



ECOMMERCE FRAUD TRENDS 2023

16 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

Introduction	3
Celebrus	4
ClearSale	8
Ekata	11
F5	15
Featurespace	18
Fime	21
Formica	25
Fraud.net	28
Fraugster	31
Nethone	34
Ravelin	37
Riskified	40
Seon	44
Sift	47
Signifyd	48
Vesta	55
About MFJ	58

2023 will be a year of huge change in 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 threats. It consists of interviews with thirteen 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 protect themselves. 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 five questions:

- What is the most important thing merchants can do to fight fraud effectively without harming the customer experience?
- What does an 'omni-touchpoint' fraud prevention strategy look like in 2023?
- What additional friendly fraud challenges will merchants face in a recessionary environment, and what is the best way to mitigate them?
- How should merchants be preparing for Payment Services Directive 3 (PSD3)?
- What will be the biggest 2023 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
 Dan Moshkovich—Co-founder & CEO

What is the most important thing merchants can do to fight fraud effectively without harming the customer experience?

Get to know your customer! After all, every customer wants an easy and good experience!

The more you know about your customers the less friction you will create in the customer journey.

A real-time, 360-degree view of each unique customer session is required for an accurate end-to-end view of the customer journey. This strategic approach enables merchants to enhance the customer experience across all channels. Singular insight from touchpoints aggregates relevant company-captured customer interaction data across multiple channels and from all available data sources. A 360-degree view of the customer allows the merchant to form a more detailed, trusted one-to-one relationship with the customer.

By aligning touchpoints, merchants can build a holistic view in real-time of who the customer is, why they are there, what they are trying to do, and what has been done before. The merchant who can get closer to customers' navigation patterns, timing, frequency, location, and how they end their sessions can tailor their service even better, reduce friction, and prevent fraud in time.

This 360-degree view of the customer enables merchants to view customer behavior patterns and provides the chance to appropriately intervene when required. By applying this new approach to gauge at-risk customer responses, merchants can determine which interventions create the best reactions from customers. Further, customer advisors and fraud prevention teams can replicate these actions for similar at-risk customers in the future.

What does an 'omni-touchpoint' fraud prevention strategy look like in 2023?

To provide a consistent and seamless customer experience merchants need to connect and support customers across devices and channels including live chat, email, SMS, social media, and any other means. As customers engage with a brand on any channel merchants should be able to respond effectively in real time. This requires a single customer identity to be maintained throughout the journey.

The merchant must be able to stitch the customer's identity through cookies, email, or login ID together to build an end-to-end singular view. Identity stitching and identity graph are important components of identity resolution and fraud prevention.

As part of the omni-touch fraud prevention strategy merchants must introduce anomaly detection to identify outliers in their customer data. This enables merchants to trigger an event when something 'unusual' happens. For example, a customer begins to use a new touchpoint or channel, but the actions don't match those of the other points of their journey.

Signals such as these can be then used for fraud analytics, decisioning, triggers, and audit.

Finally, we must remember that a detection system is essentially an alert system that notifies a merchant if an anomaly is detected. Whereas a prevention system allows a merchant to take action before any harm can be done. For this reason, prevention platforms are in demand for 2023.

What additional friendly fraud challenges will merchants face in a recessionary environment, and what is the best way to mitigate them?

Buy Now Pay Later (BNPL) abuse is a pressing fraud challenge merchants currently face. This fraud is a type of friendly fraud that is expected to be exacerbated in the current global recessionary environment going into 2023.

There are four types of friendly fraud:

- **Non-received merchandise:** The customer reports that they were charged by the credit card company, but the item wasn't delivered or received.
- **Credit card compromise:** The customer says they don't remember making the purchase so their credit card must have been compromised.
- **Never returned items:** The customer tells their credit card issuer that they returned the item to the merchant, but a refund was not processed.
- **Counterfeit return items:** The customer claims that the item purchased doesn't match the online description, and they don't want it.

There is no one size fits all mitigation for any of these challenges. Fraud moves quickly, and fraud detection must need to happen in real-time to allow for intervention and prevention. Merchants must deploy a combination of best practices, fraud prevention tools, fraud prevention platforms, chargeback management services, and payment solutions to mitigate fraud risk in the best way possible.

Merchants must know their customers well to achieve a true 360-degree customer view and fight fraud. It requires a layered approach that builds a complete digital footprint using all digital banking interactions, both transactional and non-transactional, pre and post-login.

How should merchants be preparing for Payment Services Directive 3 (PSD3)?

Payment Services Directive (PSD2) came into effect in January 2016 and since then many changes happened in the payments industry opening new opportunities for fraudsters. The Covid 19 pandemic led to rapid growth in the payment industry as consumer spending shifted online.

PSD3, the next evolution of PSD2, will focus on high-level consumer protection, with payment fraud prevention high on the agenda. Overall, PSD3 is expected to drive further innovation in payments and lending.

In the new directive, merchants can expect a number of changes from regulatory to process.

- Crypto, Buy-Now-Pay-Later (BNPL), digital wallet services, and payment processing services are unregulated, but PSD3 may look to regulate.
- The strong customer authentication (SCA) requirements period may extend from 90 days to 180 days to “reduce customer friction”.
- Greater specification of API standards, directory services, and infrastructure are expected.
- The addition of more diversified, cross-border payment solutions is also expected.
- Support for less expensive international payments by adopting global messaging standards.
- Support a seamless link for payment systems in different jurisdictions.
- New legal framework that covers all key players including the technology companies.

PSD3 will support the strategy’s objective to ensure the wide adoption of the highest security standards.

What will be the biggest 2023 eCommerce fraud trend that is currently being overlooked?

Merchant fraud prevention tools and systems must detect anomalies driven by changes in consumer behavior. These anomalies can lead to an intervention or perhaps a flag in the system suggesting that the individual’s activities might require further investigation or immediate intervention. If the merchant is sure that it is a scam, the session can be terminated immediately.

Real-time, first-party behavioral biometric data fraud prevention platforms offer this solution. Behavioral biometrics provide a superior alternative to other authentication, fraud detection, and fraud prevention methods. By allowing the identification of behavioral anomalies stronger protection against fraud is enabled. Behavioral biometrics uses multiple data points, such as how someone holds, touches, or taps their device, to guard against known and unknown attack types. These pieces of information are very difficult to replicate, but also need to be detected in real-time to stop fraud before it occurs.

Black box solutions are now outdated with a focus on assessing and comparing the collective audience behaviors on each individual process i.e., a money transfer, a loan, a credit card application, or an account opening. Black boxes assess a single point in time but do not compile or analyze a complete history of individuals in real-time, or over time. Black box solutions are limited in fighting fraud and scams, typically providing a risk score with no other information which can lead to false positives or false negatives.

Traditional transaction monitoring and rule-based decisions can no longer keep up with sophisticated scammers and fraudsters who are evolving at a frightening pace. Merchants now must look to real-time solutions that provide context to behavioral biometrics.



Serpil Hall
Head of Financial Crime and Fraud
at D4t4 Solutions, Celebris products

Serpil Hall is a fraud prevention expert whose career has spanned two decades and several industries.

She has earned industry accolades including 2022 Cyber Security Woman of the Year, in the Cyber Security Excellence Awards and is currently shortlist for Woman of the Year in the 2022 Cyber Security Awards. Serpil has held fraud roles with globally recognized brands including American Express, Visa, FICO, BAE Systems and EY. Serpil joined D4t4 Solutions 2021 to lead the Fraud Data Platform and continue to develop new fraud solutions.



ClearSale



ClearSale is an ecommerce fraud prevention solution with nearly two decades of experience, and more than 1,500 employees servicing 5,000+ brands (including enterprise retailers like Chanel, Walmart, Sony, and Rayban) around the world.

Clear.sale

What is the most important thing merchants can do to fight fraud effectively without harming the customer experience?

The most important things merchants can do to fight fraud without losing vital CX breaks down into two main ideas: fight the fraud that hurts your business specifically (which might not necessarily be all fraud), and ensure you are not causing false declines while doing so.

It's common to think that the better your fraud protection, the less streamlined your CX will be at check-out. However, if you understand the particular fraud schemes that are most likely to hit your business, you can tailor your fraud controls to suss it out without having to lock down your entire checkout with overarching protections to keep your CX secure and seamless.

Many merchants rely on the fraud systems provided by their ecommerce platforms. When seeing higher rates of fraud attempts, their fraud tolerance protocols will tighten, making it harder for good customers to complete transactions without barriers. Not seeing as much? It is tempting to drop some of your safety measures to make it easier for customers to place orders. The problem with this strategy is that fraud and false declines have a see-saw relationship: when you adjust the fraud algorithm to be more strict, you will start rejecting orders that are likely to be good and risk losing a customer for life. When you loosen those reigns, your fraud will skyrocket as you are approving all orders, good and bad alike.

Understanding this relationship and the limitations of fully-automated fraud protection will allow you to create a more personalized fraud protection plan that meets your security needs while still providing stellar CX.

What does an 'omni-touchpoint' fraud prevention strategy look like in 2023?

By opening up commerce to every digital touchpoint, consumers can interact with brands in new and exciting ways. The proliferation of mobile and social commerce and the onslaught of digital transformation tools are signaling to brands that it might be time to have a comprehensive omni-touchpoint fraud prevention strategy in place. With omnichannel retailers creating seamless customer opportunities for both physical and digital distribution, the most effective strategy will be one that can prevent and combat fraud from all angles – card-testing, account takeover, cross-channel, returns, mobile and social, just to name a few.

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.

What additional friendly fraud challenges will merchants face in a recessionary environment, and what is the best way to mitigate them?

Unfortunately, recessionary times can trigger higher friendly fraud rates as consumers are more inclined to take advantage of a system that will generally side with them, regardless of a merchant's proof otherwise.

This means that merchants may have to tighten up their fraud mitigation procedures on chargebacks that look like friendly fraud. Overall, the best way to mitigate this is to provide the kind of engaging experience and personalized support that will leave customers feeling so cared for that they wouldn't risk that relationship. However, it's a good idea to take extra security precautions now, such as clear and consistent communications on shipping, return policies that are easy to access and simple for customers to enact, robust support via phone, chat and email, delivery confirmations or signature requirements upon delivery, and keeping detailed transaction records so that you have the evidence needed to show the integrity of any transaction. And, if a chargeback does occur that has indications of friendly fraud, extreme measures can be taken (such as recording a call validating the order), but hopefully, this would only be a worst-case scenario.

How should merchants be preparing for Payment Services Directive 3 (PSD3)?

New regulations in the checkout process can be a hiccup for a merchant if they are not prepared. With the discussions surrounding the upcoming PSD3, it is more important than ever that merchants understand how a new SCA system will affect the CX of their site.

PSD2 allowed consumers to gain access to financial data and initiate instant payments by giving their consent to a third party. But, as new solutions like digital wallets, BNPL, and crypto assets continue to emerge, updated regulations are needed to extend the scope of payments. PSD3 seeks to address the gaps and outdated rules of PSD2 and more appropriately cover areas that are important for the EU payments landscape.

In order to prepare, merchants can take time to understand how their business meets the PSD2 regulations currently, while thinking about what will be asked of them to become compliant with PSD3 and making those changes over time. Utilizing this 360 scope will minimize losses while providing excellent CX to customers.

What will be the biggest 2023 eCommerce fraud trend that is currently being overlooked?

The metaverse is taking off and the possibilities seem limitless for tech giants and brands looking to get in on the early-adopter potential. And while digital payments may look the same in this emerging e-commerce environment (with a heavy leaning on crypto and blockchain payments), the fraud risk is unique and I believe we will see many vulnerabilities being exploited before the fraud prevention world gives the metaverse the attention it is due.

