abuse of all kinds occurs along two parts of the "flow" or merchant phases in eCommerce, according to Riskified VP of Business Development Eyal Raab. Policy abuse starts at the initial stages of the funnel, where eCommerce leaders spend marketing budget to acquire a customer base and get the individuals to checkout. The funnel lends itself to customer abuse throughout the process, with coupon abuse being the most prominent example of intentional funnel-side consumer fraud.

Fulfillment policy abuse comes next during the merchant phase. An example of intentional, brazen fulfillment-side policy abuse among eCommerce merchants is empty box fraud — where the seller accepts payment for an item and the buyer mails back as a return an empty box instead. A relevant example from the consumer side would be item-not-received claims — when consumers receive a package physically but claim it never arrived.

It can be hard to tell where fraud occurs between the merchant and the consumer, which opens the door to a third type of policy abuser.

> ***"You have the third group of policy abusers that impersonates consumer behaviors and creates a lot of "noise" in the system. A merchant has to deal with these distractions and implement policies that protect the good consumers, give good customer experiences, and provide good services, so they become longtime customers and try to sift out abuse."***
>
> 
>
> **Eyal Raab**
> VP of Business Development, Riskified
>
> riskified

According to Raab, where retail leaders often see these lines blur is in coupon abuse — especially in the food subscription space, where businesses depend on lengthy commitments from their customers before they see ROI from promotional offers.

In this scenario, consumers sign up for a subscription for a month or two, cancel, and then reinstate the account a few months later with a different email address to collect the introductory promotion a second time.

Policy Abuse and How It Affects Retail's Bottom Line

The leaders from Instacart, Etsy, and Gap agree: Retail leaders need to understand policy abuse — where it happens and who is behind it — in the broader context of overall customer activity before we can address how abuse impacts a merchant's bottom line.

Policy abuse challenges can be quite acute for an enterprise like Etsy since its customers include both sellers and consumers. Etsy VP of Analytics and Strategic Finance Gerald van den Berg shared about how they try to strike a balance between friction for the seller in the onboarding process and encouraging them to provide information that helps them match buyers' intent — and how machine learning (ML) assists in that process.

Van den Berg also notes that — coming from Etsy's background as an online-first company — customers historically tend to be the least forthcoming with their data during the onboarding process than at any point of the eCommerce experience. As sellers build out their experience on the site, the possibility for policy violations become apparent. In most cases, such fraud is not intentional or with nefarious intent:

> ***"It creates a tricky dynamic, where we may know some attributes tend to be more likely to be associated with bad agents, but typically, they're not enough to say you are a bad agent. And so how do we balance that?***
>
> ***[To help,] we do things like variable payout windows, depending on how risky we think you are. It's a version of control, but also thinking through the other levers, such as search visibility, sale, velocity, indicators, things like that. We're trying to personalize more and more as well."***
>
> 
>
> **Gerald van den Berg**
> VP of Analytics and Strategic Finance, Etsy
>
> Etsy

On the other hand, strategies that "crack down" on fraud often do not have the interests of the merchant in mind. Most customers engaging in policy abuse ultimately bring revenue to the business and shouldn't be categorically exiled — it can cause merchants to lose out on significant revenue. Merchants can find it a tricky balance between keeping customers who occasionally abuse policies to blocking those customers whose behavior affects a merchant's profit margins.

With AI, retail and eCommerce leaders can use analytics to enhance how fraud is detected and classify activity directly to the profitability asset any customer — even worst-case offenders — represent for the business's bottom line.

USE CASES IN FIGHTING RETAIL AND ECOMMERCE FRAUD WITH AI

USE CASE 1

Classifying Consumer Fraud

When metrics show different levels of abuse activity and reveal different kinds of policy abusers, organizations can use the same AI capabilities to classify fraud that they have from other data collection efforts across the enterprise.

