Fingerprint

2025

Payment fraud *trends guide*

Table of contents

Introduction to payment fraud

Both consumers and fraudsters are savvier than ever at getting something for nothing — and that usually means some kind of fraud is involved. For example, for just one kind of payment (credit cards), the amount of money lost to fraud has doubled in the past decade to around $35.8 billion for 2024. Worse still, merchants bear costs far exceeding the value of ill-begotten purchases.

When you think of payment fraud, your mind likely conjures cybercriminals buying easily resold items with stolen credit card information or a pickpocket rushing to buy as much as possible before a card is reported stolen.

And you're not wrong. But at the same time, payment fraud is also committed by everyday consumers who, by disputing the charge with their credit card, avoid paying for things they consciously bought. While some chargebacks are indeed due to merchant error, a high percentage of them are what's known as first-party fraud, which often goes by the ironic nickname "friendly fraud." Whatever you call it, it's on the rise — in 2023, chargeback abuse was up 69%.

This guide presents top trends in payment fraud — first-party, third-party, and B2B — and details the explicit and ancillary costs and impacts.

Chargebacks: The buck stops with you

“Chargeback” is one of the dirtiest words in business. It’s also a huge focus of this guide because credit cards are widely considered to be the primary means of payment fraud.

Think of your personal credit card. The Visa or Mastercard in your wallet offers zero liability protection, meaning you aren’t responsible for any fraudulent payment you report in a timely manner. (This is even more generous than the cap of $50 in consumer liability specified in the U.S. Truth In Lending Act). To a consumer, it looks like their card network is willing to take the loss if their card number gets stolen or a merchant misbehaves.

The reality is that, in most cases, it’s the merchant who pays, and then some. When someone disputes a charge, the credit card provider typically provides immediate credit to the cardholder and issues what’s known as a chargeback to that merchant, in addition to charging the merchant a chargeback fee (regardless of outcome) while researching the claim. On top of that, the merchant still owes the original transaction processing fees for each chargeback and risks incurring higher processing rates or even account termination with the credit card provider if they have excessive chargebacks.

When it comes to chargebacks, the burden of proof is on the seller. Visa has published guidelines on what it considers “compelling evidence,” and Mastercard provides thorough criteria of what data can be used to conclusively demonstrate that the cardholder knowingly made the purchase and agreed to terms that the merchant followed. Businesses can win more cases of first-party fraud with more and better evidence, such as device fingerprinting that ties a transaction to the device used to place it.

Naturally, if the issue was that the merchant failed to do right by the consumer — e.g., never delivered the goods, delivered later than promised, or that the goods were were subpar — and the credit card rightfully agrees with the cardholder, then the merchant loses the cost of the goods, whatever was sent, the processing fee, and often, the cost of shipping as well. But some consumers take advantage of this policy to dishonestly dispute transactions and often win. And even if they lose, there’s no penalty; the charge is simply restored to their card.

> *"Reversing a credit-card charge has never been easier — or more abused.”*
>
> **The Wall Street Journal** (WSJ)

Top payment fraud trends

Large-scale retail thefts have attracted widespread media attention (and resulted in more goods behind plexiglass) in the past few years. But the parallel boom in online shoplifting through first-party fraud is little-known outside the fraud prevention specialist circle and the sellers they support. There's still plenty of third-party fraud, too, and we'll cover both first-party and third-party fraud in this section.

Friendly fraud: First-party payment fraud trends

Estimates vary, but some sources estimate that first-party fraud accounts for roughly 70% of all chargebacks. We'll start by exploring the circumstances that are enabling so much fraud.

- **Low-effort chargebacks.**

  Disputing a charge used to require a call to customer service and a paper form. Now, with just a click and typing a few words, a cardholder can start a process that gets their money back immediately while creating a huge hassle and several expenses for the seller.

  Many have discovered that it's simply easier and faster to initiate a chargeback than to get in touch with customer service, but they still have to pretend that they tried and failed to get resolution directly. As many as 75% of consumers think of a chargeback as an alternative way to get a refund, even though it means they're ignoring the rules that require them to first seek a resolution directly with the seller.

