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

www.merchantfraudjournal.com

TABLE OF CONTENTS

> ***2024 will bring massive changes to the fraud prevention industry***

Invaluable Insights to Protect Yourself Against eCommerce Fraud

We put this guide together to help merchants, SMBs, and enterprise organizations do better to protect themselves effectively against emerging threats. It consists of interviews with ten of the most well-known and respected eCommerce fraud prevention solutions available today:

We asked these experts a series of questions about how merchants can prepare for the challenges that await in 2024. Participation was entirely free; Merchant Fraud Journal did not receive a single penny from any solution for their inclusion. We simply reached out to solutions we know are at the forefront of today's emerging fraud prevention technologies. They did not disappoint us. They answered our call with valuable insight on four questions:

- What will the impact of Generative AI be on the fraud ecosystem, and how will merchants need to adapt?
- What will the role of human fraud analysts be in a world increasingly dominated by artificial intelligence?
- What changes will merchants need to make to combat new trends in first-party fraud (friendly fraud)?
- What will be the biggest 2024 eCommerce fraud trend that is currently being overlooked?

Merchant Fraud Journal's mission is to foster collaboration between fraud prevention experts, and then pass that knowledge on to merchants. We are confident that you, our community of readers, will find this guide to be a valuable resource for improving your own understanding and practice of eCommerce fraud prevention.

Sincerely,
Bradley Chalupski—Co-founder & Editor-in-chief

ACI Worldwide

Aciworldwide.com

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

Fraudsters are already exploiting today's latest generation of freely available, low-cost AI tools to trawl vulnerabilities and automate attacks. As a result, synthetic and bot led attacks are now overtaking human led attacks, creating a surge in bad activity like account hacking.

Increasing accessibility to Generative AI tools is making it even easier for criminals to plan, perform and profit from fraud and at incredible scale and speed. We've seen a rise in online data breaches, ID theft and socially engineered attacks, especially Generative AI created emails and social messaging. These are used to drive phishing, farming and whaling attacks, where users are tricked into revealing their personal information, passwords, phone numbers, or social security numbers.
Fraudsters are also harvesting personal data, including usernames and passwords, in huge numbers from the Dark Web and are using bots to carry out card testing and credential stuffing. Once they have compromised authentic accounts, they are then able to commit a range of downstream fraud using Generative AI.

Data is key in tackling these types of attacks. Firstly, in understanding the digital identity of the consumer. Secondly, in scoring that data via a multi-layered approach that utilizes multiple tools (including AI) to frictionlessly authenticate ID for genuine customers. Merchants need to fight fire with fire, using next gen AI solutions like incremental learning to self-teach anti-fraud models instantly, so that they can automate processes and respond in real time to counter attacks as soon as they happen.

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

Despite the hype, AI's immediate goal is to support not eliminate people. With multiple retail channels generating a relentless stream of real-time data, fraud analysts simply can't keep up. They need serious machine, payments and fraud intelligence to help them analyze and use transaction data instantly and at scale.

AI-automated systems help to reduce risk, time and effort spent on fraud detection, removing the burden of data crunching and freeing human fraud analysts to focus on preventative measures. Spending more time looking deeper into critical functions and less time refreshing rules and updating models, allows analysts to add more value and be more productive.

While AI is increasing involved in rules setting and decision making, analysts still play a vital role in keeping AI on track and training it to do its job. Human oversight is essential to avoid inadvertent deviation, stop inaccuracies being replicated and ensure specific business, market and commercial nuances are considered.

There's no doubt that AI can provide enormous value in the fight against fraud, but humans are still needed to innovate and 'think outside the box' when it comes to keeping one step ahead of fraudsters. It's why even our most advanced incremental learning solutions are still backed by a team of ACI Data Scientists.

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

The challenge with first party fraud is that the perpetrator IS the genuine customer. No amount of pre-screening can truly predict if they are going to commit fraud. The risk is that frictionless transacting is also a key consumer requirement, and conversion-hungry merchants are reluctant to impede this. From multiple account users and promo fraud to returns/refund misuse and false chargebacks, first-party fraud is on the rise. It's being fueled by cost-of-living crisis, driven by social media and chat forums and made 'socially acceptable' because consumers see it as victimless and not really a crime (though it is). Recent studies show that one in three consumers admit to some form of friendly fraud. And the more they do it, and get away with it, the more likely they are to do it again.

This behavior has created an industry-wide issue that needs an industry-wide response. It's time to break down data silos and harness collective network intelligence across merchants and their partners. This can help improve orchestration of fraud strategies and reduce operational costs across the industry.

With more data signals, from more sources, merchants can gain better and faster understanding of why and how consumers are actively engaging in friendly fraud, and in which in verticals/sectors. Armed with this knowledge, they can work faster to close accounts and identify serial offenders, even if they move around.
Importantly, by using network intelligence, they can do this without having to create unnecessary check-out friction or spoil the experience for genuine customers.

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

Fraud is not always clear cut. In some cases, company policy can actively encourage abuse. This is true for returns fraud. Having free delivery, quibble-free returns and frictionless refunds may help drive conversion but, with nothing to differentiate a genuine return from a fraudulent one, the policy is easy to abuse.

One of the most common types of returns fraud is wardrobing, where people buy an item, wear it, then return it for a refund within 30 days. This is a growing issue in the fashion sector, where 'Instagram' culture and a desire to keep images 'looking fresh' has exacerbated this type of activity. Returned items may be damaged and unfit for resale, and merchants may be unable to recoup delivery and collection costs. At scale, this represents a significant financial loss for the merchant.

To protect their margins and limit their losses, those reliant on digital sales face a constant dilemma. Do they change their policy, introduce more returns friction and risk alienating loyal users? Or do they turn a blind eye, hope their margins can take the hit, and risk becoming a soft target for potential abusers? With the right fraud management approach they can find a middle ground. Using a partner like ACI can help them take a more holistic approach to payments, abuse, and chargebacks, so they can define better decision strategies and business policies.

Another overlooked fraud trend is deep fake. As the world becomes increasingly digitized, bad actors are equally able to exploit the amount of data that exists to create synthetic personas. To counter this, merchants now need to deploy cyberdefense strategies that can not only detect and prevent fraud but also enable them to authenticate and verify consumers' digital identities in real time – to protect against account takeovers, while seamlessly integrating updates to accounts. In the year ahead, we expect to see a rise in more sophisticated authentication especially biometrics for mobile commerce. In the future pay-by-voice may be as popular as tap-to-pay is today.

Erika Dietrich
Vice President, Global Fraud Prevention and Risk Services

Erika Dietrich is A certified fraud and analytics professional with over 20 years of experience in payment acceptance optimization, global fraud prevention, digital identity verification and authentication, statistical data analysis, machine learning, and artificial intelligence enterprise real-time financial decision technology solutions. Erika leads a global team of fraud professionals across six different countries overseeing customer analysis and implementing state-of-the-art intelligent solutions to reduce operational costs and generate incremental revenue. Leveraging incremental learning, pattern detection and data mining techniques, Erika's efforts have delivered best-in-class performance for leading merchants across the globe. Erika's contributions have been recognized with the 'Forty under 40' and Women in Payments Educator in 2019. Her passion for her work drives her pursuit of excellence in the industry.

