Merchant Fraud Journal

# ECOMMERCE FRAUD TRENDS 2024

10 of the leading eCommerce fraud prevention and payments solutions share what you need to prepare for in the coming year

Featuring Chargeback Gurus

www.merchantfraudjournal.com

# Chargeback Gurus

**Chargebackgurus.com**

## What will the impact of Generative AI be on the fraud ecosystem, and how will merchants need to adapt?

It is already having an impact. Generative AI is enabling more convincing scams, generating fake documents, and automating fraudulent activities. Additionally, attack velocity will increase as fraudsters leverage AI to scale their operations at a much lower cost than before. Ultimately, the whole ecosystem will need to adapt as the multi-year and multi-billion dollar investments in capacity to prevent, detect and recover from fraud will become obsolete at a much faster pace.

Some of the areas where merchants will need to be attentive:

- Behavioral Analysis: Incorporate behavioral analysis to detect anomalies in user behavior.
- Human Oversight: Maintain human oversight to handle sophisticated AI-driven fraud attempts.
- Collaboration: Share information and collaborate with peers to combat evolving fraud tactics.

Generative AI offers both challenges and solutions for fraud prevention, demanding an evolving approach from merchants to stay ahead of fraudulent activities.

## What will the role of human fraud analysts be in a world increasingly dominated by artificial intelligence?

In a world increasingly dominated by AI, the role of human fraud analysts will become ever more crucial and evolve in several ways:

- Fraud analysts will play a vital role in handling complex or novel fraud cases that AI may struggle to fully understand. As of yet, AI has not shown a capability for intuition, which plays a significant role in addressing highly sophisticated attacks.
- Fraud analysts will need to oversee AI-driven solutions. They will monitor the AI's performance, fine-tune algorithms, and provide human judgment when AI systems generate uncertain results. This will require a massive effort to retrain the existing workforce.
- Fraud analysts will be required to validate AI-generated decisions and intervene when necessary to prevent false positives or false negatives. They'll ensure that actions taken are in line with business objectives and principles established by governing bodies or internal policies.
- While AI provides efficiency and automation, fraud analysts will integrate their skills and experience into the fraud prevention process, ensuring a holistic approach that combines AI's speed and consistency with human expertise.

In summary, while AI plays a vital role in automating and enhancing fraud detection and prevention, fraud analysts will continue to be essential for their critical thinking, adaptability, ethical judgment, and expertise in handling complex and novel fraud cases. The future of fraud prevention likely involves a harmonious partnership between analysts and AI systems. In other words, the current fraud analysts will not be replaced by AI, but rather by analysts that know how to effectively manage AI to make their jobs more efficient.

## What changes will merchants need to make to combat new trends in first-party fraud (friendly fraud)?

To effectively combat new trends in first-party fraud, often referred to as "friendly fraud," merchants should implement several key strategies, while also considering the potential influence of generative AI. Clear communication and transparency remain essential, with merchants ensuring their return and refund policies are easily accessible and transparent, reducing the potential for misunderstandings that lead to friendly fraud chargebacks. Moreover, improving customer service is crucial. Responsive support can address customer concerns promptly, decreasing the likelihood of chargebacks resulting from frustration, while AI-driven chatbots and virtual assistants can enhance customer interactions.

Enhancing transaction descriptors and user-friendly interfaces, now with the aid of generative AI for improved user experiences, can minimize user errors and confusion during the checkout process, thereby decreasing the likelihood of friendly fraud. Maintaining detailed records of customer transactions, communications, and interactions, with AI-based data analytics to spot unusual patterns, is vital for dispute resolution. Additionally, implementing strong authentication measures like two-factor authentication (2FA), potentially augmented by AI for behavioral biometrics, can verify customer identities and protect against unauthorized transactions.

