Is your fraud prevention approach ready for 2024?

RETAIL DIVE

Custom content for Mastercard by studioID

Gone are the days of the solo basement fraudster, manually inputting multiple passwords to hack into accounts. Today, fraud is an industry unto itself and the cost to merchants is astronomical. In fact, Mastercard predicted global losses reaching **$48 billion** in 2023.[2] Further, Juniper Research estimates the cumulative losses to merchants due to online fraud could exceed **$343 billion** come 2027.[2]

Not only is fraud growing, but it—and fraudsters—are now significantly more sophisticated and insidious. **Fraudsters are getting more creative, finding new ways to commit undetectable or hard-to-detect fraud.** These evolving fraud threats—such as advances in technology, AI, synthetic identity theft and the escalating threat of promotional abuse—create new challenges for e-commerce businesses that have severe repercussions.

+$343B

By 2027, the cumulative losses to merchants due to online fraud could exceed $343 billion.[2]

Noelle Seawright, Director of Global Data Strategy, Mastercard Identity, believes that merchants don't always see the big picture. For example, while a merchant may dismiss a chargeback loss of $50 as a write-off, the costs add up quickly.

> "That $50 is being funneled into crimes and emboldening fraudsters to proliferate across platforms."

NOELLE SEAWRIGHT,
DIRECTOR OF GLOBAL DATA STRATEGY, MASTERCARD IDENTITY

If merchants don't take definitive actions to prevent fraud, bad actors will continue to strike — from account opening and post-transaction.

To best protect themselves and their customers, merchants need to be aware of the latest trends and adopt a holistic approach to fraud detection in 2024.

Emerging fraud types to know

While merchants are familiar with many fraudulent activities, they need to be aware of several types of escalating fraud threats for 2024, explains Michael Habermann, Director of Fraud Services, Radial.

Escalating fraud threats for 2024:

- Reshipping fraud
- Card testing
- Address manipulation
- Promo abuse
- AI-generated fraud
- Alternative pay methods

Reshipping fraud

While this type of fraud isn't entirely new, it is rising. **In 2023, 20% of merchants globally were impacted by reshipping frauds, which is an increase of 5% from 2022.**[3] Reshipping fraud can occur when fraudsters use stolen credit card information to buy goods and send them to a reshipper (who is often an unwitting part of a work-from-home scam) to send to another location.

Reshipping fraud also occurs when fraudsters, or even legitimate resellers, buy from the merchant but break the merchant's policy regarding the maximum quantity of purchases allowed or ship to countries the merchant doesn't allow.

The latest nuance in reshipping deception occurs when a seemingly legitimate reshipper issues fraudulent chargebacks, which almost always goes through, costing the company. As Seawright explains, "Now the company has lost the product, has to pay the chargeback, and the policy has been broken." She adds that the spike in chargebacks indicates a coordinated activity within the fraud community—an effort likely to grow.

Card testing

This type of fraud ranked the third most prevalent type of fraud merchants experienced in 2023 (behind phishing/farming/whaling and first-party misuse).[4] Even though this type of fraud affects **33%** of merchants globally, many don't always recognize it as a problem because the initial tested amount is so low.[5] However, fraudsters can test to see if a stolen credit card is open and valid. Once fraudsters confirm the card is valid, they may not use it for years, but when they do, it is more difficult to detect that fraud due to the passage of time.

Additionally, with bot technology, fraudsters can test multiple cards at once. When they find a successful combination, bots can make thousands of purchases before the merchant, bank or consumer becomes aware of the problem. According to the 2023 Imperva Bad Bot Report, **22.7% of all internet traffic on e-commerce and retail websites in the prior year was attributable to bad bots.**[6]

Address manipulation

This growing fraud occurs when a fraudster uses a different address to circumvent policy rules about limited purchases for promotional items. For example, a person wants to get multiple HelloFresh boxes offered to new customers, so they create email addresses to look new. A fraudster may also use a fake address to receive goods or services without being detected by the company's automated fraud rules or able to be traced back to the purchase. Whether the fraud is implemented by professional bad actors or customers, the result impacts the merchant's bottom line.