Blockchain has famously been the technology of choice for fraudsters, and they are years ahead of CNP fraud professionals on how to launder money, steal identities and implement complicated fraud schemes with this payment method. For all other payments, the lack of regulatory measures on certain platforms gives fraudsters an open field to test out new methods and enjoy nearly risk-free attempts to defraud both companies and users.

The metaverse is the new frontier that should be a significant consideration for the fraud prevention industry. The more we know about it, the better we can ensure that people can safely and confidently participate in metaverse commerce.



Rafael Lourenco
EVP & Partner, ClearSale

Rafael Lourenco is Executive Vice President and Partner at ClearSale, a global card-not-present fraud protection operation that helps retailers increase sales and eliminate chargebacks before they happen. The company's proprietary technology and in-house staff of seasoned analysts provide an end-to-end outsourced fraud detection solution for online retailers to achieve industry-high approval rates while virtually eliminating false positives.

Follow on LinkedIn, Facebook, Instagram [Twitter@ClearSaleUS](#)

Ekata



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

[Ekata.com](https://www.ekata.com)

What is the most important thing merchants can do to fight fraud effectively without harming the customer experience?

We all have high expectations for fast, seamless and low-friction digital experiences. But to make that happen, it's important to first understand identity and the critical role it plays.

For years, we have defined identity in narrow scopes for specific purposes. For example, government-issued IDs like driver's licenses and passports—documents used to prove an individual's identity as part of the verification process. In today's digital world, however, identity is much more complex and includes inputs like personally identifiable information (PII), purchase histories, location data, and IP addresses.

But verifying one or two identity elements inputs isn't sufficient. Given how sophisticated fraudsters have become, we need a more holistic view to determine if someone is who they say they are. We need to evaluate multiple identity elements, how those elements are linked together and if they are tied to a genuine consumer. If we don't expand our current perception of digital identity, we risk making it too easy for fraudsters to find the edges and go around the processes we have in place.

Digital identity verification technology provides a strong risk indicator, helping merchants find the right balance between fighting fraud, without sacrificing a great customer experience. The lower the risk, the smoother and faster the customer can move through their journey. For higher-risk transactions, merchants can layer on validation methods and add authentication tools to increase friction for potential fraudsters. Finally, when necessary, they should manually verify information at the bottom of the flow. We call this "strategic friction."

Many companies have a fraud solution in place, and they think they have it covered. But it is important to strike a balance between technological tools and manual processes to reduce risk at every turn. An Ekata survey found that 70% of companies used three or more tools to help make this incorporating-friction-process smoother. So, just because you have an existing fraud platform or home-built solution does not mean that an enhancement by a different solution should automatically be ruled out. Look for a set of capabilities that can be tuned to your business and the type of end customer that you are dealing with.

What does an ‘omni-touchpoint’ fraud prevention strategy look like in 2023?

Propelled by the pandemic, the ecommerce industry is evolving quicker than ever before. While much of the change is driven by consumer expectations (more personalization, instant gratification, and frictionless checkout), merchants are also evolving to improve experiences and limit fraud.

Even as merchants roll out sophisticated new products and services to better serve their customers, online fraudsters are innovating as well. Their evolving tactics take advantage of the creation of new customer accounts, looking for weaknesses to exploit throughout the customer journey. As a result, fraud isn't just taking place at the point of transaction; it's happening across the customer journey. Every time a merchant and customer connect, that's an opportunity for fraudulent activity. Some of the most common fraud touchpoints include account creation; account updates; payment authorization, fulfillment; loyalty and retention; and returns.

Since fraud is happening throughout these touchpoints, the first challenge is to detect it early, before the damage occurs, and the second is to stop it in its tracks if fraudsters manage to get past initial checks. Successful ‘omni touchpoint’ strategies include the use of fully automated fraud prevention platforms, machine learning (ML) models, behavioral biometrics, and other technologies that increase friction for fraudsters across all sessions and interactions.

Fraudsters are looking for the weakest link in the chain, which means businesses should have a fraud prevention strategy that extends beyond their own walls to align with PSPs, acquirers, issuers, and others.

What additional friendly fraud challenges will merchants face in a recessionary environment, and what is the best way to mitigate them?

Friendly fraud can happen for a variety of reasons – it's whenever a customer makes a legitimate purchase, but then later disputes it with their issuer. Often, these types of disputes arise because of a service issue – like goods not received – or simply because a customer didn't recognize a purchase on their statement and assumed it must be fraudulent.

While the causes of friendly fraud disputes may vary, the solution is often the same – giving consumers more details upfront about their purchases, where and when they review them, to provide clarity. For most people, this is in their digital bank channels. Providing clear details like merchant names and logos together with full digital receipts, can help clear up that transaction confusion the moment it occurs, and minimize the resulting disputes.

What will be the biggest 2023 eCommerce fraud trend that is currently being overlooked?

In the past year, over half of ecommerce companies experienced promotional abuse, where fraudsters take advantage of limited-time promotions, causing retailers a significant loss. Bad actors can also combine real and fake data (such as an address from one person mixed with another's social security number) to create a new, synthetic identity that is harder to detect. Then they open new accounts. Synthetic identity fraud is damaging for consumers and costs businesses billions of dollars annually.

Marketplaces have also seen more malicious users impacting platform integrity through policy abuse. This drives the need for strong measures to keep bad actors off a platform entirely or limit their movement. According to Ekata's research, almost one-quarter of shoppers abandon carts because they're asked to create accounts, meaning that, even with rising fraud, a streamlined sign-up process is still key to driving customer acquisition.

In today's rapidly evolving fraud landscape, companies can't risk viewing fraud as another cost of doing business. Marketing and customer acquisition teams need to be working hand in hand with their fraud teams—promotional and policy abuse are just the tip of the iceberg. The longer-term impact is that organizations may not be acquiring real customers at the rate they think. This makes it difficult to plan for future monetization of the customers in the merchant's system. It also allows fraudsters to circumvent traditional fraud prevention strategies.



Beth Shulkin,
Senior Vice President, Global Marketing

Beth leads Ekata's global marketing team. She has 20 years of experience in strategy, product, and marketing, spanning several industries including, finance, communications, digital marketing, and data API technologies.



Let's Fight Fraud Together

*Detect over 80% of suspicious
online activities with the power
of Ekata Identity Engine*

Discover the Ekata responses that are best fit for your business.

[CONTACT US TO LEARN MORE](#) 



F5



[F5.com](https://www.f5.com)

What is the most important thing merchants can do to fight fraud effectively without harming the customer experience?

To fight fraud more effectively, merchants must better align and converge their security, customer identity and access management (CIAM), fraud detection, and authentication strategies by implementing an agile, reliable, low-noise fraud detection and mitigation program that adapts as quickly as criminals do.

Aligning and converging multiple security strategies is more important than ever because criminals are exploiting vulnerabilities that have been introduced by organizations working in silos and security strategies that leaned too heavily into CAPTCHA and multi-factor authentication (MFA) techniques. These mechanisms continuously interrupt the user experience often without context of the risk level associated with the user's activity.

Implementing a transparent and continuous risk-based authentication approach allows merchants to better collaborate across their organization, reduce MFA bypass attacks, move towards a passwordless and more reliable authentication strategy, and provide ways to reduce fraud without negatively impacting the user experience.

What does an 'omni-touchpoint' fraud prevention strategy look like in 2023?

Merchants should expand beyond their traditional "omni-touchpoint" strategy for fraud prevention to ensure they gain more holistic visibility and insights across every channel the customer touches throughout the entire customer journey. This strategy should include three often overlooked key areas:

- 1. Initial channel engagement:** Focusing on when the customer initially engages will allow you to gain insight into activities from the moment a customer enters a channel or creates an account. This should also include improving visibility into client-side attacks like digital skimming or formjacking, which are often used to harvest credential and card information during new account origination, ultimately leading to account takeover and fraud.
- 2. Third-party API integrations:** While most merchants have focused on securing their web and mobile apps, they must now also ensure they include API protection in their security strategies. APIs are subject to the same attacks that target web apps, namely exploits and abuse that lead to data breaches and fraud, and introduce unintended risk from third-party integrations and ecosystems.

3. Blurring of Card not Present (CNP) and Card Present (CP) transactions: Merchants that offer new services such as proximity-based checkout, buy online and pickup in store (BOPIS), and buy now, pay later (BNPL) must understand the risks that these transactions entail and address them in their fraud prevention strategies. This includes gaining insights into fraudulent behavior patterns and sharing it across all channels.

What additional friendly fraud challenges will merchants face in a recessionary environment, and what is the best way to mitigate them?

Merchants should expect that legitimate customers will continue to conduct traditional friendly fraud and chargeback fraud scams. However, the biggest new type of friendly fraud merchants should expect to see ramp up during a recessionary environment is “fake friendly fraud.” This occurs when criminals create synthetic identities to appear like a real customer and then transact with no intention of paying for the merchandise they purchase. These friendly fraud activities can include buy-now, pay-later (BNPL) program abuse, loyalty point and refund fraud scams, and bust out fraud.

Criminals know that many merchants watch for patterns of repeat friendly fraud and create deny lists of violators to stop this type of exploitation. However, fake friendly fraud practitioners can successfully game and bypass prevention efforts because they can easily recycle stolen identity info and create new synthetic identities to open new accounts and avoid being blocked by a deny list.

Organizations can protect against new account enrollment with synthetic identities and account takeover fraud by leveraging insights from behavioral biometric patterns augmented with machine learning to give both security and fraud teams insights into compromised accounts.

How should merchants be preparing for Payment Services Directive 3 (PSD3)?

PSD2 acted as a positive forcing function to modernize and shine a light on gaps, risks, and opportunities within the payment ecosystem. However, since that directive’s initial 2018 rollout, the threat, payment, and regulatory landscape has dramatically changed. To prepare for PSD3, merchants should take inventory of new services, channels, and payment options they have adopted over the past several years. For example, are they now supporting digital wallets and crypto payments? How many new APIs with different formats from third party providers (TPPs) have they integrated?

Merchants should expect changes to the Strong Customer Authentication (SCA) requirements and start to explore how they can address the realities of modern cyberattacks that leverage malware to conduct exploits like MFA bypass techniques. Also, merchants should consider adopting modern authentication strategies that reduce user friction by dynamically aligning verification requirements to the level of risk presented by the log-in attempt.

Understanding these advances will allow merchants to prepare for PSD3 and to move from just focusing on a compliance–risk mindset for their existing API and authentication strategy, to proactively anticipating and managing the full scope of security and fraud risks that the modern open–banking API ecosystem brings.

What will be the biggest 2023 eCommerce fraud trend that is currently being overlooked?

Shadow API and JavaScript supply chain attacks are the most overlooked fraud trends merchants should focus on in 2023. That’s because criminals know that many organizations struggle to manage, track, and secure the volume, scope, and scale of scripts now embedded into websites, and they know how to exploit these scripts for their own gain.

As organizations expand their third–party ecosystem and the number of scripts on their site, they introduce new potential points of vulnerability that lead to client–side attacks such as digital skimming, form–jacking, and Magecart attacks. A digital skimming attack occurs when a criminal either injects one or many malicious script(s) or manipulates an existing script on a legitimate page or application to create a software supply chain man–in–the–browser attack. These attacks are difficult to detect since these scripts are updated frequently by third parties, often without a process for your organization to perform security reviews.

Most organizations do not have centralized control and governance over script management. If a third–party script on your site has a vulnerability and you are not aware of it, you are unable to patch it – opening the door for an attacker or exploit. This has become such a large issue that the new PCI v 4.0 guidance recommends that organizations only include “required” scripts on the pages that collect PII and payment information.