Leveraging advanced fraud detection tools driven by AI such as machine learning models to distinguish between legitimate and fraudulent chargeback requests, collaborating closely with payment providers, and educating customers about chargeback consequences, now with AI-enhanced personalized communication strategies, are all integral in the fight against friendly fraud. Furthermore, ensuring compliance with regulations and proactively adapting to changing regulatory landscapes is crucial. Regularly updating policies and continuously analyzing transaction data, potentially utilizing generative AI to identify emerging fraud patterns and behaviors, can help merchants stay ahead of evolving fraud tactics. In essence, merchants should adopt a proactive, customer-centric approach, combining clear communication, robust customer service, and preventive measures, all while leveraging the power of generative AI and data analysis to understand and mitigate the risk of friendly fraud.

## What will be the biggest 2024 eCommerce fraud trend that is currently being overlooked?

We don't know what we don't know. Predicting the specific trends or developments in eCommerce fraud for 2024 is challenging, especially since it is too early to understand the true impact of some of these new technologies such as generative AI. The landscape is continuously evolving, and new threats may emerge that are currently unknown or overlooked. In the eCommerce industry, effective fraud prevention hinges on vigilance, information, and adaptability. It's crucial to stay vigilant by actively monitoring transactions and customer behavior for any signs of abnormal activity. Keeping up with the latest developments in fraud tactics and industry trends through continuous learning and information-sharing is equally important. Being adaptable allows businesses to adjust their strategies and technologies in response to evolving threats. Collaborative efforts and the use of advanced technologies, like AI and machine learning, can enhance fraud detection capabilities. Additionally, educating customers about potential threats and dispute resolution processes can minimize friendly fraud instances. In a dynamic and ever-changing environment, a proactive and adaptive approach is vital for staying ahead of fraudsters and safeguarding eCommerce operations and customers from emerging fraud trends.

Generative AI is a transformative technology with the potential to reshape not only the landscape of fraud but virtually every facet of our world. Its capacity to generate human-like text, images, and even entire narratives is opening new doors across industries, from content creation and automation to personalization and data analysis. As we witness the rapid evolution of generative AI, it's essential to acknowledge that we are on the cusp of significant, paradigm-shifting developments that are, at this point in time, impossible to predict with certainty.

The unprecedented and multifaceted impacts of generative AI will likely bring about surprises that extend far beyond our current imagination. From revolutionizing the way we produce content and communicate to fundamentally changing how we interact with technology, this transformative force is poised to usher in a new era of possibilities and challenges. Governments, businesses, industries, societies, and communities will need to remain agile, proactive, and adaptable in the face of these emerging trends, preparing for the unexpected and harnessing the full potential of generative AI to drive innovation and progress. In this era of profound technological change, the future holds dangerous and exciting, transformative, and unpredictable possibilities.

**Rodrigo Figueroa**
**Chief Operating Officer at Chargeback Gurus**

Rodrigo Figueroa is a highly experienced professional in the field of Risk Management, serving as the Chief Operating Officer (COO) at Chargeback Gurus. His primary focus is on establishing a sustainable framework that facilitates company growth while overseeing various aspects of operations, technology, and client success. With over two decades of expertise in the Investment, Commercial, and Consumer Banking industry, Rodrigo has worked across multiple countries in the Americas, Europe, and Asia.

His extensive knowledge encompasses governance, controls, eCommerce, payments, cards, P2P networks, Electronic Wallets, as well as areas like Enterprise Risk, Operational Risk, Cyber Security, Technology Risk, Audit, International Governance, and Regulatory Management for Banking and Payments.

Rodrigo's proficiency in English, Spanish, and Portuguese, along with his diverse background and exposure to various markets and cultures, has enabled him to achieve remarkable results in challenging and diverse environments. He holds a Master of Science degree in Risk Management from NYU and currently resides in Plano, Texas.

# 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

Merchant
Fraud
Journal

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

hello@merchantfraudjournal.com

www.merchantfraudjournal.com

1-(888) 225-2909