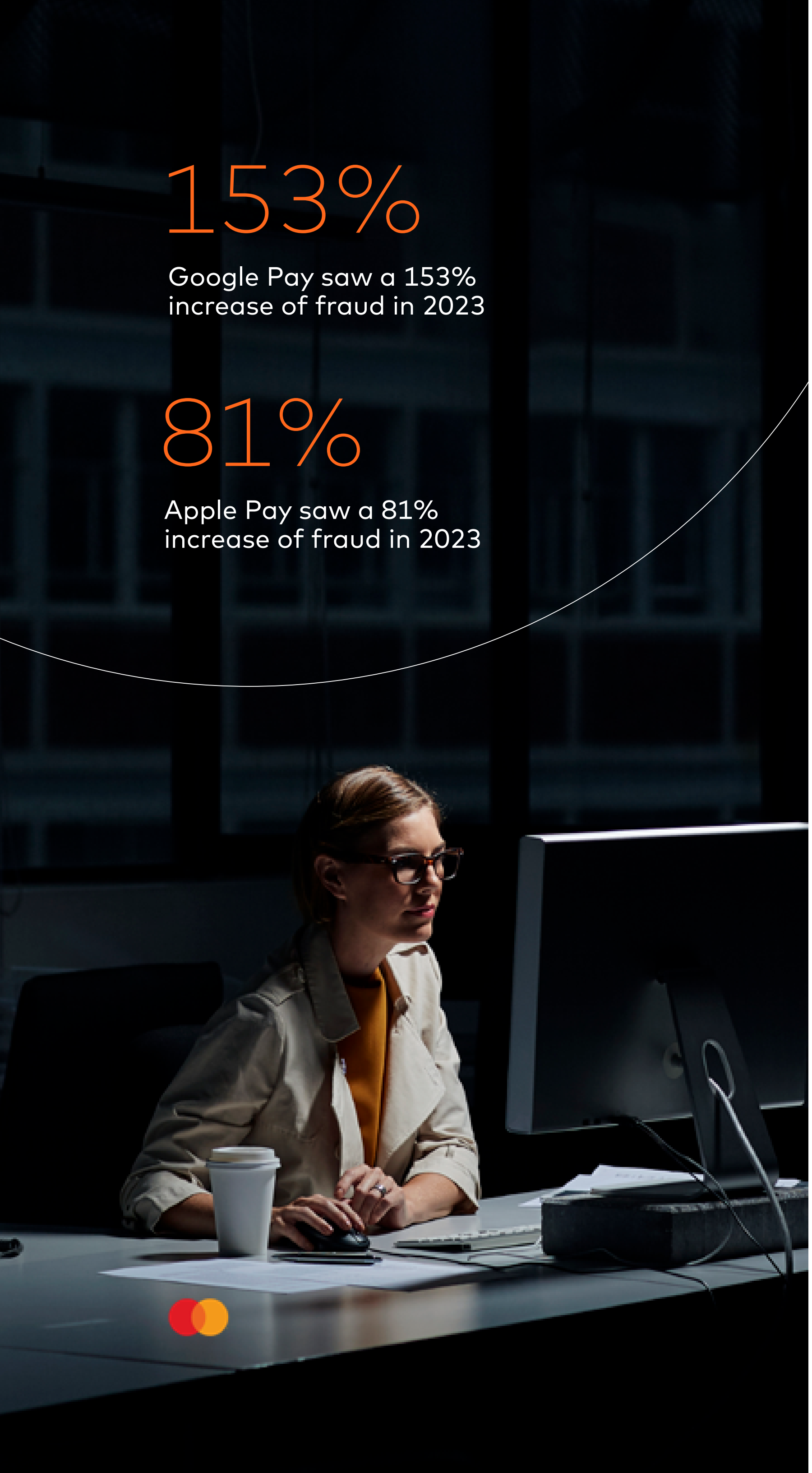
Promo abuse

While address manipulation can be used to carry out promo abuse, fraudsters use other methods to abuse merchants' promotional or loyalty offers outside of their intended use. In fact, **52% of merchants globally reported experiencing an increase in promo abuse in 2022.**[7] Some ways include sharing codes on social media, stacking codes, reselling or trading codes, or using automated tools to create duplicate codes.[8]