- **LinkedIn**
- **ACI bio:**

Celebrus

Celebrus.com

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

Generative AI has the potential to impact the fraud ecosystem in various ways, posing new challenges for merchants. Here's how:

Sophisticated Fraudulent Content: Generative AI can be used to create highly realistic fake documents, images, or videos, which makes it easy for fraudsters to impersonate legitimate customers or create fraudulent accounts. Merchants will need to implement advanced verification methods to detect anomalies and forgeries.

Chatbot Fraud: Fraudsters may deploy chatbots powered by generative AI to engage with customer support or interact with eCommerce platforms. These chatbots can mimic human behavior and deceive businesses. Merchants may need to enhance their chatbot detection and response capabilities.

Increased Social Engineering Attacks: Generative AI can assist fraudsters in crafting convincing phishing emails or messages, increasing the risk of social engineering attacks. Merchants will need to educate their employees and customers about these threats and implement behavioral biometrics systems along with robust email and message filtering.

Voice and Audio Fraud: Advances in voice generation technology can be used to create fraudulent audio recordings for phone-based fraud attempts. Merchants may need to strengthen authentication methods for phone-based interactions and consider voice biometrics.

Deepfakes for Identity Theft: Deepfake technology can be used for identity theft, where fraudsters create realistic video or audio clips to impersonate customers or employees. Merchants may need to implement identity verification methods which are multi-layered and include machine learning and behavioral analysis.

To adapt to these emerging challenges, merchants can take several proactive measures:

AI-Powered Detection: Employ AI and machine learning systems to detect anomalies and patterns associated with generative AI-generated content. These systems can help identify fraudulent activity more effectively.

Multi-Layered Verification: Implement multi-layered identity verification, which combines various biometric, behavioral, and document-based authentication methods to create a more robust verification process.

Having a strong omni-touchpoint fraud prevention strategy can include AI-based fraud management tools for detecting fraud in real-time, advanced contextual analysis by experienced fraud analysts for suspicious transactions, multi-factor and biometric authentication strategies to confirm the legitimacy of transactions, cross-channel tracking systems that monitor repeat fraud offenders across physical and digital channels, and PCI DSS payment gateways that are specific to a brand's security metrics.

Behavioral Analysis: Monitor user behavior and transaction patterns for deviations that may indicate fraudulent activity, even if the content appears legitimate.

Advanced Authentication: Invest in advanced authentication solutions, such as biometrics, behavioral analysis, and tokenization, to enhance security while minimizing friction for genuine customers.

Collaborative Data/Intelligence Sharing: Collaborate with industry peers and share threat intelligence to stay updated on emerging fraud tactics and collectively combat fraud more effectively.

Horizon Scanning and Regular System Updates: Keep fraud prevention systems and AI algorithms up to date.

Legal and Regulatory Compliance: Ensure compliance with relevant jurisdiction data protection and cybersecurity regulations.

In a world where generative AI can be used for fraudulent purposes, it's essential for merchants to continuously upgrade their fraud detection and prevention measures, and stay informed about the latest developments in AI and fraud tactics. Collaboration, intelligence sharing, and a multi-layered approach that uses behavior biometrics and analytics is key in mitigating the impact of generative AI on the fraud ecosystem.

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

While AI can automate many aspects of fraud detection and prevention, human fraud analysts will continue to play crucial roles in several key areas.

Complex Investigations: Human fraud analysts will be essential for handling complex and unique fraud cases that AI algorithms might struggle to understand fully. They can apply their experience and critical thinking skills to dig deeper into unusual patterns and behaviours.

Contextual Understanding: AI may excel at pattern and anomaly recognition, but it can lack the ability to understand the broader context of a situation. Human analysts can consider factors like customer behavior, industry-specific nuances, and regional variations in fraud cases and their unique patterns.

Decision Making: In situations where there's ambiguity or conflicting information, human fraud analysts can make nuanced decisions that align with a company's risk tolerance and customer experience goals.

Machine Learning Oversight: Human analysts will continue to oversee and fine-tune AI and ML models. They can help train models, validate their outputs, and make adjustments as needed to reduce false positives and negatives.

Customer Interaction: Handling customer inquiries and disputes related to fraud cases requires empathy and communication skills, which AI cannot replicate. Human analysts can provide support and resolution for affected customers.

Crisis Management: In the event of a major security breach or fraud incident, human analysts can help manage the crisis, coordinate responses, and communicate with stakeholders.

Strategic Planning: Human analysts can contribute to long-term fraud prevention strategies, helping businesses anticipate future threats and develop proactive measures.

The ideal approach for many organizations is to integrate AI, and human expertise, creating a synergy that leverages the strengths of both to achieve more effective and efficient fraud prevention.

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

Friendly fraud occurs when a customer makes a legitimate purchase but later disputes the transaction or requests a chargeback fraudulently. To address this growing concern, merchants may need to implement various changes in their strategies and processes:

Robust Transaction Documentation:
Maintain detailed records of all customer interactions, including order confirmations, tracking information, and customer communications.
Use digital signatures or electronic acknowledgments when possible to verify that customers have received products or services.

Enhanced Authentication Methods:
Implement multi-factor authentication (MFA) for customer accounts, particularly for high-value transactions or subscription services.
Utilize device fingerprinting, behavioral biometrics and geolocation data to verify the legitimacy of the transaction.

Data Analytics and Machine Learning:
Employ advanced fraud detection tools and machine learning algorithms to identify patterns of friendly fraud.
Continuously analyze transaction data to detect anomalies and suspicious behaviour.

Behavioral Biometrics and Analysis:
This can be a valuable way to identify first-party fraud, which involves individuals using their own information to commit fraudulent activities. Behavioral biometrics leverages the unique behavioral patterns and characteristics of individuals, such as their typing patterns, mouse movements, touchscreen interactions, and other digital behaviour. These patterns are specific to each individual and can be used to detect unusual or fraudulent behavior.

Chargeback Management: Invest in comprehensive chargeback management solutions or services to proactively prevent and dispute chargebacks.

Monitoring and Reporting: Monitor and report on transaction disputes and chargeback rates regularly to identify trends and areas of concern.

Collaboration with Payment Processors: Collaborate closely with payment processors to identify and address friendly fraud cases. Merchants should keep in mind that preventing friendly fraud requires a combination of proactive technology driven measures which are real-time and layered.

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

The below fraud types will require continuous attention of merchants.

Deepfakes and Synthetic Identity Fraud: As deepfake technology becomes more sophisticated, cybercriminals may use it to create realistic-looking video and audio content to impersonate customers or manipulate online transactions.

Biometric Data Theft: With the increasing use of biometric authentication methods, the theft and misuse of biometric data (such as fingerprints or facial recognition data) could become a significant concern for eCommerce businesses.

AI-Powered Fraud Attacks: Cybercriminals may leverage artificial intelligence and machine learning to automate fraud attacks, making it more challenging to detect and prevent fraudulent activities.

Social Engineering Attacks: Fraudsters may continue to refine their social engineering tactics to trick customers and employees into divulging sensitive information or authorizing fraudulent transactions.

Supply Chain Attacks: As eCommerce supply chains become more complex, attackers could target vulnerabilities in these chains to compromise product integrity or intercept deliveries.