Organizations not only need visibility into the JavaScripts on their site, they also need to know what data the scripts are collecting to prevent violating data privacy regulations like GDPR and CCPA and maintain compliance with the new PCI DSS 4.0 requirement 6.4.3 and 11.



Angel Grant, CISSP
Vice President, Security Product and Market Strategy
F5 Security

Angel Grant is a visionary leader with a passion for developing and evangelizing cybersecurity, fraud prevention and risk management solutions to help make our digital world a safer place. She has over 20 years of experience in cybersecurity, eCommerce and financial services industries with a background in product development, marketing and sales. In her current role, she is the Vice President of Security Product and Market Strategy for F5. Prior to this role, she held various positions in RSA Security authentication, identity, fraud, risk and threat intelligence teams. She has influenced many industry initiatives while serving on the, PCI Council Board of Advisors, Federal Reserve Secure Payments Task Force, FS–ISAC Board, Nacha’s Payments Innovation Alliance Risk, Regulatory and Security Advisory Committees. She is also a prominent diversity evangelist, author, spokesperson, and is CISSP certified.

What is the most important thing merchants can do to fight fraud effectively without harming the customer experience?

Collaboration and data are the two key areas that Merchants should be looking at;

Collaborate with Issuing banks to get a better view of the consumer. They know things you don't, and you know things they don't, so let's break down those silo's and share information for everybody's benefit. Collaborate with other teams within your business, what are the marketing team working on and how will it affect your alert rates? What are the customer service team seeing and hearing, what insights can you gather from them?

&

Ensure you have the best data available to make the decisions you're making. If there's additional fields, you have access to that will give you better insight then use them. Is all your data in one place or is it fractured? Do you know what data you have and what its possibilities are?

What does an 'omni-touchpoint' fraud prevention strategy look like in 2023?

As consumer demands for a frictionless multichannel solution increase, then so does the need for a fraud prevention strategy that can look across all these channels and adapt to changes in behavior, such as those seen during lockdown when most of us switched from card present transactions to card not present. Whether payments trends develop naturally or whether they are forced upon us by global events, the need to be responsive without the need to retrain models or rebuild your whole strategy is imperative as these take time that we don't have and result in customer friction, abandonment and potentially the loss of customers business.

What additional friendly fraud challenges will merchants face in a recessionary environment, and what is the best way to mitigate them?

Expect to see an increase in "offers" to help you beat the rise in fuel, food, and energy prices as criminals leverage people's fears and concerns during what is potentially going to be a very hard time for a lot of consumers.

In today's visual society, we face greater pressure to have the latest toys, gadgets and holidays, which sets an expectation that can be hard to fulfil at the best of times, but a holiday season during such a fierce economic climate is a perfect storm for those looking to exploit for their own gain.

We are already seeing the start of these attacks, as scams involving electronic stores offering discounts and free goods to entice consumers to share their details before having their accounts emptied as well as energy rebate scams offering an enticing way to recoup some of the huge rise in prices.

It's not just the criminal gangs that you need to worry about, but also those desperate consumers that turn to the dark side to ensure their holiday season isn't ruined. There is documented evidence showing a link between economic down-turn and a rise in first party fraud. It seems such an obvious connection, and just because you know it's coming it doesn't mean you can take it likely as it'll happen at the same time your order numbers increase as we start to enter peak period.

Several years ago, I used to manage a team of fraud fighters looking after alerts for a number of e-commerce merchants, and I still remember the 12-hour shifts, the 1000's of alerts to work through day after day during peak period. It was tiring, stressful and trying to keep my team motivated was hard despite their passion and adding into the mix yet another fraud typology to look out for was a difficult conversation to have when there was no time to investigate and fully understand it.

Thankfully times have changed and with the introduction of machine learning, easy to use analytics and access to data scientists it means that teams no longer have to work like this and can use their time more efficiently, helping customers and investigating more complex cases.

How should merchants be preparing for Payment Services Directive 3 (PSD3)?

Firstly, I'd ask whether we should be looking at PSD3 or PSD2.1, inherently the changes were good, although possibly not rolled out in the best way, but do we need drastic changes or just tweaks to what we already have?

Merchants should be assessing the impact of PSD2, what went well and what did not go so well. One of the key points of feedback I've heard is about how the gaps have been exploited, especially with BNPL, which is not covered by the existing PSD2 regulations. These gaps need to be addressed and closed as quickly as possible, and greater emphasis should be placed on these by merchant fraud teams. Just because PSD2 doesn't cover them, doesn't mean they shouldn't be a key part of your strategy, as one of the most common bits of feedback I hear is that the language was very vague and could be interpreted differently. Whilst you need to adhere to the directive, you also know your own business better than anybody else, and will know where they fall short of full protection.

What will be the biggest 2023 eCommerce fraud trend that is currently being overlooked?

I've written here about how I don't believe that fraud teams are overlooking any fraud trends intentionally, only due to inefficiencies and increased workloads that have become part of the job. Fraud teams must be as dynamic as the criminals they fight against, but this isn't as easy as it is for the criminals as they don't have regulations and procedures to work within.

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.



Fime



Fime enables its clients to create and launch trusted and secure solutions with consulting and testing services in payments, smart mobility, biometrics, authentication and open banking. It offers global cross-industry perspective, local insight, and unique heritage in testing and certification. Fime's consultants provide transformative business expertise, partnering with organizations worldwide to define, design, deliver and test their products and services.

With 400+ experts around the world, Fime works strategically to help its clients turn ideas into reality, swiftly take products to market, and achieve competitive advantage. Working together, Fime turns powerful innovations into the future of trusted transactions.

Fime.com

What is the most important thing merchants can do to fight fraud effectively without harming the customer experience?

Fighting fraud starts with a suitable fraud detection program. Unfortunately, we often see merchants with deficient systems, or even worse, none. Merchant risk analysis processes should take three major aspects into account:

- 1. Transaction context.** It is essential to gather relevant data during the user journey on the merchant's site. Coupled with AI or profile-based learning, such mechanisms can analyze behavioral patterns and prevent suspicious activity. Data that can be collected for this purpose includes order date, shipping and billing addresses selected, item purchased, support requested, and amount spent on a transaction. However, it is worth noting that merchants must be mindful of local regulation, such as GDPR, which may impact this practice.
- 2. Third party limitations.** The data gathered goes through a third party, such as a browser or mobile platform. Limitations imposed by third parties may block or reduce system capacity to retrieve information. For example, web privacy settings and browser updates can limit user data sharing with external parties, or add more controls (e.g., user-agent reduction). It is important to adjust the system accordingly to mitigate the impact of these limitations.
- 3. Card network frameworks.** Many card networks provide dedicated frameworks to help merchants fight fraud. These include chargeback protection, liability shifting, friendly fraud support and authentication programs. As issuers rarely state the explicit reasons behind declined payments, some networks also provide reason codes to give merchants more data, helping them to calibrate their systems.

Having strong and efficient fraud detection programs in place throughout the shopping experience avoids the need for disruptive interactions (e.g., strong customer authentication performed by the issuer bank), which can contribute to a poor user experience.

What does an ‘omni-touchpoint’ fraud prevention strategy look like in 2023?

During the pandemic, many merchants experimented with new retail strategies, such as ‘buy online, pick up in-store’. Now people are more accustomed to an omnichannel approach, and aware of the benefits this provides. Based on this success, merchants have opted to restructure their offering to cater to this trend. But with an omni-touchpoint approach comes new fraud patterns.

Even if threats remain mostly the same as with traditional retail channels, the way to fight them differs. Having multiple points of sale increases the attack surface and velocity. For instance, fraudsters can purchase goods online and pick them up rapidly, reducing the likelihood of the fraud being detected prior to this point. This can also be exploited during the returns process. In this instance, fraudsters can make a purchase via one channel and return the goods to another channel, bypassing the usual returns process.

An efficient fraud prevention strategy must deploy fraud management tools across each channel and implement processes to ensure cross-fraud detection. The security of authentication methods must be consistent across channels to avoid any weak points in the system which could be exploited.

What additional friendly fraud challenges will merchants face in a recessionary environment, and what is the best way to mitigate them?

In a recession, more people could be tempted to deceive retailers by requesting chargebacks for genuine purchases and then reselling the product, as a way to cope with financial difficulties. This situation would raise chargeback volumes and may exceed the acceptable threshold of chargebacks set by the card networks. If this was the case, merchants would need to rectify this or face dire consequences. In the first instance, merchants which exceed this threshold must propose a plan to lower chargeback rates. If chargeback rates do not reduce during a set period, merchants must pay fines. This results in triple pain for the merchant: lost revenue, chargeback costs and penalties for exceeding the chargeback threshold.

To avoid this, merchants should focus on the following areas:

- 1. Friendly fraud detection.** Improving fraud detection engines with profiling or behavioral patterns will help to detect suspect customers, and the goods or timeframes most subject to this fraud.
- 2. Chargeback management.** This can often be a lost battle for merchants for many reasons, such as missing the deadline for disputing a claim, or having a lack of evidence or not enough data from the acquirer. However, there are card network programs which provide merchants with support in this area. For instance, Visa and Mastercard offer initiatives, some of which guarantee liability shift, chargeback wins and prevent merchants from exceeding the acceptable threshold of chargebacks, allowing them to avoid costly fees.
- 3. Product delivery.** A lack of traceability when it comes to goods delivery can be exploited by fraudsters. To solve this, merchants could improve payment descriptors to decrease any doubt on banking account ledgers. They could also enhance delivery to provide more data throughout the process, which could be used in an investigation if required.

Taking these steps to prepare in the event of increasing volumes of friendly fraud due to the recession is key for merchants looking to diminish losses in this area.

How should merchants be preparing for Payment Services Directive 3 (PSD3)?

The European Banking Authority (EBA) plans to strengthen regulation to reduce current fraud, which is made possible by a lack of requirements. While PSD3 regulation is still under discussion, the EBA has already indicated which trends it is focused on, and provided its opinion regarding feedback received from industry participants.

One area that the EBA is focusing on is instances where merchants classify remote electronic payment transactions as MIT (merchant-initiated transactions) or MOTO (mail order/telephone order) to avoid the need to comply with SCA (Strong Customer Authentication). The need to adjust regulation to reduce user friction, and consequent cart abandonment, is recognized. However, this practice goes against the objectives of SCA and therefore must be prevented.

The EBA will clarify multiple aspects in relation to the application of the regulation to support merchants with their implementations. To name a few, the EBA will look to clarify the nature of exemptions from SCA, distinguish the difference between 'fraudulent acts' and 'gross negligence', explain the distribution of liability and make the application of dynamic linking clear.

Merchants not wanting to be caught out must take action now, even more so now that the EBA has introduced sanction mechanisms for companies which do not comply on time. As a start, merchants can use more SCA exemptions and delegation processes to reduce user friction.

What will be the biggest 2023 eCommerce fraud trend that is currently being overlooked?

Instances where fraudsters usurp the identity of trusted organizations are the most frequent attack vector. Fraudsters are innovating to carry out SIM swapping, social engineering and increasingly sophisticated and organized scamming methods (e.g., phishing). Even well-established players in the market, such as Apple Pay, have recently suffered from such attacks. With usurpation, many threats have been identified, such as carding, cashing-out and account takeover.

Finding authentication technology that is 'scam-proof' is top of the agenda for many payment industry working groups. For example, industry bodies FIDO Alliance, EMVCo and W3C are working together to strengthen payment authentication technologies. Fime is proud to actively participate in such industry groups to work with industry stakeholders to develop solutions which fight fraud.