AI generated fraud

While AI contributes to aspects of fraud mentioned above, generative AI can do even more damage. **Deepfakes, for example, increased tenfold from 2022 to 2023.**[9] With AI, fraudsters can create fake information that fools both customers and merchants. Fraudsters create customer identities and use stolen credit card information to purchase goods. More scarily still, bad actors can engineer text engineer text and voice messages to mimic the merchant to gain access to a customer's information. They also use AI for refund fraud, by fabricating photos of damaged goods to get a refund.[10]

10x increase in deepfakes from 2022 to 2023[9]



153%

Google Pay saw a 153% increase of fraud in 2023

81%

Apple Pay saw a 81% increase of fraud in 2023

Alternative pay methods

Even actions that aren't intended as fraud can be a financial burden for merchants. As Habermann explains, "Alternative payment methods, such as Apple Pay, Google Pay, Cash App and Shop Pay, bring new levels of risk." This is because merchants now must validate customer information from more sites. Therefore, fraud solutions developed for account takeovers, for example, might not adequately protect against fraud attempts on digital payment platforms. Digital wallets experienced the greatest growth in fraud in 2023, with **Google Pay seeing an increase of 153% and Apple Pay seeing an increase of 81%.**[11]

Each of these fraud types damages the merchant on multiple fronts. Merchants incur the quantifiable financial loss of merchandise and the cost of chargebacks. That financial loss also includes the higher fees a merchant may have to pay if they have too many chargebacks or if the payment processor closes the merchant's account. These frauds can drain customer service resources and cause reputational damage to the brand as well as loss of customer trust and loyalty, impacting sales.

As more threats emerge, merchants must do something different to combat fraud. Habermann and Seawright agree that merchants must reconsider their approaches to automation and leverage technology partners to embrace a holistic fraud prevention strategy.

Why traditional fraud prevention methods can't keep up with new threats

With the escalation in the scope and sophistication of fraud, old ways of addressing it won't work, says Habermann.

One reason is the sheer volume of the crime. "In the past, merchants needed high staffing levels to handle the high review rates. But as e-commerce grows, that's not sustainable," he explains.

Another reason is that organizations' typical siloed approach limits their overall perspective of fraud. For example, when departments, such as payments and fraud, monitor their data independently, neither department sees the big picture of when and how fraud occurs. This limited view makes it more difficult to identify vulnerabilities and anticipate threats.

Merchants can now use more sophisticated technology to address fraud, which provides faster and more accurate information than older solutions. For example, in the past, fraud departments used Google searches to confirm identity. Now, merchants can use data to train machine learning software to recognize high-risk transactions, saving time and creating a better, more convenient experience.

As Habermann explains, “Merchants must deliver more. The focus is more than on the point of transaction. Now, the customer journey needs to focus on loyalty and trust. They still demand speed and convenience but also want to purchase safely.”

Seawright agrees that merchants must find a way to balance fraud prevention with customer experience. “I don't know if anyone has figured (it) out yet, but it's critical.” Indeed, it's no easy task; understanding and measuring false positives, determining risk tolerance, and changing behaviors to be less predictable for fraudsters who are increasingly sophisticated with tools like AI– all while minimizing friction for good customers.

Countering today's fraud trends with a holistic fraud prevention strategy

Addressing evolving fraud threats requires a holistic fraud prevention strategy, one that is a multi-layered, integrated approach that fights fraud from end to end.

A holistic approach implements risk assessments throughout every stage of the customer journey, from the time they open the account through the transaction. But when implementing this strategy, it is essential to balance fraud prevention with offering a low-friction customer experience.

As Seawright emphasizes, "This is about getting everybody involved and ensuring everyone understands their role in the process. Your digital fraud prevention will be the connective tissue between all of these areas."

Three components of a holistic fraud prevention strategy

A successful, holistic fraud prevention strategy involves three primary aspects: data quality, identity verification and fraud prevention teams.