- **Transaction confusion.**

  There's very little space for describing a charge on a credit card bill: MasterCard has a 22-character limit (Visa's is a relatively generous 25!). Many company names are longer than that so they must be abbreviated, sometimes beyond recognition to consumers.

  In other cases, like for recurring subscriptions (which were responsible for 36.6% of chargebacks in 2024), consumers forget that they signed up for a service and file a dispute. As a result, some people dispute transactions they willingly made simply because they don't recognize the charges on their bill. Even though it's unintentional, this kind of chargeback is a form of fraud because it recoups payment from a legitimate transaction.

- **Doesn't feel like theft.**

  Nearly half of Gen Z shoppers admit to engaging in friendly fraud. There's something about online purchases, and the widespread hunt for deals and shopping hacks, that leads people to feel less guilt or have second thoughts about working the system to their advantage. In addition to specific tactics to commit chargeback abuse as outlined below, friendly fraud also incorporates practices such as using multiple email addresses to double- or triple-dip on signup promotions or coupons.

  Additionally, numerous forums that discuss how to take advantage of consumer-friendly policies exist, such as how often you can claim damage for delivered groceries before being banned. Seeing others talking about performing friendly fraud not only gives people ideas on how to do it without getting in trouble, but also simply makes it seem more acceptable — after all, if others are doing it, why can't I?

Now, let's get into some specific types of friendly fraud that are on the rise.

- **Wardrobing and staging.**

  Most commonly affecting apparel and luxury goods, this form of return fraud involves using a product and then returning it. Wardrobing is wearing clothing and then returning; staging is buying and returning fancy items that add flair to projected images such as in social media photo shoots.

  To many consumers, buying items with the full intention of returning them feels like they're cleverly taking advantage of customer-friendly policies. To retailers, it's a huge and expensive hassle: They lose out on the cost of shipping (both ways if return shipping is free!), and return logistics are expensive, costing somewhere between $10 and $40 per item.

  There's also an environmental cost: Many returned items, especially clothing, are simply disposed of. But retailers that implement stricter return policies or require buyers to pay for return shipping also run the risk of losing legitimate customers: 82% of respondents in one survey take return policies into consideration when deciding whether to purchase from a merchant.

- **Third-party payment platforms.**

  When a buyer disputes a transaction made through a third-party payment platform, the conversation gets crowded. Now there are two entities inclined to favor the consumer: The credit card company and the platform offering some sort of buyer protection.

  Many merchants, particularly small ones that pay close attention to each chargeback, are dismayed by what looks to them like outright theft compounded by corporate indifference. Sellers who are frequently subject to this issue have to make a tough choice about whether to remove these increasingly popular payment platforms and ask themselves: Will they lose more from chargebacks or uncompleted sales because of fewer payment options?

- **"Significantly Not as Described" (SNAD) and "Item Not Received" (INR).**

  Who's to say if the item you got off eBay is exactly as it was portrayed on the site, or whether an item was unreasonably delayed or damaged in shipment? Credit cards and third-party payment platforms tend to take the consumers' side on these claims, once again leaving sellers holding the bag.

  Platforms usually withhold payment to the seller while also deducting extra from their account to cover the chargeback fee. SNAD and INR fraud has become so concerning that the Merchant Risk Council recently sent out a rare special alert to its members, pointing out practices such as false photos of damage or falsified documents.

Third-party payment fraud trends

Whether it's using stolen information to access a legitimate account to go on a shopping spree or opening new accounts using someone else's identity, fraud by third parties still runs rampant. In addition to the classic mechanisms criminals use to spend money that isn't theirs, such as card testing, here are several trends to look out for:

- **Buy now, pay-later (BNPL) fraud.**

  BNPL has ballooned as a popular way to buy something now and pay for it in multiple installments, making high-dollar items more affordable to more people. As a lightly regulated industry (for now) offering instant credit, it is a very tempting and often successful medium for fraudsters.