Mobile Payment and Wallet Frauds: As mobile payments and digital wallets gain popularity, they may become attractive targets for fraudsters. Look out for trends related to mobile payment fraud.

Subscription Fraud: With the growth of subscription-based eCommerce services, subscription fraud could increase, with attackers exploiting free trials or using stolen credit card information to set up fraudulent accounts.

Cryptocurrency-Related Fraud: Phishing attacks, fraudulent Initial Coin Offering (ICO)s, or investment scams may be common in cryptocurrency.

Insider Threats: Employees or contractors could pose a significant threat if they engage in fraudulent activities or unintentionally expose sensitive data.

Serpil Hall
Head of Financial Crime and Fraud, Celebrus

- **LinkedIn**
- **Twitter**

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.

Chargeflow

Chargeflow.io

The Future Fraud Economy: Trends and Predictions for 2024

The best defense is offense. Or as I like to phrase it: proactive fraud strategies are far better than reactive tactics. The fraud economy is ever-changing—those ready for the evolving growth of schemes and scams outperform the unaware and underprepared.

Unfortunately, merchant and industry players do not own a crystal ball. You and I cannot script the future. But that doesn't mean we can't take steps to protect ourselves. Our current wealth of data does offer us a sneak peak. We can view current fraud trends and statistics and make some accurate guesses. Predictions based on educated analysis have long since defined an industry that continues to fight rapidly-changing fraud attacks.

As the year-end approaches, I find myself reflecting on the trends that will shape 2024. These trends may likely define how we combat fraud moving forward.

Fraud Trend #1: The Impact of Generative AI

First, we can't ignore the relevancy of generative AI. The value of the GenAI market itself is expected to reach $44.89 Billion by 2023. And with the influx of popular consumer AI programs, we may see growth rates at a whopping compounded annual of 24.40%. Estimates show Generative AI to reach a value of $207 Billion by 2030.

But with heightened focus and attention comes risk. Fraudsters are using AI tools to create new scams. For example, computer-generated voices can mimic the tone of loved ones over telephone calls. Or, criminals can use Language Learning Models (LLM) to manipulate text conversations over email or text. We have entered an AI-enabled fraud economy capable of exploiting human vulnerabilities.

However, the generative AI trend also has plenty of positive applications. We can use artificial intelligence to support cybersecurity measures. Typical defense solutions are static, with decisions made by strict rules (i.e. if not A, then B). But AI can improve upon itself. We can feed intelligent systems inputs that scale into dynamic solutions. In other words, AI can identify unknown deviations or patterns at a rate far beyond standard tech.

I think the cognitive learning capabilities of AI might help solve how merchants can stay one step ahead of the ever-changing fraud economy. It seems most enterprises agree: annual business spend on AI-based fraud defenses reached $6.5 billion in 2023 alone.

Fraud Trend #2: The Changing Role of the Human Analyst

Second, I see rapid changes in how we use and deploy fraud departments. Whether we like it or not, artificial intelligence can outperform a human at fraud detection.

Danske Bank introduced AI fraud detection systems and realized a 60% reduction in false positives. IBM AI can process 300 billion inference requests (transactions) per day. And generative AI can automate up to 30% of labor hours worked today by humans.

But even with those stats, I don't subscribe to the myth that AI will steal all our jobs. Instead, I think it will simply alter our approach to work. Technology still has limitations, from an inability to address context to creative or intuitive problem-solving. We still need humans to facilitate and manage our tech-based fraud solutions.

As a result, I expect the fraud analyst will take on greater importance. Yes, digital systems will handle routine tasks, but all high-impact fraud cases will filter to human specialists. We also need experts who can train these intelligent systems. And customer-facing fraud issues that require a depth of emotion are better served with a human.

Fraud analysts now are better defined as digital forensic specialists. They become your tech-enabled defense reps. Rules-based defenses with manual intervention are gone—in their place are fraud departments adept at data analysis, ML training knowledge, and payment technology.

Fraud Trend #3: New Efforts Against Friendly Fraud

Thirdly, I cannot fail to mention the problem of friendly fraud. Merchants continue to struggle with first-party credit card abuse. And for good reason: it is one of the hardest forms of fraud to identify. Simply put, there are numerous motives or reasons why a consumer might reverse an honest sale transaction. Are they forgetful? Abusing their cardholder rights? Or just feeling remorse? It might even be a case of true fraud. Deciphering between what is a false claim, malicious attacks, and honest consumer accidents is a challenge.

That's why I think we will see (and are already seeing) a renewed focus on friendly fraud. Chargebacks are too costly—anywhere from $20-$240 expense per $100 in disputes. No merchant should swallow the costs of false claims, so we need more efforts to help untangle the complexity of friendly fraud.

Already, there are numerous actions merchants can take to better identify friendly fraud. Comprehensive documentation and evidence collection help avert baseless disputes. Good refund policies, clear billing descriptors, robust customer service, and customer education campaigns help client-side efforts. And a suite of chargeback management can support risk scoring, alerts, and verifications.

Better yet, we are seeing an industry-wide push to help address the problem of first-party misuse. Visa introduced Compelling Evidence 3.0 this year, a step designed to help merchants fight friendly fraud. The new rules for evidence submission are more robust and account for factors such as previous consumer history and other digital order data. Such efforts will likely continue as the payments industry addresses the difficulty of first-party cardholder misuse.

A Look Into the Future Fraud Economy

Looking beyond 2024, we can make some informed predictions on how the fraud economy might evolve. Innovation will likely drive the next stage as defense teams and fraudsters leverage the available tools. I think the shows some growth in the following areas:

Biometrics: Experts estimate that the global digital identity market will be worth almost $71 Billion by 2027. The value of the security method comes from its ability to authenticate the unique aspects of a user without introducing undue friction. And the technology will only progress as it includes markers such as vein patterns and retina details.

Behavioral Analytics: We may also see an increased usage of behavior insights as anti-theft and surveillance systems. Digital tools set a baseline of typical consumer behavior and flag any suspicious deviations from that mean. Such behavior analysis will be indispensable toward the problem of friendly fraud identification. Little wonder the market is expected to grow at a compounded rate of 32.4% till 2031.

RegTech: Next, I think we may see attempts toward compliance standardization. At the moment, every regulatory body has complex compliance guidelines. And while effective, it also creates added difficulty and labor for merchants. To solve that problem, Regtech attempts to simplify those compliance processes. Shared efficiency can help limit the resource drain related to fraud defenses. That type of helpful automation and collaboration will be popular among numerous enterprises. Current estimates show the Regtech market increasing at a yearly compound rate of 22.6%

Defenses against novel fraud types: And of course, I believe we will see concentrated efforts to limit the damage of new scams. Synthetic fraud (where fraudsters combine fake and legitimate identity data) offers a good example, as "Frankenstein Shoppers" are estimated to drive $23 billion in losses by 2030. Other novel schemes include video deep fakes, fast fraud with peer-to-peer payments, Authorized Push Payment (APP) Fraud, and even criminal fraud-as-a-service organizations. We can prepare now for these growing threat types before they balloon into unmanageable issues.