The experts from Instacart, Etsy, and Gap all agreed that data involved in these collection efforts need to be thought of in terms of the value each customer brings to the business — even if they are the ones engaging in open, brazen policy abuse. You need to ask the question: How does this customer affect the bottom line of my business?

In particular, Gap Inc. Senior Vice President and Head of Asset Protection Chris Nelson learned this lesson the hard way. He came from service in the military, then moved on to onsite loss prevention, and finally specialized in digital fraud. At each stage of his career trajectory, Nelson describes leaving behind the black-and-white thinking suited for combat and remembering that if you stop fraud entirely, you might also be stopping business. He has found that retail and ecommerce fraud increasingly presents larger and more complex challenges.

In arriving to the world of data and fraud prevention, Nelson became acquainted with metrics like those detailed in the personalization use case. Traditionally, there are a few trends and key metrics among worst-case offenders that color these different levels of policy abuse and abusers, including:

- Velocity of purchases for similar item (especially around a launch).
- Many different accounts with very similar email/home addresses, names.
- Brand new accounts that immediately make a high-value purchase, then claim they did not receive it.
- The price of the targeted item (i.e., higher priced items usually being more indicative of and attractive to fraudsters).

As Nelson puts it, ***"You're always trying to thread that needle, if you will, to say, 'Let's do as little impact to the good customers we can and do our very best to isolate the bad customer — the bad actor — out of the equation.'"***

Repetitive Behavior and Machine Learning

Repetitive behavior, length of time, and item price help illuminate sophisticated fraud behavior, even when observed in isolation from each other. However, Nelson emphasizes that activity characteristic of the most sophisticated and highest-impact bad actors is only detectable by fusing data collection processes for these various metrics and to look for applicable patterns between them. He refers to this process in Gap's loss prevention operations as "link analysis."

> ***"Oftentimes, what breaks a case is that we're able to do link analysis. Back when I first started in the industry, you had experts who went through two weeks of training [against fraud], and they did it manually with a stubby pencil drill. Now, the software and the exception-based reporting we have can help us do that."***

According to Nelson, by blending data from various data sources — from both online and offline fraud detection efforts — we can detect patterns that show us where the "supervillains" really are in the business. It is even possible to detect patterns indicative of sophisticated fraud organizations such as insider threats (typically, disgruntled employees as Nelson describes them). These threats become far more visible through data analysis.

Nelson cites examples of using onsite security camera footage to identify the same vehicle going to multiple locations in tandem with finding similar fraud policy behavior coming from different individuals with the same address.

USE CASE 2

Fighting Fraud Through Hyper-personalized Customer Experiences

Outside of security, many systems and ways of doing business native to physical storefronts translate naturally to a personalization data collection online. Instacart COO Asha Sharma knows this well from the grocery vertical, ***"Expectations are changing radically, and now the [grocery] experience is going digital. That's bringing us into focus with personalization with fraud."***

In the grocery vertical especially — with its dependence on logistics and the challenges therein — the benefits of AI in predictive inventory to meet customers' escalating expectations stand in stark contrast to past practices.

> ***"For customers, a lot of times when I think about online grocery delivery, whether it's our partners or Instacart, service starts with knowing exactly what items are available in every single store. That requires deep integrations with all of the inventory systems. In many cases, there are gaps. It requires things like machine-learning models to predict per store, per region, per state, and per retailer what the availability is at any time.***
>
> ***To give you a sense, we update our catalog 3,000 times per second. That is what is required not only to know that we can deliver the right goods to the right person but also that we can suggest the right goods, and we can find them in the right stores."***
>
> 
> **Asha Sharma**
> COO, Instacart
>
> instacart

When Personalization and AI Work Together

Yet no matter where you are in the retail space, the best results come from personalization data and enterprise AI systems tailored to consumers and incentivizing optimal buying behaviors. Even for eCommerce brands like Etsy, whose customers are both buyers and sellers — the focus of personalization remains distinctly on one side of the equation:

