



Merchant
Fraud
Journal

5G GLOBAL NETWORK COM



ADDRESSING PAYMENT FRAUD AND THE CUSTOMER EXPERIENCE IN 2022



Sponsored by Sift

www.merchantfraudjournal.com



TABLE OF CONTENTS

Understanding the Fraud Economy	3
<hr/>	
The Customer Experience and Brand Abandonment	4
<hr/>	
Customer Friction via Fraud Solutions	5
<hr/>	
Industry-Specific Low-Friction Solutions to Fraud Tactics	5
<hr/>	
Key Takeaway	8
<hr/>	

Addressing Payment Fraud and the Customer Experience in 2022

Fraud attacks continue to increase as the payment industry grows. As retail e-commerce reached a market value of \$4.9 trillion (and a 14% year-over-year increase for U.S. online purchasing), global e-commerce losses from payment fraud reached a massive \$20 billion. Incidents of fraud build in line with industry expansion, and recent reports now state that 49% of consumers have fallen victim to payment fraud.

In response, the payment industry has committed to addressing the growing issue of fraud. The global security business has exploded to a \$139.7 billion value in 2022 as merchants adopt tools that can defend against online attacks. Ecommerce has made great strides in fraud prevention.

But new solutions can increase customer friction. Authentication applications, secure logins, and anti-fraud system integrations that address security concerns also harm the ease with which customers can access services. As consumers opt for digital channels, engagement becomes a key performance indicator for most retailers—any threat to the customer experience can hurt revenues, including fraud solutions.

A balance between prevention and consumer satisfaction is necessary. Let's explore how retailers can defend against fraud without harming the customer's sales journey.

Understanding the Fraud Economy

To accurately assess and defend against fraud attacks, all businesses must understand the nature of the Fraud Economy. While some criminals and friendly fraud are associated with smaller-scale attacks, the shift into online services has created a sophisticated network of bad actors. Fraudsters have grown skilled, and they leverage new technology to their advantage. How they operate changes based on trends and system weak points, just like any traditional economy.

As a result, the complexity of online abuse has skyrocketed. Account Takeovers (ATOs), bots, and multi-tiered scams all threaten the safety of the payments industry. The goalposts of security continue to change as digital transformation takes hold; even organized fraud rings have become common.

As it concerns the customer experience, the increase in fraudulent attack organizations most likely means that businesses can no longer remain reactive to fraud. Trust and safety teams need to stay aggressive towards potential fraud blindspots and work to eliminate the opportunities that intelligent hackers will exploit. In addition, by making security a task of active participation, anti-fraud teams can communicate security integrations to consumers, helping manage service expectations that better maintain retention.

The Customer Experience and Brand Abandonment

On the other side of the equation, merchants must remain aware of how a lack of security will also contribute to consumer brand abandonment. Almost 25% of surveyed clients who experienced financial fraud state they are “very” or “extremely” concerned about it happening again. When a customer feels at risk, they will abandon a business. Merchants cannot disregard security in a bid to keep customer friction low, as limited fraud prevention will also contribute to lost customers.

Security Fears by Payment Type

Unfortunately, incidents of fraud continue to grow, most notably within digital payment types. Offering multiple payment methods provides the user with convenience, but it also increases risk. The spikes in fraud losses by payment type give customers the right to feel wary about the brands they choose to engage with:

- **Digital wallets:** In 2022, digital wallets saw a 200% increase in payment fraud attacks
- **Payment service providers:** Payment fraud growth by PSPs grew by 169%
- **Crypto exchanges:** Crypto exchanges involve known risk but still saw fraudulent transactions rise by 140% in 2022
- **Buy Now, Pay Later:** Attempts at fraud within BNPL rose by 54%, with total item value increasing 5% to \$179
- **Remittances:** The value of remittance fraud spiked by 677% up to a transaction value loss of \$1271 in 2022

Security Fears by Industry

In addition, distinct industry verticals all experienced increases in payment fraud rates.

- **Retail:** Fraud rates rose by 12% year over year, while transaction values doubled with a 244% yearly rate increase
- **Travel & Hospitality:** As the industry vertical hit hardest in 2022, fraudulent transaction value in travel and hospitality jumped from \$332.22 to \$2,461, a 695% boost.
- **On-demand services:** Growth in smartphone and digital customer applications contributed to a 128% increase in year over fraudulent order value.
- **Marketplaces:** Fraudulent transactions values increased from a 2020 value of 2,251.73 to \$3,129
- **Networks:** Business in communications saw a 23% increase in 2022 in payment fraud.
- **Fintech:** As Fintech and related online financial services contributed to market disruption in 2022, instances of payment fraud increased with a 69% spike

Customer Friction via Fraud Solutions

To sum up, merchants face a double-edged predicament:

On the one hand, the growth in fraud losses and a lack of security contribute to brand abandonment, as 74% of surveyed customers state they would stop engaging with a brand compromised by fraud. Viewing fraud as an account-level problem or a simple cost of doing business will still lead to lost customers, even if it lowers customer friction.

On the other hand, common anti-fraud strategies that offer protection often turn away or frustrate authentic customers. Overzealous fraud solutions lead to false positives, with recent reports showing that up to 35% of rejected orders turn out to be legitimate purchases from honest buyers. Moreover, many prevention services are expensive and a challenge to scale, further hampering business growth.