Conclusion

It is impossible to completely predict how the fraud economy will escalate. And yet, data and trend analysis can help us outline a possible trajectory. That information can help us prepare defense postures that limit new attack types. Here are my recommendations for merchants as we enter the new year:

- Stay informed and update security as needed
- Use the latest Multi-factor Identification
- Invest in robust fraud and customer service departments
- Stay up-to-date on all compliance requirements
- Build a efficient chargeback management strategy
- Invest in AI-powered tools where possible
- Consider your risk level toward novel solutions
- Collaborate with other data and fraud screening partners

To that end, companies that continue to refine their defense strategies ahead of time are far more likely to maintain security. Proactive efforts will likely drive a positive return for advanced investors.

Ariel Chen
Co-Founder & CEO at Chargeflow

Ariel Chen, an Israeli-American entrepreneur, embarked on his Ecommerce journey at just 16 years old. After serving as a Technology Unit Chief in the IDF, he transitioned to Fintech in Florida, overseeing business operations. Together with his brother Avia, Ariel transformed bootstrapped projects into eight-figure Shopify powerhouses, serving over half a million global customers. Through Chargeflow, the Chen brothers now aim to reshape how online businesses handle fraud and chargebacks.

• LinkedIn

EverC

Everc.com

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

With its ability to create highly convincing synthetic content, Generative AI will undoubtedly have a significant impact on the fraud ecosystem. It can be harnessed by malicious actors for various fraudulent activities, such as creating forged documents, deepfake videos, and even convincing phishing messages.

In response, merchants will need to invest in more advanced fraud detection tools that can identify synthetic content. These tools will need to evolve beyond traditional methods to detect AI-generated fraud, including sophisticated machine learning algorithms that can analyze patterns and inconsistencies in data.

Ongoing monitoring of transactions and user behavior can help detect anomalies and potentially fraudulent activity as it occurs. This proactive approach can minimize the impact of fraudulent AI.

Merchants can also play a part in educating users about the risks associated with AI-generated fraud. By making users aware of potential threats and how to identify them, merchants can empower their customers to be more vigilant. In that same vein, merchants may also need to collaborate with other industry players and share information about emerging fraud trends. Collective intelligence can lead to more effective preventive measures.

Staying up to date with evolving regulations related to fraud and data security is essential. Adherence to compliance standards will be crucial in addressing AI-generated fraud effectively.

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

In an AI-dominated world, human fraud analysts will pivot toward more strategic and oversight roles. While AI can efficiently detect patterns and anomalies, human analysts will provide critical context, make nuanced decisions, and manage evolving fraud tactics. They'll focus on refining AI algorithms, adapting to new fraud trends, and fine-tuning the system's parameters. Human analysts will also handle complex cases, ethical considerations, and maintain the human touch in customer interactions. Overall, their role will shift from day-to-day monitoring to higher-level strategy, ensuring AI remains a valuable tool in the ongoing fight against fraud.

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

Unfortunately, today's risk management solutions are not robust enough to prevent persistent online fraud, which is preventing marketplaces from being able to focus on the business of driving growth. And based on the global cost of ecommerce fraud last year, it's a multibillion-dollar problem that needs a new approach.

Merchants must therefore consider implementing advanced real-time fraud detection systems that can promptly identify signs of fraudulent activity, allowing merchants to take immediate action. And they must establish clear procedures for resolving disputes to ensure that issues are handled efficiently and fairly.

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

In addition to being the most common method of online financial fraud last year, transaction laundering accounted for the largest increase in the first quarter of 2023, leading all other fraud types by 39%, and continues to be a concern.

As a known method to facilitate a range of financial crimes, the negative impact of transaction laundering is far-reaching. The anonymity provided by transaction laundering can enable criminals to maintain fraud rings across the globe, many of which have been connected to human trafficking rings or shown to support terrorist organizations. Criminals operating with the objective of transaction laundering will use approved merchants to process payments on behalf of another entity unknown to the acquirer or payment provider, thus violating the merchant's agreement with the latter. In essence, the traditional "car-wash" method of cleaning gains from illicit activity has moved online.

Tying as the second most common fraud, pharmaceuticals, intellectual property rights infringement, and gambling all accounted for 15% each of illicit payment activity. The illicit sale of pharmaceuticals without authorized prescriptions poses significant health risks to consumers, as these substances may not be safely tested. Intellectual property infringement, or the sale or distribution of unlicensed material without authorization from the rights holder, has exploded in the post-pandemic boom across ecommerce. Additionally, illegal gambling has grown due to ineffective anti-money laundering protocols on many gambling sites.

Accounting for 12% of illicit payment activity, illegal substances remain a top fraud type. Also ranking as a major fraud type, adult content makes up 9% of fraudulent activity, contributing to human exploitation. The sale of counterfeit goods is also a growing problem for the online marketplace. In the case of fake cosmetics, EverC was able to remove over 40,000 counterfeit products from its partnering marketplaces in 2022. This included perfumes (63%), skin care (16%), and make-up (15%), for a combined worth of more than $2 million.

Additionally, connections to terror financing will be a major trend. The U.S. Department of the Treasury's Financial Crimes Enforcement Network (FinCEN) recently issued an alert to help financial institutions identify funding streams supporting the terrorist organization Hamas. FinCEN is urging financial institutions to be vigilant in identifying and reporting suspicious activity relating to financing Hamas, and provided seven red flags to monitor. One example of a red flag is a charitable organization or NPO that receives large donations from an unknown source over a short period of time and then sends significant wire transfers or checks to other charitable organizations or NPOs.

FinCEN's rapid response is indicative of how much of a priority this issue has become with regulators.

Ariel Tiger
CEO

Ariel Tiger is the CEO of EverC, a cross-channel risk management provider transforming the internet into a more transparent and trusted place for ecommerce. Utilizing groundbreaking, AI-driven technologies, EverC' s scalable solutions power growth for global marketplaces, top financial institutions and payment providers.

Ariel's dynamic leadership encourages the global team to pioneer game-changing technology in an ever-changing industry. Prior to joining EverC, he was a founding executive at WeWork and M&A Investment Banker at Deutsche Bank Securities.

A graduate of the Naval Academy, Ariel spent years in commanding positions in the Israeli Navy. He holds an MBA from The University of Chicago Booth School of Business.

• LinkedIn

Featurespace

FEATURE SPACE

OUTSMART RISK

Featurespace.com

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

Generative AI has already made a big impact on our society, with use cases being identified across multiple areas of life, from academic to business and as with all new technological advancements, criminals are at the forefront of pushing its limits to take advantage of the slower moving legitimate members of society who are regulated by laws and morals. What GenAI provides to these criminals, is (and to use business parlance) a quicker route to market and a better ROI. It's massively scalable and requires little of the overheads that their organisations face, it also adapts with little human interaction making it harder and harder to identify either by a machine or by the human eye.

To combat this new threat, merchants need solutions that can scale alongside, with their own AI/ML solutions that can cope with high volume and high velocity attacks, that also adapt to the criminal's new weapon trading blows in real time.
With this in mind Featurespace has recently launched its own version of Gen AI in the form of a Tallier-LTM™ the world's first Large Transaction Model.

Built on the foundations of AI for Good, TallierLTM™ protects consumers and makes the world a safer place to transact. Pre-trained across billions of transactions using a self-supervised approach, making it highlyaccurateand representative of real-world consumer transactions, it can predict with high accuracy what the next transaction will be, in the same way that a LLM predicts what the next word in an email you're writing, flagging when there is a deviation from the expected and allowing you to take the appropriate action to protect yourselves and your customers.