> ***"When I think of personalization in the context of Etsy, I tend to think more from a buyer perspective, meaning, how are we matching the inventory that we have to buyers needs. But I think the general tools of machine-learning data and analytics very much apply to this problem of fraud and identifying which sellers we want to apply what sort of risk controls to and what that looks like."***
>
> 
> **Gerald van den Berg**
> VP of Analytics and Strategic Finance, Etsy
>
> Etsy

Van den Berg finds challenges in building personalization systems, particularly when it comes to privacy and advertising. Integrating these systems between online and onsite operations also presents a challenge: ***"We've seen across the industry that [integrating systems has] been a more challenging area in the last couple of years,"*** Gerald shared.

Like Etsy, Instacart has a similar online/onsite duality built into its online-first status as an enterprise. Sharma discusses how Instacart uses machine learning and AI capabilities on both sides of the equation and in fusion:

> ***"I think there's a misnomer that ML and AI only apply to online. There's so much opportunity in the store as well. And it's even more powerful when you can make it omnichannel. When we think about dynamic pricing, we look at it across the store and online," Sharma says. "That's really when you start to get into the next frontier of what's possible and optimizing your full business and not drawing an artificial line between modes of communication."***

Because machine learning aims to recognize patterns, it usually becomes apparent when fraudsters find a loophole to exploit and result in a high volume of fraud attempts.

Yet up until the moment action is taken against perpetrators, nothing about their particular pattern of shopping behavior may indicate anything but legitimate activity. Consider how there are many instances of "spikes" of legitimate consumer behavior based on real demand – such as promotions that fraud teams may be unaware of, weather incidents, the COVID-19 pandemic, or even a celebrity popularizing a certain item.

To better strike a balance between addressing fraud and preserving the business, Sharma emphasizes the importance of optimizing search options for customer behaviors as personalization systems mature. As search engines develop, so will coordination with logistics efforts on the inventory side.

In also building AI-enhanced search capabilities, specific metrics for fraud activity begin to float to the surface of data collection efforts.

Sharma describes an example of a worst-case offender from Instacart: a user who opens 100 different searches for only high-value items in a single minute – when the typical purchasing behavior for that item is a single search completed in about seven minutes.

Even with extended fraud detection capabilities, it's typically when personalization models are trained to maximize what Sharma calls ***"customer inspiration"*** that most incidents of fraud are disincentivized. As she describes Instacart's strategy: ***minimizing fraud through high-quality customer experiences.***

Key Takeaways

Top retailers fighting fraud around the world are using AI and machine learning to:

- ✓ Classify the three kinds of policy fraud, the customers behind them, and their relationship to revenue flows.
- ✓ Identify key metrics in fraud detection data that separates the rest of the customer base from the most organized, sophisticated, and costly fraudsters.
- ✓ Personalize customer experiences to incentivize regular customers away from policy fraud.

ABOUT RISKIFIED

Riskified (NYSE:RSKD) empowers businesses to grow eCommerce revenues and profit by mitigating risk. The world's largest merchants and prestige brands partner with Riskified for guaranteed protection against chargebacks, to fight fraud and policy abuse at scale and to improve customer retention. Supported by the largest team of eCommerce risk analysts, data scientists and researchers, Riskified's machine learning platform analyzes the individual behind each interaction to provide real-time decisions and robust identity-based insights.

Learn more at *riskified.com*

Visit
riskified.com

Contact
riskified.com/contact

ABOUT EMERJ AI RESEARCH

Emerj Artificial Intelligence Research is a market research and advisory company focused exclusively on the business impact of AI.

Companies that thrive in AI disruption run on more than just ideas. They leverage data and research on the AI applications delivering return in their industry today and the AI capabilities that unlock true competitive advantage into the future - and that's the focus of Emerj's research services.

Leaders in finance, government, and global industries trust Emerj to cut through the artificial intelligence hype, leverage proven best-practices, and make data-backed decisions about mission-critical priorities.

Visit
emerj.com

Contact
research@emerj.com