Merchants might feel stuck in a no-win situation. Defending against tech-savvy and organized fraudsters will require real-time and active responses. Choosing not to implement any fraud prevention could expose businesses to fraudulent transactions and chargebacks that lead to brand abandonment by customers. But installing aggressive anti-fraud solutions will drastically boost friction within the user's experience, once again reducing customer satisfaction and leading to lost clientele.

Industry-Specific Low-Friction Solutions to Fraud Tactics

To achieve the right balance between fraud prevention and customer experience, customization may offer a potential solution. Instead of staying reactive to the sophisticated tactics used within the fraud economy, businesses can leverage tailored anti-fraud solutions that manage risk and offer higher probabilities of protection to particular instances of fraud.

Let's examine some common techniques used by bad actors, and use that as a basis for potential strategies prevention teams can build or devise to better protect payment industry businesses.

Account Takeover

Hackers take advantage of simple logins, credential stuffing, or other phishing scams to access confidential services administered through networks. Once they have ownership of customer accounts, they can engage in further illegal activity for personal gain (or even use a compromised account to hack into business databases). Account Takeovers (ATOs) are common, occurring in 1 out of 5 adults.

In response, merchants should employ low-friction preventions tactics such as:

- **Multi-factor authentication:** While requiring two pieces can create additional login friction, the security benefits far outweigh the risk.
- **Behavioral data collection and analysis:** Incorporate data services that can provide actionable insights on login attempts and restrict access levels, helping deter fraudsters from taking over accounts.
- **Fraud monitoring solutions:** Employ services that scan the web for suspicious activity related to a business and any customer data.
- **Support programs:** Customer service can encourage and inform customers on how to protect their accounts (e.g. creating secure passwords, or checking fraud-prone areas of business such as coupons or discounts codes). Not only does this improve communication channels, but it can actively protect any business system.

Payment Abuse

Both honest customers and bad actors take advantage of the payment system for monetary gain. Most payment abuse falls under three broad categories:

- Unauthorized transactions (stolen credit cards, data theft)
- Lost or stolen merchandise (Shipping scams, refund abuse)
- False disputes (chargebacks, friendly fraud, bounced cheques)

Because it is so hard to determine the intent behind payment abuse, it is a challenge for fraud prevention teams to evaluate and defend against fraud. For example, a long-term priority customer might dispute a transaction when they wait for their package and it arrives late. By accident, they keep both the product and the returned funds (a form of friendly fraud). Or, they might dispute a charge if they order a package that is stolen from their porch. Merchants will have a very hard time deciphering what disputes are the result of payment abuse, mistakes, technical errors, or customer dissatisfaction.

In all situations, merchants are responsible for the losses, and increases in chargeback disputes strain the customer-to-business relationship. Mitigation solutions are necessary.

There are several ways that businesses and safety teams offer a high-quality shopping experience without sacrificing the security that can limit payment abuse:

- **Chargeback mitigation solutions:** AI-power chargeback services can evaluate and dispute many false claims, from both honest and malicious users.
- **Store policy:** Use your customer service reps, refund policy, and listed terms and conditions to manage customer expectations. Good store guidelines deter instances of fraud and refund abuse, while honest customers will be happy to oblige
- **Encryption:** Tokenize and encrypt all transaction data to better protect any information transmitted through a payment gateway and check-out flow.
- **Update:** Upgrade all of your security software, firewalls, and networks to best protect against instances of payment fraud (e.g. stolen credit card use)

Automation and Bots

To gain every possible advantage over security applications and fraud prevention teams, bad actors leverage bots and automated attacks to breach business systems. Botnet use has increased by 106% in 2022, with payment card-specific incidents jumping 111%.

Examples include scraping for tickets, where technical systems buy up every ticket at a venue, leading to exorbitant resell prices. Another scheme involves gift cards, where bots check millions of potential coupon numbers variations for illegal gain. In each instance, merchants must cover any losses due to fraudulent bot schemes. The issue continues to grow, as some reports consider 51.8% of all internet traffic to be bots, with 28.0% designed to subvert ecommerce transactions.


Bots are a direct threat to customer satisfaction. Attacks on shopping carts can cause consumers to lose purchases. Data breaches expose confidential user information that can lead to further identity theft and financial harm. Of surveyed customers, 80-90% stated they wished they could trust more companies with their data—brand engagement will increase by preventing bot attacks.

To defend against bot attacks without introducing undue customer friction, use the following prevention techniques:

- **Shopping cart services:** When possible, use up-to-date software integrations that can flag and locate bot purchases. Particular attention to card-not-present transactions can help boost system security.
- **Verification:** Collect card verification details that can confirm the identity of each buyer and that they are human (e.g. CAPTCHA)
- **Smart services and device activity:** Bots do not operate like humans, and behavior data analysis can help track such differences. As fraudsters grow more sophisticated in their attacks, merchants can leverage AI security as the first line of defence.

Key Takeaway

The Fraud Economy continues to grow in step with the payments industry. But while instances of fraud and fraud prevention increase consumer friction and threaten brand abandonment, merchants can take steps to integrate security solutions that do not negatively impact the customer experience. Adaptability and flexibility within safety teams and anti-fraud solutions will help businesses remain at the forefront of security, all while limiting total user friction within payment check-out flows.



***“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.




Contact Merchant Fraud Journal

Editor In Chief - Bradley Chalupski

bradley@merchantfraudjournal.com




 290 Caldari Road,
Concord, Ontario L4K 4J4
Canada

--

 hello@merchantfraudjournal.com

 www.merchantfraudjournal.com

 1-(888) 225-2909