In particular, FIDO Alliance and W3C have produced a biometric-based authentication method, which is supported within the latest version of the EMV® 3-D Secure (3DS) Specifications. There is by no means a lack of solutions out there to address the problem of fraud – but are merchants fully informed on how best to tackle this?



Jean Luc Di Manno

Solution Architect & Payment and Authentication Expert

Jean Luc has 10 years' experience in the industry. At Fime, he started as Trainee Software Developer. In his current role, he works with customers to identify their needs and help them select the best solution for their business.

He specializes in the payment ecosystem, digital identity and authentication. He has designed certification tools for technologies such as EMV 3DS and ISO 8583. He provides consultancy on the technical level, regulation, specification details and payment scheme requirements that stakeholders must navigate when introducing new technologies.

Jean Luc is involved in industry groups, such as the Web Payment Security Interest Group, which aims to enhance the security and interoperability of web payments.



What is the most important thing merchants can do to fight fraud effectively without harming the customer experience?

When merchants offer a customer experience, the payment process is a part of this journey. Securing the payments and adding too many steps can lead to the abandonment of the transaction. On the other hand, if merchants loosen the security measurements and potential buyers face a problem, they might change their minds and renege on their transactions. When it is the case, merchants should keep the balance.

The most crucial point to be considered by merchants in detecting fraud is the false positive phenomenon. Confusing fraud activity with real customers is an action that can profoundly damage the customer experience. Putting the two in the same basket in the filtering process may result in the actual customer breaking his heart and moving away from shopping or even from that e-commerce platform altogether.

While examining the false-positives, with the proper filtering process and even the most suitable risk platform, the sorting should be done automatically without muscle power, and the customer should be prevented from wasting time. If I had to summarise, the process must be continued seamlessly and must work flawlessly especially with the right platform.

What does an ‘omni-touchpoint’ fraud prevention strategy look like in 2023?

Regardless of offline, online, wallet or p2p payment, Merchants should monitor all data on a single platform. At this point, it is vital to observe the risk process 360 degrees by looking at multiple issues instead of focusing on a single perspective. Using different applications or fraud platforms for each vertical can be very frustrating for merchants at the end of the day. It can increase the number of overlooked errors or create more human needs than necessary.

Considering all these, applications or brands that can carry out all risk processes on a single platform will be the critical point for fraud prevention strategies in 2023. We can say that e-commerce companies, which have already proven themselves in the sector and break records with their daily transaction numbers, work with brands that are beneficial for the single-screen operation in all their processes in the wallet and shopping sections. I can say that we will see and hear more of such merchants in 2023. While the different kinds of fraud cases will increase, usage of one-screen fraud prevention platforms –risk orchestration platforms– will increase.

What additional friendly fraud challenges will merchants face in a recessionary environment, and what is the best way to mitigate them?

With the pandemic outbreak and the economic recession increasing, we can say that the online shopping process has attracted more attention than ever before. Many people affected by the crisis turned to online shopping by doing price research in the virtual environment instead of going to the physical store.

It would not be a lie if we say that friendly fraud is the most challenging type of fraud to detect among the fraud types. Compared to other fraud types, it can be much more difficult to see more clear evidence and take action. I can say that the most significant help in detecting this is keeping the blacklists in more detail. Because based on our experience and what we have seen, I have observed that a person who makes transactions with the information or cards of a relative, friend or acquaintance will continue to do this periodically by making it a habit.

In the case of opening a new membership with the same information, keeping it on a blacklist so that merchants can follow closely is becoming an essential detail in preventing friendly fraud. In addition to that, merchants also can use one of the kind risk orchestration platforms that observe the whole data in one screen.

How should merchants be preparing for Payment Services Directive 3 (PSD3)?

PSD3 will broaden PSD2's application to payments. This entails more apparent differences between online and offline payments and a deeper comprehension of "sensitive" client data and transactions that are initiated by the business. Multi-factor authentication is one of the more robust authentication methods introduced by PSD2. Modern PSPs' sophisticated AI-powered fraud solutions have made it simpler to monitor real-time transactions and stop fraud. PSD3 will build on this even more by adding more robust security, transparency, and fraud protection measures.

Another issue that PSD3 will address is API standardization for improved, more secure access to financial data by all parties, including retailers and PSPs. All companies that accept digital payments and the banks and PSPs that handle and process these payments must comply with PSD3.

What will be the biggest 2023 eCommerce fraud trend that is currently being overlooked?

Many fraud trends started to advance in 2022 and we expect to increase in 2023. The first of these is the chargeback issue, which is on the agenda for all of us. Chargeback, which has become a serious problem, especially in regions such as the UK, which has proven itself in the field of eCommerce, will continue to be on the agenda in 2023 and will be a nuisance to merchants if the necessary measures are not taken.

To resolve the chargeback, you should get in touch with your customer. It's possible that you can explain the misunderstanding or come to an agreement with the customer. If you come to an agreement, then you should tell the customer to contact their bank and say that they want to drop the chargeback. Merchants also can use industry-proven risk orchestration tools to reduce chargeback rates and prevent this problem.

Another fraud trend that we expect to increase in 2023 will be BNPL. I predict that the BNPL service we are used to seeing in 2022 and the BNPL fraud cases arising from this service will increase considerably in 2023. Currently, many companies provide BNPL services. While the provincial idea of the companies is that we will be able to both make a turnover and distribute credit, there is also a serious increase in fraud.

I can say that two types of fraud have increased with the BNPL service. One of them goes under the name of friendly fraud, and the other is the inability to collect the loan. While KYC assistance measures continue to be taken, we may have to produce more sophisticated solutions with the increase I expect in 2023. As Formica, we see that even the voices of people are imitated by the fraud cases we have experienced. If we use the right risk platform, it is a problem that we can easily avoid in this situation.



Özgür Oktan
CEO & Founder

Özgür Oktan is the CEO and Founder of Formica. He has always been enthusiastic about software, science, and technology since his childhood. So it was his first decision to have his university education in Computer Engineering. After university, he worked as a Software Engineer for about 14 years before he founded Trlogic.

At Trlogic he and his team have developed a Real-Time Risk Orchestration Platform called Formica. He is passionate about Formica and working hard on it since the launching.



Fraud.net



Fraud.net operates a real-time fraud detection and analytics platform, helping enterprises quickly identify transactional anomalies and pinpoint fraud using big data and live-streaming visualizations. The platform allows organizations to monitor their fraud program's performance, identify process improvements, and gain insights into developing fraud trends in minutes instead of months.

Fraud.net

What is the most important thing merchants can do to fight fraud effectively without harming the customer experience?

Merchants ride a fine line between risk and revenue. As a business, the merchant will embrace a degree of risk so as to reduce friction for the consumer and increase revenues. The single most important thing in this equation is to accurately assess the risk of each transaction and approach this balance of risk vs reward from a position of knowledge backed by science.

The production of the intelligence to inform these decisions is multi-layered and backed by syndicated threat intelligence, utilizing custom-supervised AI, all with the single objective of delivering an accurate assessment of risk. Fraud.net delivers the risk assessment in real-time, within milliseconds, keeping the risk to the customer experience as low as possible.

What does an 'omni-touchpoint' fraud prevention strategy look like in 2023?

As the channels for consumers expand, so does the ability of a criminal to abuse the very systems designed to provide the consumer with convenience. Criminals committing fraud are not tied to a particular channel and will learn to adapt their strategies to suit what works for them. In the fight against fraud, ensuring that transactions and actions across the attack surface are connected and modeled enables merchants to defend against cross-channel fraud.

At each touchpoint in the interaction with a consumer -- account creation, login, transaction, account changes -- Fraud.net has the opportunity to assess risk, tying intelligence into each decision, creating feedback loops that ensure the criminals are locked out from the front, back, and side doors. Whilst digital channels offer a rich feed of digital signals, it's important to capture and evaluate actions through operatives and the sequence of interactions to fully protect the business.

What additional friendly fraud challenges will merchants face in a recessionary environment, and what is the best way to mitigate them?

In a recessionary environment, all fraud types tend to increase. That's no secret. In terms of friendly fraud, we will see more 'goods lost in transit', 'wardrobing' (wearing and returning items), increased levels of transaction disputes, and faked returns.

The best operators right now have taken control of their returns processes, plugging this into the fraud platform, but moreover, actually processing returned packages. Too often, spending time on returns processes is seen as a waste of resources. Sadly this in itself is a criminal opportunity. There is very little profit in selling to a person who repeatedly gets refunds for his power tool and returns a bag of carrots!

How should merchants be preparing for Payment Services Directive 3 (PSD3)?

There is an expectation that PSD3 will be formulated over the coming years, particularly as the European Commission issued a Consultation entitled 'Payment services - review of EU rules' in May 2022. To second guess what might happen may be a little premature, as this will move through several stages as changes emerge and are built out during the various stages of consultation. However, the outcome and summary of the responses to the initial consultation are available (<https://ec.europa.eu/info/law/better-regulation/>). SCA is in the spotlight, with a suggestion towards more technological innovation as well as the continued expansion of open banking adoption. Clearly, the focus on fraud reduction will continue, with 17% of the EC's consumer respondents having experienced fraud. Merchants who manage their risk will ultimately be in a better position to face whatever PSD3 brings.

What will be the biggest 2023 eCommerce fraud trend that is currently being overlooked?

Claims fraud. Most merchants are concerned with transaction fraud and return fraud, namely chargebacks, but this fraud type may be overlooked. While a good claims process is necessary and contributes to customer satisfaction and loyalty, some customers take advantage of this process in order to keep merchandise from a retailer for a free or lower cost. They falsely claim an order was lost, stolen, or damaged. In response, retailers will either offer a refund, price adjustment, or even re-ship the good and with a growing share of claims being fraudulent, this has a significant impact on a retailer's bottom line.

Merchants often default to a customer-first policy, shipping a replacement or refunding a purchase without proof, which allows this type of fraud to slip through the cracks. Tracking, examining, and reporting on stolen or damaged items is a cost, but many merchants are proving a strong business case to capture this feedback, deploying fraud prevention technology at the point of return and recording the physical return.

By referencing Fraud.net's database of known bad actors, as well as applying AI tools to track and flag patterns such as frequent claims from a particular customer, merchants can combat claims fraud accurately and efficiently without sacrificing the claims experience for legitimate shoppers.



John Marsden
Sales Director, EMEA

John Marsden currently looks after Fraud.net's business across EMEA, solving the problems of fraud and financial crime for client's businesses. For over 20 years, John has been at the leading edge of e-commerce, helping clients to navigate the risks and customer experience challenges involved in safely transacting with customers in digital channels. From the early days, specializing in Merchant Acquiring, then through Credit Reference Agencies, using data assets and systems to confirm Identity and manage fraud risks, and now with Fraud.net, John continues the career theme of making the world a safer place for our clients to do business, and often making it easy for good customers.

John's expertise stemming from years of experience with Barclaycard, Experian, Equifax, iovation (TransUnion), and now Fraud.net has covered Identity, Fraud Prevention, anti-money laundering, and counter-terrorist financing efforts. In a world where the internet is the playground for nefarious actors to gain finance and facility, John's knowledge and understanding has been crucial to clients' projects and process success.



What is the most important thing merchants can do to fight fraud effectively without harming the customer experience?

A recent [report](#) discovered that consumers would abandon a transaction if they had to wait more than 30 seconds for it to go through. This calls for merchants to leverage technologies like data enrichment and network analysis, powered by Machine Learning to assess customer risk.

Such advanced technologies allow for basic data points such as customer name, email address, payment information, phone number etc to be enriched and used as a means to gain insight on customer level attributes such as location, transaction history across merchant data network, device type and age, card type etc. The detailed customer and transaction level attributes allow merchants to assess risk more accurately, without inducing unwanted friction.