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

The human mind can't compete with today's AI technology, we don’t have the speed or the analytical capabilities that a machine does, nor can we perform at the same level 24 hours a day, 7 days a week, 365 days a year. But what we do have is contextual knowledge, that it is (currently) very difficult to teach an AI solution. We need to identify each's strengths and weaknesses and use these to our advantage. There will always be a role for human analysts within a company's fraud strategy, machines can and should perform the heavy lifting taking away the repetitive tasks leaving the analysts to perform more in-depth investigations and interpret subtleties from our own real-world experiences that don't translate into algorithms.

We also have one thing that you can never train a machine on, and that is an emotional connection, we can see the human behind the transaction, not just the data presented on screen, but the mother, father, son, or daughter making a transaction using their hard-earned money which is especially tight at this time.

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

According to stats from the MRC, since Compelling Evidence 3.0's, launch 52,000 First Party Misuse Chargebacks have been deflected, valuing over $8,000,000. Currently, the deflection rate ranges from 45-70% at merchant with the aim to grow this number to 90% as the system improves.

Merchants need to ensure all departments are aligned and know what activity to look for, from customer service teams to those in the warehouse, there needs to be a joined-up strategy and processes to allow for a feedback loop to occur at all points of customer interaction. Fraud prevention is not just the remit of the fraud team, it's the responsibility of the whole company. Collaboration doesn't just mean speaking with other merchants, collaboration must start within your own organisation, share insights, trends, gut feelings with your colleagues across the business as to what your customers are doing.

It's unlikely there is anywhere else in your business with the amount of data at your fingertips than you do as part of your fraud strategy, are you using reporting to provide insight into customer activity, looking for trends and patterns that can translate to your fraud strategy?

Continuously monitor your customers and understand where and when they turned to the dark side, you need a (buzzword alert) 360 customer view to profile the good from the bad to be able to spot a customer who has decided to move from one to the other.
The cost-of-living crisis affects us all, and there will be customers who have transacted perfectly respectably for many years, who suddenly change their behaviour due to their own financial difficulties and have decided to turn against you. There are those new customers who follow social media "influencers" who want to try their luck at gaining the system, and there are those who just have bad intentions. All have their own specific signals they provide, and you need to understand these and share with your business to be able to stop them in their tracks.

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

Overlooked is perhaps too strong a word, Fraud teams are overstretched and face a continuous onslaught of orders to review and fraud to stop, they often don't have the time to analyse everything and there will be some trends that don't get the attention they need because you want the biggest bang for your buck. What is needed are solutions that level the playing field, that reduce the number of false positives and give teams the time to look at the actual fraud, gather and share intelligence to identify new trends more quickly. Having a solution that automatically adapts to behaviour and learns new fraud patterns itself isn't just a nice to have, it's imperative in todays fight against fraud.

With the speed and technologies that criminals have, as well as their networks of information sharing, we're on the back foot and will always be playing catchup to the new attack vectors they deploy. But it doesn't have to be that way, with technologies such as Featurespace's Adaptive Behavioural Analytics, and its new groundbreaking TallierLTM™ you can close the gap and be right on their heels frustrating them and forcing them to make mistakes.

Fraud will always change and adapt to the current environment, whether it be a global pandemic, a natural disaster, economic downturns, or the death of a monarch. Even the most successful fraud team cannot predict where the fraudster will go next, but they will be quick at closing the gap forcing them down another avenue of attack, and that can be achieved with an adaptive solution that learns what good behaviour is and identifies those activities that fall outside of what "normal" is.

Steve Goddard
Fraud Market Expert

Steve Goddard has worked within the fraud and payment industry for over 14 years, in the banking, travel and retail space. He has worked closely with merchants advising on fraud strategies as well as running operations teams. He has worked with Banks and PSPs globally in product management roles, leading major development initiatives to deliver solutions to external customers.

• LinkedIn

Identiq

Identiq.com

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

With Generative AI's rise, the fraud ecosystem will see a massive surge in successful spear phishing attacks that are highly customized to their targets on a personal level. The number of stolen credentials will increase exponentially, leading to a rise in all types of fraud rates.

Additionally, GenAI will equip fraudsters with the tools to defeat document, facial, and voice recognition systems, leading to increased identity theft. These tactics will largely affect FinTech, other regulated industries, and merchants that rely on such documents as part of their verification processes.

Merchants need to be prepared; to do so, they must begin analyzing their current defenses and identify areas of weakness. Whether new account fraud, ATOs, or credit card fraud, merchants should explore and adopt new technologies to limit their vulnerabilities. However, it's essential to note that many available tools cannot adequately catch GenAI's newly created identities. Instead, merchants should seek solutions to identify true identities and transactions that AI can't alter. For example, positive identification and data validation tools can determine that real credentials match up, whether it's a credit card connecting to the correct shipping address or an email address matching up with a phone number. These are attributes that can be relied upon.

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

When making decisions about what is and isn't real, a deep understanding is needed of how fraudsters operate and how the world works, which GenAI is incapable of. While GenAI can put together sentences or develop a story, it can't respond to anything in the real world and, therefore, can't detect new fraud patterns.

For example, GenAI can be trained to compute numbers by combining different parameters. But to the model, they are just numbers without meaning. With fraud, GenAI can't tell you how risky a number is, while an analyst can have many other conclusions to make when they see a high-risk score.

For the foreseeable future, analysts will be necessary to make informed decisions about fraud and AI will help them be faster and more accurate. AI can assist by helping identify similarities, take an analyst's findings and apply them at scale, or remove some of the manual work.

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

Merchants may hesitate to deny service or refunds regarding suspected first-party fraud. The “customer is always right” attitude and concerns about losing good clients create a lot of pressure. However, merchants can overcome this predicament and the increased rate of friendly fraud by adopting stricter policies and monitoring the behaviors associated with these types of fraud as well as the perpetrators. Technologies that can cross reference these data points will be crucial in identifying potential risk before the fact and fighting back against this.

Credit card policies need to be amended so that merchants have a fair chance of winning. Merchants should push for a revised definition of "compelling evidence" by payment providers. This would allow them to make rulings in favor of merchants rather than buyers in cases where legitimate evidence of first-party fraud exists rather than third-party fraud. The policies mentioned above will enable merchants to establish this.

Finally, merchants can refer to historical customer data to avoid expensive false declines or add additional preventative measures. When a consumer has previously committed first-party fraud, the likelihood of them doing it again is 100 times higher. Merchants possess this information and can work together, through peer-to-peer collaboration, to help one another identify potential fraudsters.

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

Many merchants and consumers heavily rely on one-time passwords (OTP). However, attacks on security measures are increasing, and 2024 will likely see a huge surge in fraudsters overcoming OTP.

Two factors are at play. First, for OTP to be effective, the networks where passwords are sent must be adequately secure. Whether SMS, email, or phone, there are many ways that fraudsters can bypass these networks, and they are doing so with ease. One type of attack is SIM swapping, where attackers trick a mobile network operator into transferring a victim's phone number to a SIM card they control. By doing this, the attackers can intercept one-time passwords (OTPs) sent via SMS and use them to gain unauthorized access to the victim's accounts.

