Merchant
Fraud
Journal

Fraud Prevention Tactics that Enable Exceptional Customer Experiences

Sponsored by Ekata

www.merchantfraudjournal.com

Table of Contents

Fraud Prevention Tactics that Enable Exceptional Customer Experiences

Fraud is a growing threat to merchants and customers alike. In 2021, global ecommerce losses due to payment fraud reached a massive $20 billion, representing a 14% growth rate compared to the previous year. The global digital payments market has expanded to a value above $5 trillion, incentivizing fraudsters to find new and creative attack vectors.

As a result, the global fraud prevention and detection market is expected to grow at a rapid compound annual growth rate (CAGR) of 21.5% as enterprise companies invest in cybersecurity and payment protection. Businesses are adopting a myriad technical fraud solutions to handle the volume of diverse customer interactions they process while still providing customers with the protection and experience they demand.

Against this backdrop, standalone technical fraud solutions — no matter how powerful — are not enough. These tools must exist as part of a carefully constructed, holistic fraud prevention strategy.

Below, we dive into three tactics merchants can use to stop fraud while still providing an exceptional experience at every stage of the customer journey.

Fraud Prevention Tactic #1: Account Opening Solutions

In this world of ever-growing ecommerce activity, taking a more holistic approach to fraud prevention is paramount. Retailers that wait until the transaction stage to assess risk are leaving the door open to increasingly sophisticated fraudsters that understand there are steps in the customer journey that might provide easier entry.

With that in mind, one of the ways retailers can combat this trend when dealing with open and accessible account sign-ups and rapid payment options is to assess risk at sign-up — and customize the customer journey accordingly.

A fraud scheme that demonstrates the potential damage that can happen when sign-ups are allowed to happen unchecked is promo abuse. On the next page, we take a look at the intersection of this popular fraud attack vector.

Defining Promo Abuse

Promo abuse entails customers or fraudsters taking advantage of business offers for personal gain. Reports state that over 42% of organizations allow customers to abuse store publicity events, while 73% of U.S. retailers with revenues above $100 million all confirmed some level of promo abuse. For example, bad actors take advantage of counterfeit coupons or leverage computing power to crack discount codes. Many fraudsters hack into loyalty rewards accounts to steal the victim's reward balance, while others create synthetic identities to capture referral bonuses.

The problem becomes extremely acute during the holiday season. Holiday promotions are rife with fraudulent activities. Fraudsters know the increased volume and pressure to close as many sales as possible can result in companies increasing their risk thresholds and turning a blind eye to edge cases to keep acceptance rates as high as possible for holiday shoppers.

Why Promo Abuse Persists

Discounts, coupons, and online sales methods draw in new customers and reward loyal customers. Reports state that 91% of consumers enter an online store because of an online deal or sale, and 93% of shoppers shared that they used a coupon throughout the year. While promotions create system complexity and increased opportunity for fraud, they are invaluable for driving organic traffic and giving customers an attractive sales journey. It is an indispensable form of lead generation that creates accounts and sales.

Moreover, promotions are a useful way to boost client retention, satisfaction, and overall brand engagement. Engaged customers are good for business, with 63% less customer attrition and a 55% higher share of wallet spend. Merchants rely on promotions, and in competitive markets, they are willing to balance those benefits with potential fraud.

By the same logic, companies can benefit from also implementing flexible risk thresholds, even during the holiday period. This may seem counterintuitive — promos are designed to increase purchases, so why limit their impact by turning away customers? But the increase in promotional discounts is known to raise risk, and so something must be done to balance that additional risk. If mitigation measures aren’t taken, the volume of chargebacks can end up creating a significant dent in top-line revenue. Given the thin margins these promotions often provide, chargebacks can even end up jeopardizing the profitability of the entire strategy.

Ultimately, given a choice between paying out large numbers of chargebacks or introducing targeted friction based on a well-constructed risk profile as part of a holistic account opening solution, companies that choose the latter will likely benefit more from promotional periods.

Controlling Promo Abuse

Building anti-fraud strategies into promotional campaigns can help limit or prevent promo abuse. Account opening solutions and technical applications that ingest internal as well as third-party identity and behavioral data are able to monitor sign-ups, new account creations, used voucher codes, and repeat referrals from single users. When issues arise or are flagged (sometimes with as little as an IP address and phone or email), companies can automate the introduction of pre-defined levels of friction based on the risk profile to conduct additional checks and more accurately define and block fraudulent transactions.

Moreover, automated risk solutions that use third-party identity and behavioral data can either be built in-house or integrated directly into a merchant's current infrastructure, meaning it creates no additional friction to the sales experience for legitimate customers. Digital solutions built to specifically identify promo abuse can help prevent fraud without hurting the lead generation efforts of marketing teams and the entry points into a secure sales funnel.