What does an 'omni-touchpoint' fraud prevention strategy look like in 2023?

Omni channel methods such as BOPIS (Buy Online Pickup in Store) are set to reach over \$700 billion in spending over the next five years. As customers are likely to purchase more items when visiting a physical store to pick up their online order, such business models have proved to be lucrative for merchants.

Merchants adopting omnichannel strategies however need to appreciate that additional comfort to customers comes at the cost of a broader attack surface for fraudsters to exploit. The situation is made trickier as verifying users' identity becomes difficult due to the lack of information on physical addresses.

In such a scenario, merchants need to gain a more holistic view of the customer. This can be achieved by blending server side data with that from account and payment fraud systems.

There is a further need for merchants to amend their fraud prevention strategies and adopt solutions which leverage advanced technologies like linking analysis. This lists all transactions engaged in by the customer using the same shipping address, IP or email address. Machine learning assessing over hundreds of data points can further aid in spotting mismatches in device or IP location. This supports merchants in accurately assessing risk while ensuring a seamless customer experience. Additional velocity checks to catch any bot like behavior can further help.

What additional friendly fraud challenges will merchants face in a recessionary environment, and what is the best way to mitigate them?

Recessionary environments pose a tricky challenge, as people have less money to spend but still want to maintain the lifestyle they are accustomed to. Friendly fraud attempts have been seen to increase sharply in past economic downturns, costing merchants close to 2x the transaction amount.

A 21% uptick was further seen in friendly fraud in 2021, when compared to 2020 levels, given COVID-19. Sectors with high Average Order Value (AOV) such as travel and fashion have been worst hit. Fraugster's data further demonstrated a unique trend of uptick in 'angry chargebacks', defined as chargebacks filed by customers where the merchant is unwilling to offer a refund, increasing from a pre-pandemic baseline of 15% to over 50%. Merchants should be prepared for a rise in such evolving patterns of friendly fraud in response to inflationary pressure.

Apart from investing in challenging chargebacks posing a high probability of winning, merchants can be a step ahead by focusing on root causes and taking necessary actions to prevent them. Some best practices include:

- 1. Quick and easy resolution of consumer issues:** this can be achieved by providing clear and direct channels for customers to resolve issues and offering seamless order and shipment tracking services.
- 2. Accurate merchant and billing descriptors:** improving transaction descriptors that cardholders see on their statements and providing smart terms and conditions with respect to returns and refunds, aid in achieving this goal.

How should merchants be preparing for Payment Services Directive 3 (PSD3)?

Although PSD3 will only come into effect in the next three years, recent discussions have focused on areas of Strong Customer Authentication (SCA) and improved open banking standards. The extension of SCA period from 90 to 180 days has been one of the key topics in discussion, expected to positively impact merchants by reducing customer churn. Emerging areas like cryptocurrencies, BNPL or other forms of alternate payment methods must be prepared for increased regulations.

In lieu of additional regulations, merchants must be ready to innovate and shift to advanced fraud prevention solutions that leverage device fingerprinting and behavioral data points to accurately verify customer identity without inducing unwanted friction.

What will be the biggest 2023 eCommerce fraud trend that is currently being overlooked?

It will become increasingly complex to tell apart genuine shoppers from bots and fraudsters, especially as fraudsters are becoming more sophisticated at mimicking the behavior of good users to avoid detection. On the one hand this could increase the percentage of false positives, on the other hand it will test how accurately vendor solutions can distinguish good transactions from bad ones. This would be even more complex, as merchants revamp security systems to counter increasingly sophisticated and automated attack vectors including bot attacks, SQL injections to test stolen credentials and Man in the Middle attacks.

Additionally, an increase in interconnected smart devices and online activity has made customers more vulnerable to fraud. This can be seen in the increasing number of data breaches (up by 68% in 2021), which has subsequently contributed to a surge in synthetic identity fraud, increasing at +109% in 2021, as discussed in our latest Payment Intelligence Report.

Merchants also need to prepare against fraudsters ready to exploit the openness of web3. The rise of web3 and the metaverse would not only trigger increased purchases of high value digital assets like NFTs but also low value, high frequency in game purchases like that of swords, skins, and usernames. These environments can thus be preferred locations for fraudsters testing stolen financial instruments before going on to make higher value purchases. This in turn presents a massive chargeback risk for merchants, and especially gaming companies.



Christian Mangold
CTO

Christian Mangold, the CEO of Fraugster is a seasoned executive who successfully scaled SOFORT before its acquisition by Klarna, where he served as Managing Director for the DACH region. He is a lawyer by education who worked in strategy consultation and corporate finance prior to joining the company. Now he has more than 15 years of experience with executive positions in rapidly growing, private equity backed companies. Christian draws on his strategic consulting capabilities to spearhead fraud prevention for PSPs, Crypto, BNPL, and others. Christian is a keen helmsman and outdoorsman, spending his free time exploring the wilderness of his native Bavaria.



Nethone



Nethone is a machine learning (ML) based fraud prevention SaaS company that allows online merchants and financial institutions to holistically understand their end-users—also referred to as “Know Your Users (KYU)” in industry parlance. With its proprietary online user profiling and ML technologies, Nethone is able to detect and prevent payment fraud, account take-overs with unrivalled effectiveness.

[Nethone.com](https://nethone.com)

What is the most important thing merchants can do to fight fraud effectively without harming the customer experience?

A customer-centric strategy that combines a frictionless checkout process with fraud prevention must rely on Artificial Intelligence. As opposed to traditional methods, AI-based fingerprinting tools automate the decision-making process to the greatest extent possible. With a real-time risk assessment, a merchant can distinguish between fraudsters and legit consumers and, thus, rightly decide who to let through the checkout. And due to its silent background operation, such a tool would go unnoticed by the user, streamlining the entire purchase process.

Striking the right balance between protection and convenience on the consumers' end boils down to three pillars that a successful strategy is built upon: an integrated data approach, which uses customer data from multiple sources to provide a holistic view of each customer; fast customer verification, which reduces the time needed to detect fraudulent behaviour; customer interaction analysis, which enables merchants to identify specific engagement patterns and create profiles of customers based on those interactions.

What does an 'omni-touchpoint' fraud prevention strategy look like in 2023?

To observe and address fraud across multiple touchpoints and channels, ecommerce businesses need multiple layers within their fraud prevention strategy. Essentially, they would need an initial layer of pre-filtering fraudulent transactions with their platform, followed by multiple tools running in the background. This technique can be perceived as an orchestration layer that performs individual fraud assessments on specific use cases. Moreover, automated tools are designed to assess transactions' riskiness and investigate further into consumers' backgrounds to validate their information or to confirm any fraud history attached to them. Ultimately, all these techniques add up to a scalable solution that can support business growth with minimal disruption.

What additional friendly fraud challenges will merchants face in a recessionary environment, and what is the best way to mitigate them?

As modern problems require modern solutions, most likely, fraudsters will explore more creative ways to escape paying for their purchases, which could increase the number of illegitimate chargeback claims. Unlike situations where fraudsters are blocked on their way at the checkout, a chargeback case requires evidence that the transaction actually happened. Ideally, one should determine the true intentions of their user before allowing them to exploit friendly fraud opportunities and let them make the purchase.

When dealing with a legitimate request, however, merchants should be vigilant enough to refund the customer before the latter files a claim. A prompt action resolves the matter and avoids further complications. For all these reasons, it's crucial for merchants to know and understand their users' behavior like the back of their hands to prevent a claim in a timely manner.

In a high-ticket purchase instance, it may be worth running some extra checks to ensure a secure transaction. As a means of providing additional security, behavioral biometrics are just as useful as AI-based automated tools, and these solutions serve as a heavy combo to ecommerce businesses.

How should merchants be preparing for Payment Services Directive 3 (PSD3)?

The new directive will extend some of the provisions of PSD2, so the entire payments industry should, first of all, be all set for the current one before moving forward to other review processes. An upcoming directive such as PSD3 seems like a logical next step once SCA requirements and exemptions are understood and correctly implemented by all parties involved – issuers, PSPs, and merchants.

PSD3 is likely to be influenced by the market as well, with merchants playing an important role, but this requires a thorough understanding of PSD2. Ecommerce players that have a clear perspective on the current flaws and strengths of PSD2 can further develop new ideas on how an upcoming revised direction can be leveraged and personalized according to their needs.

To meet and even go beyond SCA requirements, advanced fraud solutions, supported by machine learning models that incorporate behavioral biometrics and digital fingerprinting, are proven to be the most effective. This approach results in a 360-degree understanding of every user making an online transaction; and by maintaining the highest level of protection, SCA can be reduced by maximizing the use of Transaction Risk Analysis (TRA).

Furthermore, discussions revolve around the EU's Retail Payment Strategy's integration into PSD2 revision. An important aspect of this legislation regards more support for cross-border instant payments through an improved payments infrastructure.

The push for real-time payments is evident, and it's fair to say that adapting to this new environment requires fast reactions when it comes to transactions, protection, and settlements. Merchants should particularly focus on providing a seamless customer payment journey with the highest level of protection. Once again, to meet this scope, employing an automated tool that provides real-time recommendations for every flagged user interaction is key.

What will be the biggest 2023 eCommerce fraud trend that is currently being overlooked?

I don't think there is a particular fraud trend that is being overlooked, but more issues we should continue to keep a sharp look out for, such as account takeover (ATO) that is still prevalent, the sophisticated bad bots, first-party misuse, policy & promo abuse, to name a few.

Some merchants are rather missing out on the right strategy for dealing with fraud because they think it can't happen to them. As well, the dark web is not fully explored to its greatest potential – that is the place where one can anticipate fraud trends and behaviors based on the information that circulates there. So the possibility of becoming vulnerable to fraud by not protecting their business and customers is sometimes overlooked, but the fraud trends are visible to the whole ecommerce industry.



Patrick Drexler
Head of Business Development at Nethone

Experienced sales and partner manager in the payment and financial industry with 10+ years of experience. Prior to joining Nethone, Patrick managed the partnership department at Paysafecard (for Europe and Asia), and later represented the group in Germany. For the last 5 years, Patrick has built up the partnership department at Dalenys/Natixis Payment in France and led the sales activities in the DACH area.

Patrick is building and executing the business development strategy for sales and partnership teams to establish an international footprint for Nethone.



Ravelin



Ravelin provides technology and support to help online businesses prevent evolving fraud threats and accept payments with confidence. Combining machine-learning and graph network visualisation, Ravelin helps businesses draw deeper insights from their customer data to detect fraud, account takeover and promotion abuse and increase payment acceptance.

[Ravelin.com](https://www.ravelin.com)

What is the most important thing merchants can do to fight fraud effectively without harming the customer experience?

For many of the world's largest online merchants, fighting evolving fraud threats is perpetual. It often requires a dynamic and nuanced approach, one that can keep pace with an increasingly sophisticated spectrum of fraudulent behaviour. Bespoke machine learning models can help merchants monitor their customers' behavior to identify potential account takeover attempts at login and checkout helping to secure the entire customer journey. Coupled with link analysis and an expert rules engine, there should be no need for clunky security checks or added friction. Our forward-thinking fraud platform only recommends step-up authentication if it is deemed necessary. We believe that fraud prevention shouldn't get in the way of good customer experience. Our dashboard and investigation tools allow merchants to analyze emerging threats and react accordingly so that you'll always see what's coming next.

What does an 'omni-touchpoint' fraud prevention strategy look like in 2023?

Online merchants should be looking into articulated solutions that combine powerful technologies such as machine learning, graph networks, behavioral analysis with expert rules capabilities. This will provide accurate fraud insights that cover online payment fraud, account security, policy abuse and payment acceptance. A platform that can adapt to evolving fraud challenges and provide clear analysis alongside informed recommendations will help merchants combat the fraud that they have today and whatever might come tomorrow.