Second, fraudsters employ social engineering techniques to extract OTPs from unsuspecting users. They can pose as customer support personnel or a real organization and convince users to share their OTPs.

As we approach 2024, merchants will face new challenges in preventing fraud. With advancements in technology, fraudsters will become more sophisticated in their tactics, making it crucial for merchants to be creative and explore new avenues of fraud prevention. However, this cannot be done alone. The community at large will need to come together and collaborate to create a safer online environment. This will involve validating trusted users through various means. By working together and utilizing the latest technologies, we can ensure that the online marketplace remains a secure and trustworthy place for everyone.

Uri Arad Co-Founder
CTO

Uri Arad, Identiq's co-founder and CTO, has been fighting fraud for over a decade, witnessing fraud and identity challenges from the perspectives of product, risk, and R&D. Previously, Uri was Head of Analytics and Research at PayPal's risk department.

• LinkedIn

Nethone

Nethone.com

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

Fraudsters increasingly leverage AI-enabled technology to automate their actions and produce new fraud streams. For example, Generative AI helps fraudsters create highly convincing synthetic data, images, videos, texts, and documents that can further support social engineering. In the wrong hands, AI technology enables the creation of counterfeit documents, fake profiles, and even voice recordings that closely resemble authentic ones. As a result, traditional fraud detection systems face the challenge of telling apart genuine activities from fraudulent ones.

Generative AI also contributes to developing advanced biometric authentication methods, such as deep learning-based facial recognition and voice recognition systems. These technologies increase transaction security and reduce the risk of fraudulent activities like the ones mentioned above. Merchants may consider integrating such authentication methods into their systems to prevent unauthorized access and protect their customers. What's more, Generative AI can assist in more accurate and granular behavioral analysis that merchants can use to create detailed user profiles and analyze user behavior patterns. In-depth data about the user helps detect anomalies and unauthorized activities more effectively, proving especially valuable in preventing account takeover and identity theft.

At the same time, merchants can get equipped with AI tools to increase their fraud detection performance. Machine learning models, including those built on generative AI, can analyze large datasets and identify patterns and anomalies that signal potential fraudulent behavior. Fraud prevention providers can leverage generative models to produce synthetic data to train their fraud detection systems and make them stronger and more precise to better serve their customers – ecommerce merchants.
Therefore, generative AI presents both challenges and opportunities for merchants when it comes to preventing fraud. It brings out more advanced ways to commit fraud, but it also provides resources to improve fraud detection, authentication, and behavioral analysis, ultimately improving the overall online transaction security.

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

Certainly, fraud analysts will play an important role, just as they've been playing so far. Even better, as AI technologies, including machine learning and generative AI, continue to advance, fraud analysts will have the chance to improve their working strategies. It's not about AI replacing human expertise, but human expertise taking value out of AI. And here's how.

Fraud analysis will continue to oversee the AI-based fraud detection systems. They will monitor the AI's performance, fine-tune algorithms, and ensure the system works as expected. Human oversight is critical to prevent false positives and negatives and, by extension, ensure the fraud detection system's precision.

AI is excellent at handling routine and known fraud patterns, but fraud analysts are better equipped to deal with complex and new fraud cases and trends. Take Generative AI, for instance — it's one of the best examples. They can use their experience and knowledge to investigate further and understand unique fraud scenarios and patterns that emerge over time.

Lastly, where fraud is suspected, analysts will still be the ones to review the case and interact with customers to confirm or deny fraudulent activity.

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

First of all, merchants need to adapt to the changes regularly made by card networks to combat new first-party fraud trends. For example, the most recent update from Visa is the Compelling Evidence 3.0 (CE3.0). This new protocol allows merchants to present records of previous transactions to counter false claims under the 10.4 reason code. Merchants would have a standardized framework to share information and make rock-solid cases during a payment dispute initiated by their users. If they can provide compelling evidence fulfilling the new requirements, the liability for the dispute will be transferred to the issuer.

As well, Mastercard will also update the compelling evidence requirements for several reason codes, such as Cardholder Dispute and Fraud. The evidence requirements will include more types of documentation and data that merchants can use to support the validity of a transaction or the delivery of goods or services.

To make sure they qualify for these updates that involve past transaction data for dispute resolution and evidence collection, merchants should keep detailed records of transactions, including IP addresses, shipping addresses, device information, and purchase history.

Friendly fraud sometimes stems from consumers' confusion when looking at their bank statements and not recognizing the transaction. And since we live in the era of convenience and speed, we can't expect the consumer to make investigations by themselves. The next logical step for them is to call the bank and file a dispute, thinking that transaction is fraudulent or an error. For situations when the customer doesn't recognize the transaction, merchants can adjust their descriptors to be easily matched with the brand name. Merchants should provide the desired updates for their descriptor, which may include changes in the name displayed or contact information.

As anti-fraud prevention measures, we recommend multi-factor authentication (MFA) or 3DS2, identity verification techniques to confirm the customer's identity, and real-time transaction monitoring systems that can detect unusual behavior patterns or high-risk activities.

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

From our position, we can't afford to overlook any fraud-related trend or topic. On the contrary, we constantly keep an eye on existing fraudulent activities and discover new patterns through extensive proprietary research on the Darknet and Clearnet.

At the payments and commerce industry level, we see a collaborative ecosystem where online businesses rely on each other insights and share their challenges with each other. So, there is an information-rich environment that helps everyone to be updated without missing key fraud trends.

Something that is not necessarily overlooked but could get more attention is the swift changes in consumer behavior. The industry should keep up with these changes before fraudsters do. Otherwise, fraudsters will better manage to impersonate and mimic genuine user behavior.

Another key aspect is the interconnected fraud sequence across the user journey. One form of fraud can trigger a chain reaction: social engineering may lead to account takeover (ATO), leading to payment fraud, eventually evolving into friendly fraud. This is just one scenario, and others can develop, such as synthetic ID fraud leading to account opening fraud, which may further lead to lending fraud. The concept underlines the importance of adopting a 'helicopter view' of fraudulent activities. While we don't assert that this aspect is overlooked, given the escalating trends in online fraud, there is certainly room for more proactive measures, such as identifying the potential root causes to stop them in their tracks.

Maciej Pitucha
Chief Data Officer at Nethone

- **LinkedIn**
- **Twitter**
- **YouTube**

Persona

Withpersona.com

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

Generative AI is set to significantly impact the fraud ecosystem. Most significantly, it will lead to an increase in overall fraud. Access to AI-generated scripts and malware lowers the entry barrier for cybercriminals, and fraudsters will harness AI to quickly identify and exploit vulnerabilities, even those considered "buried" or “exceptions.” As a result, the fraud landscape will evolve even more rapidly than it has in the past.

Furthermore, generative AI will supercharge all types of fraud, from identity theft to payment fraud — not just the kinds merchants are experiencing today. The speed, volume, and sophistication of fraud attempts will surge, resulting in increased financial losses.

With AI in the picture, merchants can’t just wait for fraud to hit and react when it happens. Instead, they need to adapt proactively, operating under the assumption that they are already at risk. Instead of writing off fraud instances as unfortunate losses, they should attempt to learn from the attacks and implement countermeasures. For example, they should ensure their existing tools can adapt to new types of attacks and handle high volumes of fraud attempts. Automation is non-negotiable, as it’s the only way to keep up with the scale of AI.