Fraud Prevention Tactic #2: Transaction Risk Profiles

Business stakeholders sometimes describe optimizing customer journeys as if the only way to accomplish it is an absolute proposition for every order submitted — even in the face of fraud risk. Often, this thinking leads to a mandate for a 'zero friction' approach that assumes you should review every order for fraud in the same way. But the reality is much different.

Just like product, sales, or marketing teams will tweak customer journeys based on the profile of the lead or customer, fraud teams should strive to deliver experiences commensurate with the amount of risk an order presents — instead of delivering 'frictionless' customer journeys as an absolute rule. **In other words, fraud teams benefit from introducing a variable amount of friction that balances the financial risk and reward of accepting or declining an order — and that starts at account opening.**

To accomplish this, companies must build transaction risk profiles that allow them to increase or decrease friction according to risk throughout the customer journey.

Use Internal Data

Data science, especially when able to access a wealth of data points, can infer behaviors that target and address possible instances of fraud. Compared to overall transaction volume, data on instances of fraud is limited, making siloed data sets ill-equipped to determine future fraud.

Transaction risk profiles start with internal data to build accurate digital identities for potential customers, allowing companies to construct a baseline to assess risk. Things like on-site behavior, social media presence, order volume, and other technical signals from across the digital ecosystem are key to accomplishing this. In addition, information on verification, transaction type, monetary amount, bin ranges, and more, makes risk profiles far more accurate. Such data is also of immense importance to limiting false positives, helping determine which transactions are a result of fraudulent activity and which are initiated by honest customers.

The most effective companies also take this baseline assessment and enrich it with considerations of lifetime customer value (LTV), customer satisfaction, and potential damage to brand reputation before making a decision about where, when, and how to introduce any additional friction into the buying process.

Expand with Broader Network Data

Taking the idea that more data equals more accuracy one step further, it becomes clear that a company's inability to analyze data sets beyond its own transactions severely restricts the accuracy of its risk profiles. Even the largest company will process only fractions of a percent of the total global ecommerce order volume, giving them tunnel vision on the current trends in fraudster methodology and risking the introduction of undetectable biases now and in the future.

To combat this, companies can seek out ways to increase their access to data from a larger section of total ecommerce order volume. **In short, looking beyond siloed proprietary data must be a key strategic goal for fraud prevention teams.** The best way to accomplish this is to partner with an ecommerce fraud solution that reviews orders using insights gleaned from an analysis of trends across their entire ecosystem of partner companies. Companies that take this approach can also benefit from the successes and failures of other companies, providing a stronger statistical basis for making decisions about when to introduce additional friction into the buying process.

The Ekata Identity Engine, for example, is able to validate five key identity elements — name, IP, address, phone, and email — and analyze how they interact and behave in digital interactions beyond a single retailer. The result is a comprehensive view of a customer's digital identity as well as a more accurate assessment of their risk at every stage of the journey.

Address Weak Spots

Combining and comparing identity risk scores against an overall network of active transactions gives direct information on threat activity. Apart from the obvious help such insights provide to risk assessment teams, businesses can use that information to create dynamic solutions to recurrent problems. If specific verification issues result in data breaches, hacks, or attacks by fraudsters, you can take proactive steps to resolve weak points and incorporate other fraud applications that address them.

Enterprise companies need practical data that can guide the next steps for fraud prevention. Risk profiles compiled across digital and solution ecosystems enable the creation of such data sets, leading to integrations of preventative solutions that provide a higher rate of efficiency and overall security. Best of all, risk profiles remain invisible to customers, meaning these integrations have a limited impact on and introduce no additional friction to the customer journey.

Fraud Prevention Tactic #3: Manual Review

As you can see, there are huge advantages offered by automated fraud prevention solutions that use algorithmic, machine-learning techniques to identify fraudulent orders. From the highest level of abstraction (risk profiles) down to attack methodologies for individual orders (promo abuse), automation is a crucial, indispensable tool for companies to effectively prevent fraud. However, this is not to say it’s a panacea — the reality is much more nuanced, and the increase in operational efficiency and accuracy is not without its limitations.

Algorithms cannot accurately account for all the variables that define the customer experience across the buyer journey. For example, algorithms cannot factor in risk to brand reputation, product design, or customer churn the way a human fraud team can when integrated into an organization.

Perhaps the most important piece is that even the most sophisticated algorithmic solutions cannot deliver a clear accept or reject decision in every case. For this reason, **manual review is still a necessary piece of the puzzle for moments when automated solutions are not able to cleanly determine risk.** Even with the most powerful automated solutions, these situations arise.

In such cases, the extra friction and cost of manual review enables a more confident risk decision where it makes business sense to do so. The alternative is to make approve-or-decline decisions based on inconclusive analysis, a strategy that guarantees a much higher rate of chargebacks. During periods of increased volume — such as the holiday season — this can cause a large spike in successful fraud attempts, causing the post-holiday chargeback count to mount. This is a phenomenon (un)affectionately known as the ‘holiday hangover.’