What additional friendly fraud challenges will merchants face in a recessionary environment, and what is the best way to mitigate them?

Unfortunately the COVID-19 pandemic has been accompanied by a significant increase in fraud, an increase that shows no sign of slowing. Opportunistic and professional fraudsters alike have profited from the rise in online traffic caused by global lockdowns. The former have been tempted into committing "softer" types of fraud such as exploiting returns or promotions policies to save a few pennies amidst an ever-inflating cost of living.

Meanwhile, professional fraudsters have thrived directly by defrauding merchants using stolen card details and exploiting digital wallet loopholes. They have also capitalized on an increasingly socially-connected population by offering their services directly to consumers – a technique also known as “fraud-as-a-service”. These services can be accessed by anyone who might be scrolling through popular social media platforms such as Telegram, TikTok, Instagram or Whatsapp, with naive opportunists paying a named fee to professional fraudsters to obtain in-demand (and often high-value) goods and services at a fraction of the price.

These new types of fraud are often costly and difficult to contest, rendering them incredibly challenging for online merchants. To respond to this, merchants should seek technologies that can give greater visibility across the entire customer journey. Not only can a nuanced approach like this help stop fraud occurring upfront by analyzing customer behavioral patterns but it can also enable a reduction in volume and associated costs of any chargebacks that occur where the former might not have been possible.

How should merchants be preparing for Payment Services Directive 3 (PSD3)?

Just like its predecessor (PSD2), PSD3 will address Strong Customer Authentication (SCA) and open banking standards, aimed at making transaction experiences smoother and more secure for consumers interacting with both merchants and banks alike. For online businesses that accept electronic payments and for the financial institutions that process them, PSD3 compliance will eventually become mandatory – once ratified in law, an implementation deadline will be announced, a process that has a conservative estimate of approximately five years (if the PSD2 equivalent is anything to go by).

There will be penalties for non-compliance, meaning that merchants should do their utmost to keep well-informed about the impending roll-out. It is also anticipated that the implementation of PSD3 will likely be accompanied by another increase in fraudulent activity as it enlarges the attack surface available to the nefariously-minded. Shared identity information across multiple platforms and institutions will undoubtedly be targeted as a loophole by professional fraudsters yielding the promise of high rewards. So, although PSD3 will improve payment security and efficiency for both consumers and our global economy as a whole, it will not come without its challenges and extended risks.

What will be the biggest 2023 eCommerce fraud trend that is currently being overlooked?

Promotion abuse is a rapidly growing fraud vector, the impact of which is frequently negated by the actions of eager marketing teams looking for impressive new customer metrics. But stripping away the rose-tinted glasses can reveal an ugly truth. Even one’s genuine customers can stray into taking advantage of your promotional discount codes, sign-up and referral bonuses.

Our recent research found that 49% of eCommerce businesses have experienced a rise in promo abuse, and 51% have experienced a rise in refund abuse since mid-2020. It’s easy to see why. During various COVID-induced lockdowns, customers flocked to online merchants in place of physical shops, while merchants scrambled to attract new customers through compelling promotional campaigns.

We regularly see promotion abuse occurring within our customer data – obvious signs include the suspicious creation of multiple accounts, using jiggled credentials to repeatedly access a free trial or giveaway. Multi-accounting can range from something as basic as a customer logging out of one account and signing into another, to professional fraudsters creating fresh IP addresses or synthetic IDs. We've also seen promotion abuse evolve into more organised reselling schemes, where fraudsters take advantage of high-value product promos to amass merchandise to sell on at a higher price. At either end of the spectrum, it's clear that this problem isn't going away anytime soon.



Gerry Carr
Chief Marketing Officer

Gerry Carr is the Chief Marketing Officer of fraud detection company Ravelin. Ravelin's mission is to help businesses grow securely in an online world of increasing risk. Gerry has helped Ravelin since its inception to grow out its impressive client list around the world and build its reputation as a technical innovator in the world of payment and risk. Prior to Ravelin Gerry has led marketing efforts at Brightpearl, Canonical and Sage CRM Solutions.



What is the most important thing merchants can do to fight fraud effectively without harming the customer experience?

Balancing CNP fraud prevention and customer experience has always been a delicate act, but today's inflationary context complicates the equation. As margins tighten, eCommerce fraud continues to rise, hurting merchants' revenue at a time when every dollar counts. The surging trends are on two ends of the fraud spectrum: On one end, there's sophisticated fraud, such as phishing scams, fraud rings, and of course, account takeovers. On the other end, more simplistic MOs like friendly fraud and policy abuse scams have become widespread. Whether professional or opportunistic, both types of fraud are equally difficult to detect by traditional anti-fraud systems.

This state of affairs erodes merchants' confidence levels and negatively impacts risk management. Mastering the aforementioned balancing act when confidence is low is almost impossible. Fraud prevention done defensively becomes rigid, leading to friction, cart abandonment, false declines, and ultimately reduced CLV. And even if this lost potential doesn't show up on the balance sheet, the losses are real: We estimate that 40% to 70% of orders declined at checkout are actually legitimate.

An effective fraud prevention strategy is about more than preventing fraud; it's about the trade-off between approval rate and risk. It starts with looking at metrics comprehensively, beyond the chargeback rate, to determine the cost of letting a bad actor through vs. the cost of losing a good customer. To grow, merchants must reach new segments of customers, increase the LTV of the existing ones, and improve operational efficiency. So, setting the right KPIs and gaining the necessary visibility to accurately assess how a risk platform impacts acquisition, retention, and operations is crucial.

What does an 'omni-touchpoint' fraud prevention strategy look like in 2023?

Delivering a fully integrated customer experience across all channels is complex. The more channels, the more touchpoints, the more data. For retailers, it's both a challenge and an opportunity. They must invest in developing the capabilities to manage this influx of data; but when done successfully, they can leverage it to build the integrated, seamless, personalized purchase journey today's customers expect. In an omnichannel world, AI-powered solutions have become a must; they see the big picture and reveal nonintuitive patterns and subtle trends, even in vast datasets.

In terms of fraud prevention, different channels involve different challenges. Shopping behaviors and fraud MOs can vastly vary according to the shopping journey. A one-fits-all approach to risk is no longer practical. On mobile, for instance, shoppers tend to be more spontaneous, making multiple low-amount purchases that are likely to be flagged by legacy or rule-based systems.

Fraud prevention needs to be tailored per channel. And here too, it all begins with setting the right targets for key fraud performance metrics, this time specific to each channel. Merchants should aim for different metric thresholds for their web, click-and-collect, or in-app order flows.

What additional friendly fraud challenges will merchants face in a recessionary environment, and what is the best way to mitigate them?

Friendly fraud occurs when a cardholder makes a legitimate purchase yet later files a chargeback. Sometimes, the cardholder doesn't recognize the charge, but in some cases, the abuse is intentional. The shopper may experience buyer's remorse and prefers to deal with the bank rather than the merchant to obtain a refund. The phenomenon became rampant during the pandemic, and today, with hiking prices and a substantial loss of purchasing power for consumers, we can expect an increase in buyer's remorse, liar-buyer, and other forms of chargeback fraud.

While typical CNP fraud happens at checkout, friendly fraud occurs post-checkout. So traditional anti-fraud measures intended to catch fraudsters in their tracks can't help in case of chargeback abuse. And the fact that the transaction can be traced to a legitimate cardholder makes the situation even more delicate. The only way to deal with this type of fraud is to dispute each fraudulent chargeback by providing sufficient and compelling evidence to prove that a cardholder authorized the purchase.

When done manually, this process takes considerable time and resources. Some merchants decide that the cons outweigh the pros and prefer to pay out the unjustified charge. Not only do they leave money on the table, but they risk encouraging repeat abusers: Nearly half of abusers file another illegitimate chargeback within 90 days. By automating part or all of the dispute process, merchants can accelerate recouping losses and reallocate resources to revenue-generating tasks.

Additionally, recovering these charges can rebuild their confidence and encourage them to approve more orders upfront.

How should merchants be preparing for Payment Services Directive 3 (PSD3)?

You can only evaluate what's missing from a regulation once it's fully deployed. Since its enforcement, PSD2 has constantly evolved, undergoing revisions and improvements. Payment professionals, along with the EBA representatives, are deeply involved in reshaping how the regulation is applied. And while the market is still busy adapting to the new rules, resolving 3DS-related technical issues, and looking for the best ways to leverage exemptions, the conversation about PSD3 and RTS2 has already started.

We can expect future changes to keep following the same direction: make online payments safe and convenient while incentivizing competition and innovation. Among the points shared by industry representatives are their expectations regarding the treatment of the inherence factors of strong authentication (SCA). For instance, can behavioral biometrics be treated as one of the factors? Or can two factors of the same category be applied?

There's also a possibility for the whole scope of the regulation to be widened. It's becoming increasingly imperative to cater to emerging trends and new payment methods, such as BNPL and cryptocurrencies, as well as protect against new types of fraud. But realistically, it's far too early to have any certainties, as both PSD3 and the revised RTS2 are to be enforced only in 2027, and many negotiations are still ahead.

What will be the biggest 2023 eCommerce fraud trend that is currently being overlooked?

We see policy abuse as a particularly challenging threat to online merchants. It's multiform and cannot always be strictly defined as fraud. Detecting it and mitigating it requires a very different set of capabilities than when managing traditional eCommerce fraud. Since the COVID disruption, an increased number of consumers have developed a habit of 'cutting corners' and engaged in various types of policy abuse. But should they be viewed and treated as fraudsters?

For instance, between serial returners and fraudulent returners, there may be a fine line. It's up to merchants to decide where to draw it, at the risk of alienating loyal customers who merely need to be reminded of terms and conditions. What constitutes abuse? Who's a full-time fraudster and who's just a misguided customer? And what is the optimal response? Once again, merchants are forced to strike a delicate balance to protect their bottom line, customer experience, and CLV.

To effectively prevent policy abuse, merchants need to look at identities instead of monitoring accounts: If they're able to recognize that multiple accounts are all linked to a single customer with a high item-not-received (INR) rate, it's obvious they're dealing with a bad actor. AI-powered solutions analyze interactions throughout the purchase journey, such as account creations, requests for return, or missing package claims. They can cross-check this data to reveal sophisticated abuse patterns, removing the uncertainty for merchants while ensuring a frictionless experience for customers



Valérie Candau
Senior Content Strategist

As a Senior Content Strategist at Riskified, Valérie Candau addresses key challenges relating to eCommerce, online fraud, and payments. A subject matter expert specializing in the fraud prevention niche, Valérie closely follows the disruption brought about by emerging consumer behaviors, new technologies, and regulatory changes shaking the eCommerce ecosystem.

SEON



At SEON, we strive to help online businesses reduce the costs, time, and challenges faced due to fraud. With a real-time, flexible API, we collect relevant risk-related data points. Once connected, we provide an overall risk score that leverages data enrichment and machine learning to help make the right decision.

Seon.io

What is the most important thing merchants can do to fight fraud effectively without harming the customer experience?

Friction is a buzzword that many in our industry like to throw around. And for good reason. The way each company approaches friction is often what differentiates it from the competition. For us at SEON, it is all about customizability and dynamic friction.

Too much friction harms the customer experience. But too little friction makes you an easy target for fraudsters. Plus, friction is increasing due to mandatory regulations such as PSD2, so merchants ought to be proactive in countering these pressures.