But merchants shouldn’t rely solely on technology, either — human intervention will still play a crucial role in the ever-evolving world of generative AI. However, fraud teams will need to evolve to adapt to AI-driven threats. Leveraging human intuition and the ability to contextualize investigation information will remain essential, especially as generative AI models rapidly understand more nuance and update the details of their output accordingly.

The impact of generative AI on the fraud ecosystem is already profound and has led to increased fraud attempts and losses. Merchants should prepare for the worst-case scenario, stay proactive, and continuously adapt to evolving threats. Fortunately, while the challenges are daunting, there are many opportunities to enhance fraud prevention by combining AI and human context and intuition.

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

In a world increasingly dominated by artificial intelligence, human fraud analysts remain crucial for several essential purposes.

Firstly, humans are needed to tweak and update workflow logic. While machine learning models can automate a lot of tasks, they are not immune to issues like score drift, where the model's effectiveness diminishes as it's applied to new types of fraud, leading to more false negatives and false positives. Human analysts can recalibrate the model by adjusting the logic based on their contextual awareness and experience, ensuring the model remains effective.

Secondly, human analysts provide valuable feedback for machine learning models. Training data for risk-scoring systems often relies on human input, as humans are often better suited to label and categorize data accurately. While the prospect of fully automating data labeling is being explored, human involvement remains essential for now.

Finally, fraud analysts will still need to review AI-generated outputs, as LLMs aren't industry experts — they're simply predicting what should come next in a sequence of words. This necessity is particularly relevant for official forms, such as Suspicious Activity Reports (SARs).

In an AI-dominated world, the core responsibilities of fraud analysts may not drastically differ from their current duties. However, the depth of investigation required will increase significantly.

Today, fraudsters can discover highly niche and deeply embedded vulnerabilities that are not apparent to the surface observer by using AI to systematically probe and discover weaknesses in systems — much like the velociraptors testing the fences for weaknesses in Jurassic Park. As such, fraud analysts will need to go deeper in their investigations to figure out what happened and how to avoid attacks in the future.

In short, while AI is transforming the landscape of fraud prevention, human fraud analysts will continue to play a vital role in shaping and fine-tuning automation, providing valuable feedback, and conducting in-depth investigations to counter increasingly sophisticated threats.

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

To combat new trends in first-party fraud, such as refund abuse, merchants may want to implement a number of strategies and mechanisms, including:

- **Identity verification during refund and claims processes:** Merchants may want to consider verifying customers when they attempt to initiate refunds or claims. For example, if a customer claims they never received a product, the merchant can ask them to submit their driver's license and a selfie to verify their identity. This approach adds an extra layer of scrutiny to discourage fraudulent activities. To mitigate risk while keeping user experience in mind, merchants can consider implementing a tiered approach — for example, using automation to verify individuals requesting low-value claims and automatically flagging claims with higher-value transactions for manual review.

- **Reverifying information:** To discourage fraudsters from using stolen or synthetic IDs, merchants can introduce elements that create pressure. For example, when initiating a refund, the customer might be prompted to provide additional information, such as personal information or purchase details, which can be challenging for fraudsters to provide on the spot. This approach aims to spook potential fraudsters into reconsidering their actions and providing accurate information.

- **Link analysis:** Most first-party fraudsters tend to be habitual offenders, making repeated attempts at fraudulent claims. Merchants should implement link analysis tools to identify clusters of suspicious claims associated with the same users. This enables them to spot and stop potential fraud rings. Preventing fraudulent claims beyond the first occurrence is essential — as the saying goes, "fool me once, shame on you. Fool me twice, shame on me."

In the battle against first-party fraud, stringent verification processes, accurate information, and link analysis are essential. Reducing the learning curve for fraudsters and making the process challenging for them is vital to protect against friendly fraud while ensuring customer satisfaction.

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

One of the biggest overlooked eCommerce fraud trends is the rising threat associated with faster deliveries and payments. The increasing emphasis on immediacy in transactions has led to an environment ripe for exploitation by fraudsters. Historically, the point of assessment for fraud has been at the transaction, which is understandable as fraud teams like to see the exact monetary amount that is at risk. However, given faster deliveries and payments, it's important to realize that the risk is now present as soon as someone creates an account on your platform.

Faster payments enable individuals and organizations to transfer large sums of money with remarkable speed and ease. But they also make it harder to recover stolen funds. Also, given the speed with which synthetic identities can be spun up in a GenAI world, accounts created en masse only further this risk exposure.

One of fraudsters' favorite tricks is impersonating legitimate entities and tricking victims into sending funds. Once a payment is sent, its rapid clearance leaves little time for error correction. Fraudsters quickly transfer funds to other accounts, making recovery difficult.

As faster deliveries and payments become integral in eCommerce, addressing the associated fraud risks is crucial. While measures like Confirmation of Payee (CoP) and the Contingent Reimbursement Model (CRM) offer some protection, continued vigilance, consumer intelligence, and a combination of preventative strategies are essential to counteract this emerging trend effectively.

Jeff Sakasegawa
Trust & Safety Architect

Jeff Sakasegawa is Persona's Trust & Safety Architect. With over a fifteen years of experience in the Trust & Safety space across companies such as Google, Facebook, Square, and Sift, Jeff is an expert on Risk Management and Compliance. He is passionate about ensuring safe online experiences for all users.

- **LinkedIn**
- **Twitter**
- **Instagram**

SEON

Seon.io

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

Generative AI will give fraudsters greater ability to extract money from both businesses and consumers. That's because, much like the internet, AI is open to everyone and there's a big incentive for fraudsters to adopt these tools.

With it they can run tasks faster, with greater speed and efficiency. For example, they can customize and tailor phishing messages in seconds. Phishing is already the most common form of fraud.

Fraudster's who couldn't code before are now able to build browser automation scripts that connect to residential proxies in order to scale up account take over (ATO) or automated check-out operations.

This can include re-using the credit card information or login details they would intercept through phishing, social engineering or by running fake webstores – which can also be built with generative AI-based codes.

Merchants need to implement the best tools and also use machine learning-based fraud detection solutions. Ideally, those should be whitebox, so AI can be supervised and maintained by humans at all times.

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

- Despite worries, humans will be needed for a long-time to come. They need to scrutinize AI, feed it the right data, analyze its output and share findings with other stakeholders.
- Fraud analysts need to make sure machine learning is being fed with the right data for their training model, which means pointing out the right false positives and false negatives in order to avoid disorientation in the system's accuracy.
- They can help the model make better assumptions by ensuring they use the right features from the merchant's side, and work cross-functionally across the business to understand what factors can be derived from each step of the customer journey. They need to capture and save these signals, translating them to features for the model.

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

- Merchants have to adopt solutions that collect data points from the customer's digital footprint, based on the collected data points during check-out. These are their name, address, email address, phone number and IP.
- If you can validate that your customer works at a specific company where the goods are to be delivered, or you find their home address in publicly available databases, you can use this to provide additional clues about the buyer – and whether they are who they say they are.
- Using a customer's email address, you can confirm their full name and check whether it's a legitimate email or one that's just been opened by a fraudster for the purposes of crime.
- Their IP also tells you if they are where they say they are. Perhaps geolocation shows a different address to the one given, that they are in a high-risk area, or they have masked their IP, which is another indication of fraud.

