# Fraudulent chargebacks set to cost merchants $15bn by 2025, warns Mastercard study



Fraudulent chargebacks are increasingly becoming a significant financial and operational challenge for businesses around the world, according to findings from a Mastercard-sponsored study conducted by Datos Insights. The research highlights an alarming trend: merchants could potentially lose a staggering $15 billion to fraudulent chargebacks by 2025. The total volume of chargebacks is projected to escalate from $33.79 billion this year to an eye-watering $41.69 billion by 2028 if effective measures are not implemented promptly.

The study identifies "first-party fraud" as a major contributor to this issue, accounting for nearly 45% of all chargebacks. This type of fraud occurs when legitimate customers falsely deny transactions, exploiting the user-friendly interfaces of banking applications that facilitate chargeback claims even in the absence of substantial evidence. Mastercard warns that, without intervention, the number of chargebacks could rise to 324 million by 2028, an increase from 261 million anticipated in 2025.

As e-commerce continues to flourish, the expansion of digital and card-not-present transactions has made online shopping more convenient but has also increased vulnerability to fraud. The implications of this rising trend are profound, affecting a broad spectrum of stakeholders from merchants to consumers.

For many merchants, particularly small and medium-sized enterprises (SMEs), the burden of dealing with chargebacks is not merely a financial inconvenience; it can threaten their very survival. The average chargeback value exceeds $120 in some industries, and as a consequence, many businesses choose to dismiss low-value claims to save time—a strategy that can lead to cumulative losses. SMEs, already under financial pressure, now find themselves at a crossroads: either absorb the losses associated with fraudulent chargebacks or heavily invest in enhanced cybersecurity measures and dispute resolution strategies.

Data from Mastercard reveals that 46% of SMEs have suffered a cyberattack, resulting in dire consequences: 18% of those affected have filed for bankruptcy, while 17% have ceased operations altogether. As a result, cybersecurity is increasingly prioritised, with 62% of SMEs considering it a top budget concern. Approximately 80% of respondents deem robust cybersecurity measures critical to daily business operations.

To tackle the growing menace of fraudulent chargebacks, Mastercard advocates for the adoption of advanced artificial intelligence tools that can improve transaction monitoring and dispute resolution processes. These technologies can offer automated alerts, clearer transaction labels, and detailed digital receipts, significantly enhancing merchants' ability to contest chargebacks effectively. According to Mastercard, businesses that employ these AI tools have had successful outcomes in over half of their representation cases.

In light of these developments, Mastercard emphasises the need for businesses to collaborate with reputable merchant service and payment gateway providers. Without cohesive strategies to combat fraudulent chargebacks, the financial strain may ultimately be passed on to consumers in the form of increased prices and slower service.

Source: [Noah Wire Services](https://www.noahwire.com)

## Bibliography

1. <https://www.mastercard.com/news/press/2023/october/mastercard-targets-friendly-fraud-to-protect-small-businesses-and-merchants> - This Mastercard press release discusses the First-Party Trust program, which aims to combat first-party fraud, also known as 'friendly fraud,' by providing merchants and issuers with tools to prove genuine purchases and prevent flawed disputes. The program leverages enhanced transaction insights, AI, and risk modeling to help merchants address the challenges posed by first-party fraud.
2. <https://b2b.mastercard.com/news-and-insights/blog/the-growing-threat-of-first-party-fraud-and-its-impact-on-the-payments-ecosystem/> - This Mastercard blog post highlights the increasing prevalence of first-party fraud, also known as 'friendly fraud,' and its significant impact on the payments ecosystem. It discusses how this type of fraud occurs when legitimate customers falsely deny transactions, exploiting user-friendly interfaces of banking applications to initiate chargebacks without substantial evidence.
3. <https://www.mastercard.com/news/perspectives/2024/sellers-beware-getting-to-the-bottom-of-first-party-fraud/> - This Mastercard Newsroom article addresses the challenges merchants face with first-party fraud, also known as 'friendly fraud,' where customers dispute legitimate transactions. It emphasizes the importance of merchants understanding and addressing this issue to prevent financial losses and operational challenges.
4. <https://www.crowdfundinsider.com/2023/02/202156-chargebacks911-says-e-commerce-merchants-should-protect-themselves-from-first-party-fraud/> - This article discusses the rise of first-party fraud, also known as 'friendly fraud,' and its impact on e-commerce merchants. It highlights the importance of merchants protecting themselves from this type of fraud, which has been increasing since 2020 and leads to significant revenue losses.
5. <https://www.merchantriskcouncil.org/who-we-are/mrc-news/press-releases/2024/for-the-first-time-in-25-years-merchants-have-identified-refund-policy-abuse> - This press release from the Merchant Risk Council reveals that, for the first time in 25 years, merchants have identified refund/policy abuse and first-party misuse as the leading threats, surpassing phishing in North America and Europe. It underscores the growing concern over first-party fraud and its impact on merchants.
6. <https://www.signifyd.com/blog/rise-in-friendly-fraud-2024/> - This blog post from Signifyd discusses the unprecedented increase in first-party e-commerce fraud, also known as 'friendly fraud,' and suggests that organized criminals are likely a significant factor in the attacks. It highlights the challenges merchants face in combating this rising threat.
7. <https://news.google.com/rss/articles/CBMihAJBVV95cUxNbU8yc2VSZ2VuNGZLdWJ4al85VS04ZThhZzFOSjBjTnFGVl95YW1iUWNOaUJJYXhYTmZBZ0pRUmVMQ3BUVkhUbXdHQ2N4cWdHeWpxZ2pSbDExcElfQVF6VTlfRzNTeURMYkxGQjVZLTVkRXdOdy0zTWozTUFuYV9LZ1pkb1pPLWdLaHhrb1ZSd2N0YlNSc1ZzMlBrNmZnbUJJWTVZNUI1ZG1oMERRS2MwQ0Vxa1owN1EtRTFSU2E5cjVCSDFMaTR0Q3lxSWlHZ19jUWR0a2RjU1Nab0NBaHYwRE4xODNVX3dRWEpFMkVXOUdMU2JnN203QWFIblowT0FJMFgtUw?oc=5&hl=en-US&gl=US&ceid=US:en> - Please view link - unable to able to access data