SEON analyzes the customer's setup, IP address, email address, etc., and enriches this data using hundreds of data points, without interrupting the customer's journey. This way, we can access whether they are high, low or medium risk before we ask them for any verification at all – and ask them for the type of verification that suits how risky they are.

At the same time, this means we do not need to reject slightly suspicious customers outright. A common pain point with legacy anti-fraud software is that it tends to be too strict, which means more false positives. With our solution, merchants can implement dynamic friction – which means that for those uncertain cases, who are not obviously good customers but we aren't certain they are fraudsters, we can always ask them for additional verification or authorization.

So, to answer your question, the most important thing a merchant can do is to set up dynamic, adaptable and customizable systems that apply the level of friction that is suitable for the specific customer and transaction. This way, you can reward good customers with frictionless shopping and reduce false positives, without compromising security.

What does an 'omni-touchpoint' fraud prevention strategy look like in 2023?

True real-time fraud prevention allows us to monitor customers and their actions every step of the way. The idea is to continue to analyze their behavior and setups without interrupting them, with each action and data point adding to or subtracting from their fraud score.

Data enrichment is key to us. SEON enriches readily available primary data such as an email address or IP address using 50+ OSINT sources, including social media and online platforms. This provides more accuracy and confidence. We call this someone's digital footprint.

Every fraudster out there will use OPSEC tools to spoof their systems and hide their location. But they will not create a detailed digital footprint for every one of their synthetic personas, because this is very difficult to scale – and brings little return on their time investment. So digital footprint analysis is very reliable and difficult to falsify.

SEON's modules will study this digital footprint as the customer signs up, browses the website, attempts a payment, etc., informing us when an action is suspicious or risky, and exactly why that may be. This will be combined with fraud prevention staples like device fingerprinting, velocity checks, etc. From there, our end-to-end platform allows for automation, manual reviews, etc. Everything is granular, customizable and explainable.

If we're talking about multichannel and omnichannel shopping models, fraud software that updates in real time and is based on real-time data will allow all staff to be fully up to speed with the status of each order, and how much risk it poses, in order to catch and stop fraud.

What additional friendly fraud challenges will merchants face in a recessionary environment, and what is the best way to mitigate them?

A recession does not necessarily bring different challenges but certain data shows that it intensifies the scale and frequency of attacks. We recently published on our website [a report on the link between recession and fraud](#). We studied existing metrics and concluded that there seems to be higher risk of online crime at times of economic downturn, though we would like to see even more in-depth research into this question.

Some of the fraud trends we've seen in recent years indicate that individuals who would like to commit fraud are finding it easier than ever to begin. There are online tutorials, accessible tools and leaked credentials even in the clearnet and we are also seeing a rise in Fraud-as-a-Service offerings, which is alarming.

How should merchants be preparing for Payment Services Directive 3 (PSD3)?

At the moment, not much is known about the decisions that will drive PSD3, but we can look at the past to make some informed guesses.

We might possibly see another payments liability shift from banks to merchants or vice versa.

But we can safely presume is that the European Commission will attempt with the new Directive to boost online CNP payments and make them safer – as well as expand and simplify on open banking standards, which have generally been a success.

The PSD3 will be a response to the quickly shifting payments landscape online, so I am personally expecting to see new guidance related to BNPLs, crypto and neobanks as well.

What will be the biggest 2023 eCommerce fraud trend that is currently being overlooked?

Fraudsters' attacks on MFA and OTPs have been intensifying while merchants and customers are demonstrating a false sense of complacency. It seems that not everyone is aware that these too can be breached, so it is up to our community to raise awareness.

We're seeing more phishing for MFA/2FA and real-time scraping of the target to grab one-time passwords. With many contemporary stores, browsers, etc. saving customers' cards for easier purchases, the stakes are higher than ever.

Primarily, fraudsters are attacking people without MFA and, importantly, those whose cards do not have 3-D Secure 2.0 enabled. Although SCA is almost everywhere throughout Europe and much of North America, there are discrepancies when we look worldwide. Countries such as India and Brazil have mandates for 3DS and yet others don't, with about 71% adoption in nations like the USA and Germany.

Fraudsters are targeting those payment gateways that have decided not to turn SCA on because they have chosen low friction over security. However, because more and more gateways support this out of the box, those who don't are even more at risk.

A merchant would do well to consider exactly where the liability lies when they use SCA vs when they don't. Though it seems to add friction, 3DS can make all the difference between who has to suffer the consequences of carding, fraudulent payments, chargebacks etc.



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.



Sift



Sift is the leader in Digital Trust & Safety, empowering companies of all sizes to unlock revenue without risk. Sift prevents fraud with industry-leading technology and expertise, an unrivaled global data network, and a commitment to building long-term partnerships with our customers. Twitter, DoorDash, and Twilio rely on Sift to stay competitive and secure.

[Sift.com](https://www.sift.com)

What is the most important thing merchants can do to fight fraud effectively without harming the customer experience?

Dynamic friction, or adapting the customer experience based on riskiness, will help stifle bad actors without treating customers like criminals. After all, safety is a hallmark of an optimal customer experience but friction should only be applied when and where appropriate. With a well-defined strategy that includes robust fraud tooling, businesses no longer have to choose between increasing revenue and decreasing threats.

Too little friction will give fraudsters a better opportunity to do harm, while too much will result in user churn. The ability to walk this fine line is based on having a fraud solution that is capable of accurately differentiating between fraudulent and legitimate events. This is best accomplished by leveraging real time learning from all the data inputs that you can connect to your fraud prevention platform.

Merchants should adopt a digital trust and safety strategy to prevent fraud while maintaining the best possible experience. This approach bakes risk detection into the decision-making process while also striving for growth and positive customer experiences. Each organization must define that balance within the context of their business and customer needs.

What does an ‘omni-touchpoint’ fraud prevention strategy look like in 2023?

It’s important to remember that attackers rarely stick to a single platform. An omni-touchpoint fraud prevention strategy considers each part of the user journey and has fraud considerations based on whatever channel an account or order originates from. This means that the same fraud logic — the rules and signals used to measure attacks — should not be applied universally to all touchpoints.

To better understand the many ways fraudsters target businesses, merchants can take advantage of machine-learning based fraud solutions which gain insights from thousands of signals. With this real-time fraud signal analysis, fraud teams can better identify attack types and mitigate them as they happen, greatly reducing potential harm before a fraud event can even occur.

How will fraudsters exploit return policies, and what will effective detection and prevention strategies look like?

Fraudsters have the time and motivation to identify vulnerabilities in merchants' return processes, and will continue to collaborate on forums like Telegram to reverse engineer, exploit and monetize refund policies.

Typically smaller, independent merchants don't have a dedicated fraud team in place, so the key is to begin planning as soon as possible. This starts with evolving beyond legacy approaches and adopting a Digital Trust & Safety strategy – one that dynamically addresses fraud while creating a more seamless experience for legitimate customers.

Effective detection and deterrence comes down to having clear return policies on the front end and machine learning on the backend to identify the clusters of bad actors that are causing the most coordinated harm. As merchants who expanded into ecommerce during the pandemic return to their brick-and-mortar operations in some capacity, they need to ensure that their online and offline systems are synced. Otherwise, they will be defrauded via items bought online and returned in store.

Traditional manual review processes and systems, such as caps on order volumes and values, aren't equipped to detect fraud during high-traffic periods. Instead, they're stopping legitimate transactions completely or creating friction within the customer journey. By implementing technologies like machine learning, retailers can better defend against fraud this holiday season at scale. Ingesting thousands of different signals beyond purchase data, machine learning systems can quickly adapt to detect suspicious

What additional friendly fraud challenges will merchants face in a recessionary environment, and what is the best way to mitigate them?

During 2021, even before the current economic challenges, Sift research found that nearly 20% of consumers who filed a chargeback admitted to "friendly fraud." During more volatile economic times, we expect this behavior to increase. With rising inflation and reduced purchasing power, people will be more likely to dispute legitimate transactions in order to receive goods and services for free, while merchants will be more heavily impacted due to the unsteady economy.

Merchants can best mitigate friendly fraud by completing linkage analyses to better identify and block repeat offenders from attempting to do this again in the future. A thorough linkage analysis helps capture all shared attributes between customer interactions – accounts, orders, logins, and more – for fraud assessment, so businesses can better understand fraud vectors and address them accordingly.

Additionally, merchants should prepare for next April's changes to Visa's dispute program, which aims to allow merchants to provide additional data or evidence to show that disputed charges are invalid. This change will ultimately improve protection for small businesses and merchants dealing with unnecessary losses — not just from fraud, but the related costs of labor, shipping, and increasing chargeback fees.

How should merchants be preparing for Payment Services Directive 3 (PSD3)?

The best way for merchants to prepare is to keep up with European Banking Authority developments and opinions on the matter.

Since the directive hasn't been formalized, merchants should ensure they have a pulse on the direction the industry is headed. It's important for merchants to speak directly with their payment service provider(s) on how they are preparing for PSD3 and what they are doing to support businesses.

PSD2 and PSD3 are steps toward more secure online payments, but still not fool-proof solutions against fraud on their own. Companies must continue to apply the rules dynamically to avoid too much user friction, and have a concrete understanding of what role they should and should not play in their digital trust and safety strategy.

What will be the biggest 2023 eCommerce fraud trend that is currently being overlooked?

We believe there will be a significant rise in mobile fraud due to the transition from card-present to card-not-present payments. For example, paying for a dinner check on your smartphone will become the norm as opposed to handing payment to the server.

While in-person e-commerce sounds like an oxymoron, this payment model will drive more self service across all business types to enhance the customer experience. As popularity rises, so will opportunities for fraud. Merchants will have to fortify websites and apps with even more fraud protection to defend against these attacks.



Jeff Sakasegawa
Trust & Safety Architect

Jeff Sakasegawa is a Trust & Safety Architect at Sift who helps customers implement strategies that cross-functionally align risk and revenue programs and ensures online experiences are safe from all vectors of abuse. His experience is in the online payments space, and he's led various risk management and compliance teams at Google, Facebook, and Square.

Jeff is sought-after industry thought leader and active public speaker. His main topic areas of interest are focused on how brands can turn the tide on fraud by navigating the intersection of fraud and user experience. As a recognized fraud expert, Jeff has spoken about trending fraud topics at the Merchant Risk Council conference in Las Vegas and Europe as well as other industry shows including Marketplace Risk Management Conference, Merchant Advisory Group, Phocuswright, CNP Expo, PaymentsEd Forum, Payments Summit, SUBCOM and NYPAY.

Signifyd



Signifyd empowers fearless commerce by providing an end-to-end commerce protection platform that protects merchants from fraud, consumer abuse and revenue loss caused by friction in the buying experience.

What is the most important thing merchants can do to fight fraud effectively without harming the customer experience?

The key to modern fraud management comes down to a change in mindset. As ecommerce has become a demonstrably larger share of retail sales, modern risk intelligence teams need to switch from a defensive outlook to the idea of being teams that optimize revenue.

The math is clear. Online retailers turn away about one in seven customers for fear of fraud, according to 451 Research. We know from industry averages that the proportion of fraudulent orders is generally fewer than one in 100.

The most successful fraud and risk operations focus on capturing those good orders that are being declined. And more importantly, those good customers who are being turned away and potentially lost for good.

How do they do it? By working to understand the identity and intent behind each order. By knowing whether a customer is one who has bought from them before or by being able to use transaction and behavioral intelligence to spot the signs of a bad actor, merchants can capture sales that would otherwise be lost while still protecting the business from fraudsters.

Risk teams need to think creatively. For instance, follow up on declined orders. While declined customers often silently turn to other merchants for their purchases, if you can engage with them, you can begin to understand who is being wrongly declined and why. Talk to your customer support teams to get a read on complaints resulting from declines.