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

Automation has already started to play a significant role, but now with enhanced Gen AI powered tools ready to use, the possibilities are endless. Although we don't have a crystal ball, the overall growth trends are worrying. Credit cards remain one of the most desired digital assets for fraudsters to capture and re-use for illicit gains.

Tamas Kadar
Co-Founder of SEON

The Co-Founder of SEON Fraud Fighters, the Hungarian startup that broke funding records, Tamas Kadar is also the founder of Central Europe's first crypto exchange. In fact, it was serendipitous events right then that led him to start working on his own fraud prevention company, when he realized what was already on the market didn't cover his needs. Starting with the bold idea of utilizing digital footprints and social signals to assess customers' true intentions, SEON promises to democratize the fight against fraud. Today, the company protects 5000+ brands around the world as an industry-agnostic, fully customizable yet intuitive end-to-end fraud prevention solution that's highly ranked in the industry.

• LinkedIn

Signifyd

Signifyd.com

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

Generative AL will no doubt be deployed for a host of fraud use cases as time goes on. For now, we are mostly seeing the emerging technology being used by criminal enterprises to up their phishing game.

Generative AI means criminal rings can devise social engineering schemes that even savvy consumers can fall for. Rooms full of bad actors with gen AI at their fingertips can summon a professionally sounding email that appears to be from a well-known company asking the recipient to provide valuable, personal information.

Gone are the days of phishing attempts riddled with misspellings, poor grammar and indecipherable syntax. Generative AI can churn out convincing requests for personal information that will unlock accounts, provide credit card details and the other raw material fraud rings use to create synthetic identities or break into and take over existing accounts.

While all that is going on, black hats in the gen AI field are working on a new breed of generative AI called autonomous AI agents — in essence, fraudsters can move from running a script that does a repetitive task over and over again, to an AI agent that continually learns and improves its execution based on the goals assigned to it.

As generative AI matures and improves, fraud rings can operate with very little human intervention and with a relatively modest investment. As it would in any business, this creates great advantages in terms of scale, efficiency and economics.

Merchants, of course, are not standing still as generative AI marches on. Future-focused retailers are already engaged in a battle of AI vs. AI. Now they need to expand to the new arena by deploying machine learning systems that can understand the identity and intent behind every online transaction.

Such technological solutions can protect accounts throughout the buying journey — at creation, modification and checkout. In that way, they can stop account takeover and the creation of fraudulent accounts.

As for the coming attack of the autonomous agents, merchants need to depend on those with deep AI expertise to continually improve the models that successful retailers depend on today to identify the patterns that expose a fraudulent order. It is not different in kind from the work experts at companies like Signifyd are doing today to protect merchants. The rise of generative AI is simply the next stage of an ongoing battle.

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

Modern risk intelligence teams are no longer defensive players. They are business optimizers, who are able to increase profitability by maximizing the number of legitimate orders that are shipped to customers.

Risk intelligence teams built for our times have everything to do with creating a superior customer experience for digitally savvy customers who are showing that they are increasingly willing to abandon favored brands for another that offers a better price, better selection — and yes, a better experience.

Artificial intelligence is the risk team's partner in achieving the goals of increasing revenue and improving customer experience. Machines are fast and humans are smart. Machine learning models can evaluate orders at a speed and scale that no team of humans could achieve.

Automation ensures that orders are reviewed quickly so that fulfillment times meet customers' expectations in the age of Amazon. Finely tuned models ensure in milliseconds that legitimate customers' orders won't be declined for a misplaced fear of fraud.

But humans have the experience and intuition to recognize when the models need adjustment due to circumstances the models have not encountered before. Humans are capable of empathy and compassion. Few traits are more important in building a customer experience that will delight shoppers and keep them coming back.

Modern risk teams measure success by analyzing the extent to which they've increased conversions and reduced the time between order and delivery. They move the profit number and like other teams, they are wise to automate those tasks that can be automated while they focus on higher value initiatives.

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

A recent snapshot from Signifyd data shows that while payment fraud attempts were growing at a 34% annual rate, first-party fraud was increasing 36% year over year.

It's another reason fraud teams need to focus on the entire buying journey. When Signifyd asked consumers whether they'd ever engaged in first-party fraud, 21% and 22% respectively said that in order to get a refund, they had falsely claimed a package never arrived or falsely claimed that an order was significantly not as described.

The most successful online brands and merchants have applied some of their best practices in combating payment fraud to tackling first-party fraud. The primary goal of combining the speed and accuracy of artificial intelligence with the wisdom, intelligence and intuition of human risk professionals is to develop an understanding of the identity and intent behind every online transaction.

Building such insight requires a broad network of merchants whose many transactions establish the patterns of good and bad online behavior. A large network allows merchants to identify combinations of signals in a given order that have previously been present in friendly fraud attempts. That degree of vision into intent allows merchants to add additional friction to suspect orders while ensuring that good customers continue to have a seamless buying experience.

Finally, merchants need to be in position to make their case when confronted with an unwarranted first-party fraud claim. The time to prepare for that inevitably is before such a claim is made. Visa's updated compelling evidence rules, for instance, include very particular requirements for merchants to prove a first-party chargeback is illegitimate.

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

Merchants who overlook the rapidly increasing sophistication of organized fraud rings do so at their peril. The truth is, fraud attacks are growing in size, surprise and scope in part because of the industrialization of organized fraud.

A year or so ago we reached a tipping point. A fraud ring based in Southeast Asia sprung a holiday season attack in 2022 that was massive, efficient and relentless. In all, Signifyd estimated the operation made off with more than $600 million in goods from U.S. merchants in November alone. The ring was organized like a Fortune 500 company, exhibiting expertise in fraud, ecommerce, merchandising, fulfillment and cross-border commerce.

It was not that they were able to operate undetected; it was that once detected, they were able to pivot, add a new twist, and continue their attacks without changing targets.

The new rules of engagement require merchants to keep up with professional fraudsters when it comes to innovation. The building blocks are there: Fraud protection systems driven by artificial intelligence and fed by large networks of data. Deploying a data-driven, machine learning approach allows merchants to detect novel attacks quickly and to prevail even in escalating battles.

The same insights can be applied to the entire buying journey as fraud rings diversify — protecting accounts, securing the integrity of discounts, shutting down unauthorized reselling, identifying first-party fraud and vetting returns and refund requests to avoid post-purchase fraud and abuse.

In short, the network approach gives retailers the insight they need to turn away fraudulent transactions. More importantly, it gives retailers the confidence to increase conversion by allowing more legitimate orders and customer requests through. That's a win for customer experience, customer lifetime value and profitability. Exactly what modern risk intelligence teams are built to do.

Michael Pezely
Director of Risk Intelligence

Michael has been working in fraud detection and protection for more than 20 years, building and running organizations that tackle fraud and commerce risk. He's spent a career managing fraud, risk and business issues from online and offline marketplaces, user-generated content, phishing and social engineering, account security, payments, chargebacks, spam, botnets, cyberbullying, product quality, physical safety, intellectual property and compliance.

Before Signifyd, Michael held key roles at eBay and OfferUp. He is dedicated to protecting merchants and key commerce players from risk while constantly improving the customer experience they offer.

• LinkedIn

“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