This is why the perception that manual review is nothing more than a source of additional costs and friction in the customer experience is simply incorrect. Manual review is a critical source of human intelligence for edge cases, expensive items, and bulk purchases — to name a few examples.

The Risk of False Positives

Chargeback prevention is not the only reason you need a manual fraud review team. False positive declines — defined as incorrectly categorizing and declining legitimate orders as fraudulent — are another. In many ways, these false positives are a bigger problem than chargebacks themselves.

For starters, the cost to merchants is estimated at nearly $450 billion in revenue just from lost sales alone. But the more insidious revenue killer is the disastrous customer experience companies provide when they decline a legitimate purchase. Potential customers often take these declines very personally, and are far more likely to abandon a merchant forever than they are to contact them about the mistake or make a subsequent attempt at a purchase.

And where is the most obvious place these false positives occur? **At the margins where the algorithmic risk assessment can't provide a confident approve-or-decline decision.** In the mirror image of the chargeback issue (where fraudulent orders get approved), the failure to have a manual fraud review team can also result in many more false positives (where legitimate orders get declined).

Blending Automation With Manual Review

Whether you come at the problem from the perspective of declining more fraud or from the need to approve more legitimate purchases, a manual fraud team is essential to striking the right balance between risk, customer experience, and profit. The investment in a human fraud analyst team more than pays for itself in increased accuracy, customer satisfaction, and ultimately, dollars.

This is why the future of fraud prevention looks to marry manual review and machine learning capabilities of automated fraud prevention solutions to capture the advantages of both options.

Ekata Solutions

Fraud will continue to hurt merchant revenue as ecommerce expands and rapid payment systems make online shopping convenient. Although a frictionless customer experience is great for conversion rates, it exposes retailers to fraud — such as promo abuse — from ever-more-sophisticated fraudsters.

Finding a balance between customer access and security remains the ideal approach, but is difficult to achieve. The Ekata Identity Engine offers global digital identity verification data through an **ever-expanding suite of solutions that can help you better detect fraud, validate identity, and provide valuable insight about your potential customers.**

- **Account Opening Solutions:** With data insights from the Ekata Identity Engine, quickly distinguish between good user accounts and fraudulent ones at account sign-up. Verify honest consumers with minimal customer inputs to fast-track promotion eligibility while restricting permissions for high-risk users.

- **Transaction Risk API:** By building combined risk scores leveraged from the Ekata Identity Engine, this solution creates comprehensive assessments that determine good or fraudulent transactions. Low-risk customer profiles enjoy a frictionless sales funnel with reduced amounts of false positives, while high-risk transactions are rejected based on customized risk tolerances.

- **Pro Insight:** A SaaS manual review support solution, it auto-populates customer data from order pages and reviews a top-line Identity Risk Score and metadata flags to reduce manual review times for risk assessment teams. Pro Insight makes it possible to analyze billions of behavioral data points from logged transactions to flag and evaluate risky orders that need further review.

Want to know more about Ekata solutions?
Contact us for more information about identity verification and fraud prevention.

“If everyone is moving forward together, success takes care of itself”

Henry Ford

About MFJ

Merchant Fraud Journal is an independent and unbiased publication dedicated to empowering online sellers to greatly reduce the impact of eCommerce fraud on their businesses. Its core mission is to break the silos surrounding merchants' internal fraud prevention processes by bringing together industry professionals to share their knowledge with one another.

Unfortunately, the business process knowledge needed for online sellers to greatly reduce the impact of eCommerce fraud is scarcely available right now. There is no single forum and resource where merchants, payment professionals, and other industry professionals could go to get educated on the myriad of challenges they face.

We seek to fill that gap by being a resource that collects insight from industry thought leaders and fraud prevention tool experts on topics such as chargebacks, false positive declines, account takeover fraud, friendly fraud, data breaches and more. Our goal is to help honest businesses quickly understand their security options and take action, so they can get back to focusing on their core business activities.

About Ekata

Ekata Inc., a Mastercard company, empowers businesses to enable frictionless experiences and combat fraud worldwide. Our identity verification solutions are powered by the Ekata Identity Engine, which combines sophisticated data science and machine learning to help businesses make quick and accurate risk decisions about their customers. Using Ekata's solutions, businesses can validate customers' identities and assess risk seamlessly and securely while preserving privacy. Our solutions empower more than 2,000 businesses and partners to combat cyberfraud and enable an inclusive, frictionless experience for customers in over 230 countries and territories.

Contact Merchant Fraud Journal
Editor In Chief - Bradley Chalupski
Bradley@merchantfraudjournal.com

Contact Ekata to learn more.
www.ekata.com | 1.888.308.2549

Merchant
Fraud
Journal

📍 290 Caldari Road,
Concord, Ontario L4K 4J4
Canada
--

✉ hello@merchantfraudjournal.com

🖥 www.merchantfraudjournal.com

☎ 1-(888) 225-2909