Look to build a larger network of transaction data — perhaps by working with a consortium of non-competitive retailers who can look for patterns beyond your own transaction data. Create a feedback loop by occasionally shipping an order that presents some red flags, but is not obvious fraud. Chart the results and add that to your knowledge base to help with future, similar orders.

And consider outside help. There are a number of machine learning solutions that automate the process and rely on the sorts of large networks that provide the intelligence needed to sort legitimate from fraudulent orders.

What does an ‘omni-touchpoint’ fraud prevention strategy look like in 2023?

The COVID-19 lockdowns accelerated retail’s omnichannel transformation. Buy online, pick up in-store (BOPIS) and curbside pickup exploded in popularity. The convenient fulfillment channels remain a must-have in the post-COVID world given their popularity with consumers.

In a recent Signifyd poll, 50% of respondents said they would do more of their shopping online post-COVID. Moreover, 43% said they were more likely to pick up those orders in a store and 31% said they were now more likely to use curbside pickup.

Shoppers are putting their money where their mouths are. Curbside and in-store pickup sales on Signifyd’s Commerce Network were up 176% in 2022. Retailers have responded. At the start of the pandemic, 6.6% of the Top 1,000 retailers offered curbside pickup, according to Digital Commerce 360. By early 2021, that number was at 51%.



All that means that retailers need to be agile in reviewing orders for fraud. In-store and at-the-curb orders need to be ready to be handed to a customer in an hour or two or the options lose much of their appeal. Risk teams need to make decisions based on fewer signals than standard orders because BOPIS and curbside orders arrive with no delivery address.

Retailers in the post-COVID era need to consider the cost-benefit of hiring additional team members to handle in-store and at-curb pickup. Training existing teams to reliably verify identities is one way to limit loss. Additionally, machine learning solutions can greatly reduce the time and personnel needed to keep BOPIS and curbside orders moving.

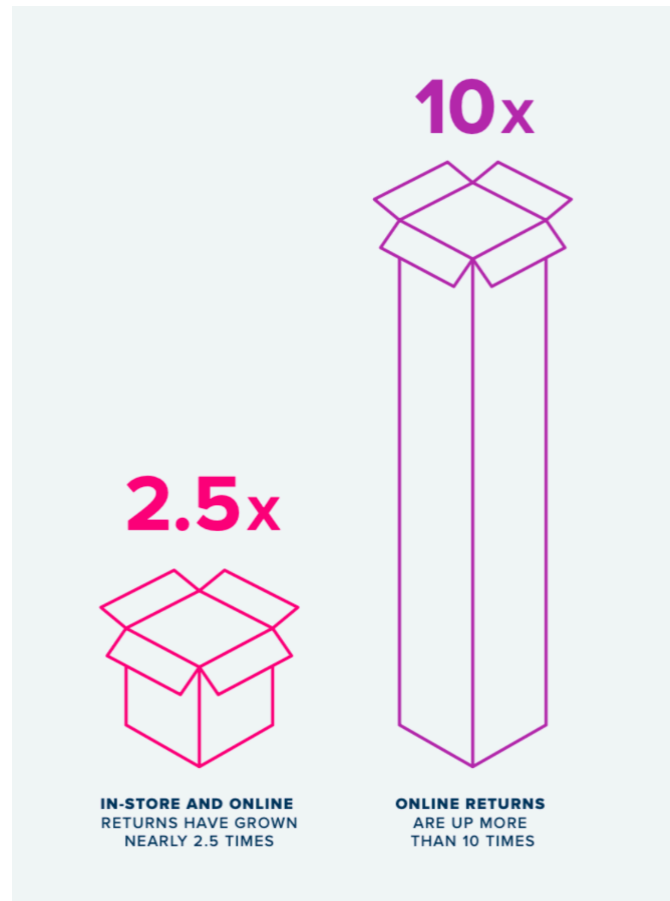
What additional friendly fraud challenges will merchants face in a recessionary environment, and what is the best way to mitigate them?

Signifyd is seeing an uptick in friendly fraud and return abuse coinciding with high inflation and increasing pressure on household budgets. And consumers have been remarkably frank about their willingness to be dishonest in order to get a refund while keeping a product that they ordered.

In Signifyd’s recent consumer survey, 25% of respondents said they had requested a refund with the intent of keeping a product that arrived in satisfactory condition and having the retailer refund the purchase price. Drilling down a bit, 22% admitted falsely claiming that a product they received was unsatisfactory or damaged. 21% admitted to falsely claiming that a product that did arrive never arrived.



Meanwhile, the National Retail Federation found that online returns reached \$218 billion in 2021. More than \$23 billion were fraudulent, according to the NRF. Return scam artists are diabolically creative, returning to be scanned for an instant refund everything from empty boxes to boxes filled with candy, rocks, broken electronics and even a potato to approximate the weight of their original purposes.



The rise in friendly fraud and return abuse are likely being encouraged by both hard economic times and professional fraudsters' move to attack the entire buying journey — from account creation to returns. As merchants and technology get better at disrupting fraud at checkout, professional rings are exploiting new targets. In response, merchants should harden their targets up and down the buying process.

How should merchants be preparing for Payment Services Directive 3 (PSD3)?

The best preparation for the early efforts to iterate on PSD2 is to learn the lessons from the PSD2 process. The path from ideation to implementation was long and fluid. While ideas are being floated to improve open banking and modify Strong Customer Authentication (SCA) the coming changes are far from set in stone and likely years away. But this is no time to be complacent

Retailers doing business in affected regions should consider forming a team to monitor discussions and find ways to add their input and make their positions known. It would be particularly helpful to join with other merchants to present a united front, whether that is through existing industry organizations or by forming an alliance specifically for monitoring and influencing PSD3.

The series of delays implementing PSD2 and the experience of stumbling out of the gate that plagued some merchants can be avoided this time around by early and consistent vigilance.

What will be the biggest 2023 eCommerce fraud trend that is currently being overlooked?

Increasingly, merchants are reporting an emerging trend that has the potential to mold the next generation of account takeover fraud. “One-time passcode defeated account takeovers” have been growing in number over the past 12 to 18 months. In 2022 it moved well past the cottage industry stage and we look for it to be industrialized by 2023.

For some time merchants have deployed countermeasures to foil credential-stuffing attacks that are at the heart of account takeover. The key barrier historically has been to trigger a second authentication factor in some or all login attempts. In many cases the second authentication is achieved through SMS — the consumer is sent a one-time passcode, or OTP, that the consumer uses to complete their login.

The system, familiar to most consumers, has served merchants well. But fraud rings have adjusted. Just as fraud protection has steadily evolved and improved through innovative technology, professional fraudsters are turning to inventive solutions.

While professional fraudsters turned to bots some time ago to scale up their ability to launch credential stuffing and other attacks, the latest iteration of automated attacks includes a social engineering element.

These relatively recent attacks consist of automated credential stuffing paired with an automated trigger that contacts the legitimate account holder and persuades them to provide the one-time passcode sent in response to the fraudster’s login attempt. That practice has given rise to what we call OTP-interception-as-a-service bots.

When implemented correctly, these attacks can have success and lead to extremely high fraud impact. They also undermine all the security built around these anti-credential stuffing measures.



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.

Vesta



Vesta is the only instant, end-to-end transaction guarantee platform for online purchases, delivering unparalleled approval rates, a better customer experience, and eliminating fraud for leading brands in telco, e-commerce, travel, and financial services. Using machine learning backed by 25 years of transactional data history, Vesta increases approvals of legitimate sales for its customers, while eliminating chargebacks and other forms of digital fraud, driving the true cost of fraud to zero and transferring 100% of the liability for fraud, including chargeback processing, so customers can focus on increasing sales. The company is headquartered in Portland, OR, with offices in Atlanta, Miami, Ireland, Mexico, and Singapore.

Vesta.io

What is the most important thing merchants can do to fight fraud effectively without harming the customer experience?

The best way to fight fraud without harming the customer experience is to proactively engage a capable fraud detection system that uses auto-decisioning to differentiate between a malicious fraudster and a legitimate customer. In fact, the right solution can actually enhance the buying journey for legitimate customers. OFDs (Online Fraud Detection systems) that use advanced machine-learning modeling techniques combined with customer behavioral data are very efficient at making automatic decisions in milliseconds, without adding friction or inconveniencing customers with extra steps.

What does an ‘omni-touchpoint’ fraud prevention strategy look like in 2023?

As an industry, we’ve been incorporating more segments of the customer journey into the overall view of fraud prevention, and there are a few solutions out there that will look at account access events, purchase events, return events and promotional events. There are still additional single-point solutions, such as validating identity at account opening, that should be added to get the most thorough coverage across the customer journey. Merchants should look for ways to orchestrate these solutions together, or for vendors who offer the solutions in an orchestrated way, to effectively understand and deter fraud from the various vectors across every entry point.

What additional friendly fraud challenges will merchants face in a recessionary environment, and what is the best way to mitigate them?

Times of financial uncertainty typically see an increase in all types of fraud. For friendly fraud, merchants can expect to face a potential rise in “Item Not Received” disputes, as well as more traditional first-party fraud cases such as claiming that they didn’t make the purchase when perhaps they forgot they did or weren’t aware that a family member or authorized user made the purchase. This type of fraud is very hard to predict, and the best management strategy is currently to leverage chargeback alerts/deflection products to minimize these types of chargebacks. Additionally, offering Buy Now Pay Later payment options can tempt individuals to spend outside of their limits, creating more opportunity for return fraud.

How should merchants be preparing for Payment Services Directive 3 (PSD3)?

It is likely a bit too early to begin true preparations, however there are a few things that can be done to help ensure you're ready when the new framework is released.

- 1. Evaluate the payment types you allow for purchases.** One of the specific topics being considered is additional regulations for nearly unregulated payment types like BNPL and crypto. Inventorying those additional types you allow, as well as understanding how much of your revenue they make up in a given month, will prepare to understand the potential impacts of new rules for these.
- 2. Conduct a 3DS exemption review.** If you're currently operating under PSD2 and leveraging 3DS for your transactions, understanding how much of your order traffic is eligible for exemptions will help you understand the impact of any changes to the exemption process, limits and other changes that might impact your payment flow.
- 3. Look for Strong Customer Authentication (SCA) products other than 3DS.** As PSD3 is considered, other or newer SCA methods may be introduced. Understanding the vendor landscape for authentication techniques such as location-based authentication or biometric authentication could put you ahead of the pack in implementing these.

What will be the biggest 2023 eCommerce fraud trend that is currently being overlooked?

Unfortunately, there are several types of fraud that seem to be on the rise and should not be overlooked. First, fraud from social engineering is a growing concern, especially during an economic downturn. Financial uncertainty breeds increased susceptibility to email, text and telephone phishing attacks.

Secondly, machine learning-enhanced attacks are also a growing threat. This is the idea that the bad guys are using the same advanced technology and tools to perform fraud that we are using to prevent it. They are using ML to create and enhance synthetic IDs, which optimizes attacks on merchants. ML by the bad guys can also be used to anticipate and counter fraud detection and prevention measures.

Lastly, ecommerce merchants need to beware of growing fraud through alternative payment methods, such as BNPL. These new payment types are popular and convenient for the shopper, but don't have a standardized dispute process or solid policies for chargebacks, and companies are losing big money.



John Venglass
VP Product

John Venglass leads the product team to drive new features, products, and innovations that our customers can use to eliminate fraud and grow their bottom line. John came up in the core banking sector, delivering products that manage collections, recovery, service, and lending for a major bank. For the past 8 years he has turned his focus to understanding CNP transaction and account-level fraud to deliver advanced solutions for businesses transacting online.

***“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