Let's explore each of these:

- Data quality
- Identity verification
- Fraud prevention teams

Data quality

"You need to have the right data and the right amount of data."

NOELLE SEAWRIGHT,
DIRECTOR OF GLOBAL DATA STRATEGY, MASTERCARD IDENTITY

A fraud prevention solution should always be able to gather the information needed to make speedy and accurate fraud decisions.

As Seawright explains, "Even when when customer data changes, a robust fraud prevention solution recognizes when an email address was used previously and that it's attached to a phone number, that it's not a prepaid or burner phone, and that it's in the same area code as the shipping address."

Tagging or labeling data helps maintain data quality. For example, if you cancel an order because the payment or authorization was declined, tag that reason. Then, build those details into future fraud prevention models to establish and identify patterns.

Identity verification

Businesses must sort through mountains of data to provide accurate information that informs good decisions. This task can feel overwhelming. One suggestion is for merchants to assign different risk tiers to customers, adding more friction as the risk increases or when the risk level is unknown.

In Habermann's case, his company recognizes good customers 70% of the time, so there's no need to hold their transaction. "Unfortunately, 30% of the time, we don't recognize the customer and that's when we call Mastercard Identity to provide identity data and insights for a manual review," he explains. Habermann emphasizes that looking at just one set of data is not the best approach. This is because customer records can change so frequently. **"This is why we turn to Mastercard Identity - they have got the most updated information to put in the decision models."**

Fraud prevention teams

Fraud prevention is a team sport — everyone needs to pitch in, involving departments who can add insights into the behaviors and, importantly, the underlying symptoms of fraud.

While the e-commerce fraud team should lead the efforts, consider the following departments:

- Payments teams see all payments and payment processes and are often the first to recognize a fraud issue.
- Fulfillment/logistics sees symptoms of fraud other departments may not, such as sending unusual shipments or orders with high address correction fees.
- Physical security departments in physical retail stores can share insights on what items are targeted in the store for the black market.
- Accounting manages chargebacks and will notice if patterns emerge.
- IT departments manage the critical technology for payments and fraud prevention.
- Marketing departments initiate promotional campaigns which, in turn, create opportunities for bad actors. Knowing when these campaigns are launching prepares everyone to anticipate vulnerabilities and recognize when spikes in customer behavior are due to promotions versus possible fraudulent activities.
- Customer support is the first to know when a customer orders a product and hasn't received it or is charged for an item they didn't purchase.
- Compliance must ensure customer data remains safe.

Both Habermann and Seawright agree that beyond bridging silos, companies should seek to understand the each department's goals and KPIs. This ensures everyone is on the same page - and the same team, when it comes to defeating fraud.

Building your holistic fraud prevention strategy

Ready to strategize, holistically? It's time to think like a fraudster. As Habermann explains, "Have a good understanding of how your website functions. You have to get in the head of a fraudster and how they're going to try to expose any vulnerabilities."

As Seawright adds, it's vital to understand the data — and invest in the technology that enables fast but accurate analysis. "It is literally impossible to have an effective fraud prevention strategy if you don't have it massively automated. **Identity solution providers (like Mastercard Identity) help you cull information and provide you with the data you need 100% of the time."**

Talk with other departments to identify holes. Work with other functions, especially departments like marketing, as they find creative ways to drive sales or adopt new payment methods that may also introduce new risks, Habermann suggests. Finally, talk not only with other departments to identify holes in your fraud prevention strategy, but to anticipate future spikes (like promotional campaigns). Go one step further and network with peers outside your company too - this is an industry-wide mission, after all!

In closing, remember: fraud prevention can feel overwhelming, but it's important not to minimize its importance. Preventing fraud helps to enhance customer experience and the financial security of your company, all while limiting funding for criminal acts.

"Fraud prevention is not one-size-fits-all. It's a multilayered approach and creating coalitions within and outside the organization with a holistic fraud strategy is vital to staying ahead of the escalating challenges."

MICHAEL HABERMANN,
DIRECTOR OF FRAUD SERVICES, RADIAL

Sources

1. Mastercard. (2023, September 13). Ecommerce fraud trends and statistics merchants need to know in 2024. *Mastercard.* https://b2b.mastercard.com/news-and-insights/blog/ecommerce-fraud-trends-and-statistics-merchants-need-to-know-in-2024/

2. *Online Payment Fraud Losses to Exceed $343 Billion Globally Over the Next 5 Years.* (2022, October). Juniper Research. https://www.juniperresearch.com/press/ecommerce-losses-online-payment-fraud-48bn/#

3. *2023 Global Ecommerce Payments and Fraud Report.* (n.d.). Merchant Risk Council. Retrieved February 22, 2024, from https://ww2.merchantriskcouncil.org/l/314271/2023-03-06/m2lzy/314271/1678824436MFYohYjQ/2023_Global_Ecommerce_Payments_And_Fraud_Report.pdf

4. *2023 Global Ecommerce Payments and Fraud Report.* (n.d.). Merchant Risk Council. Retrieved February 22, 2024, from https://ww2.merchantriskcouncil.org/l/314271/2023-03-06/m2lzy/314271/1678824436MFYohYjQ/2023_Global_Ecommerce_Payments_And_Fraud_Report.pdf

5. *2023 Global Ecommerce Payments and Fraud Report.* (n.d.). Merchant Risk Council. Retrieved February 22, 2024, from https://ww2.merchantriskcouncil.org/l/314271/2023-03-06/m2lzy/314271/1678824436MFYohYjQ/2023_Global_Ecommerce_Payments_And_Fraud_Report.pdf

6. *2023 Imperva Bad Bot Report | Resource Library.* (2023, May 26). Resource Library. https://www.imperva.com/resources/resource-library/reports/2023-imperva-bad-bot-report/

7. Ravelin. (n.d.-b). *Global Fraud Trends: Fraud & Payments Survey 2023.* https://pages.ravelin.com/fraud-and-payments-survey-2023

8. Identity, M. (2023, July 20). *The dark side of discounts: understanding and preventing promo code abuse.* Ekata. https://ekata.com/blog/the-dark-side-of-discounts-understanding-and-preventing-promo-code-abuse/

9. *2023 Identity Theft & Fraud Statistics | SUMSUB.* (n.d.). Sumsub. https://sumsub.com/fraud-report-2023/?utm_source=pr&utm_medium=article&utm_campaign=fraud_report2023

10. Lynch, J. (2024, February 20). *Tackling AI fraud in Retail: a new frontier in consumer misconduct.* Rosetree Solutions. https://rosetreesolutions.com/tackling-ai-fraud-in-retail/#:~:text=The%20industry%20is%20now%20facing,or%20videos%20of%20damaged%20products

11. Pymnts, & Pymnts. (2023, October 20). Digital wallets exhibit highest increase in fraud. *PYMNTS.com - What's next in payments and commerce.* https://www.pymnts.com/fraud-prevention/2023/digital-wallets-exhibit-highest-increase-in-fraud-among-all-payment-methods/#:~:text=Banks%20in%20the%20U.S.%20report,sophisticated%20fraud%20and%20financial%20crime

How Mastercard Identity helps

Today's digital economy opens a world of opportunity for everyone everywhere to connect. Mastercard Identity securely and seamlessly connects people with merchants, banks, and businesses worldwide — enabling them to interact with confidence how, where and when they want. Powered by global identity technologies, data and insights, machine learning scores and biometrics, organizations worldwide can verify and authenticate more genuine consumers and prevent fraud in real-time. From the initial account opening through account changes – and across the entire payment transaction and fraud ecosystems, Mastercard Identity instills trust on both sides of the interaction.

Learn more

studio / ID

BY INDUSTRY DIVE

studioID is Industry Dive's global content studio offering brands an ROI rich tool kit: Deep industry expertise, first-party audience insights, an editorial approach to brand storytelling, and targeted distribution capabilities. Our trusted in-house content marketers help brands power insights-fueled content programs that nurture prospects and customers from discovery through to purchase, connecting brand to demand.

LEARN MORE