  Most of the techniques are the same as straightforward credit card fraud, such as using stolen or synthetic identities to apply for new accounts or performing account takeovers (ATO) to run up charges on existing accounts. (With a BNPL login, fraudsters can essentially buy from any merchant associated with that BNPL provider!)

  It's also easier to avoid detection. Sometimes fraudsters will make the first of four payments for a specific purchase, but by the time the remaining installments are due, they're long gone with the goods. If they do so with a stolen credit card, it may take a while for the consumer to notice. In the case of BNPL, however, it may go entirely unnoticed if the account holder has lots of BNPL purchases and doesn't scrutinize every line item on their bill.

  There is one bright spot for sellers, however: BNPL firms are the ones responsible for any missed payments or chargebacks since it was their decision to extend credit. However, sellers still end up paying in the form of extra fees to BNPL providers (some of which goes to covering fraud expenses), plus their damaged brand reputation in the minds of consumers whose identities were abused.

- **Synthetic identities.**

  Scammers have figured out that if they combine real and fake information and go slowly, they're much less likely to get caught. So they cultivate synthetic identities over time, based around real information such as Social Security numbers from people unlikely to use credit, such as young children. They can then add these identities to existing credit lines, establishing a legit-looking track record with a number of small transactions before committing large-scale fraud. Since these synthetic identities don't actually exist, they can cause significant losses because there isn't a real person who would flag the fraud to their financial institution — and it's something every business should pay attention to since over 80% of new account fraud is attributed to synthetic identities.

- **Customer account takeovers (ATOs).**

  Fraudsters also like using stolen credentials to break into an account at online sellers so they can make transactions using saved payment information. In 2023, ATO fraud made up 29% of all fraud in e-commerce, an increase of 7% from the previous year. Additionally, ATOs generally have the added benefit of reduced transaction scrutiny since the account already has a track record with the business.

- **Almost entirely online.**

  Only 7% of reported fraudulent third-party fraud in the U.S. resulted from physical cards being lost or stolen, which makes sense — after all, as soon as someone realizes they no longer have a card in their possession, they'll report it and have it canceled. On the other hand, as many as 80% of active credit cards have been compromised online through large-scale data breaches.

- **Business email compromise (BEC).**

  Many of the biggest, costliest, and most embarrassing hacks have come from criminals phishing or otherwise finding their way into the employees' online accounts. From there, they can cause all sorts of havoc. One common tactic is once a fraudster gets access to an executive's email, they then send urgent instructions to an employee to send a payment to a vendor via a wire transfer — but the payee account information provided belongs to the fraudster.

- **Impersonation using AI.**

  A recent study shows that 62% of businesses find that generative AI makes invoice (accounts payable) fraud more convincing. For instance, a fraudster can impersonate a supplier and send an invoice instructing that payments be sent to a new bank account. Or, combined with BEC, a scammer may impersonate a manager and urge real employees to make payments to a fake account. Generative AI makes it a whole lot easier to be convincing, such as in the case of an initially skeptical worker convinced to pay $25 million by a deepfaked CFO.

- **Real-time payment (RTP) fraud.**

  With real-time payments between bank accounts via platforms like Zelle and India's Unified Payments Interface (UPI), there's no time for canceling and no way to claw back funds. That's why fraudsters are instructing businesses to use these systems to pay fraudulent invoices. (In the U.S., where RTP is still in its infancy, check fraud is still amazingly persistent, which perhaps shouldn't be a surprise since checks display full account information right on the bottom.)

Cost of payment fraud for 2024

While there's no readily available estimate of fraud across all types of payment mechanisms, we do have a number for credit card payments: $35.8 billion. MerchantSavvy has found that although fraud as a proportion of total credit card payments globally is holding steady at around 6.5 cents per $100 spent, the total number is increasing as such payments continue to grow.

And that's just the payments themselves. Businesses incur many costs, directly and indirectly, in preventing, investigating, and responding to this form of fraud — one estimate is that every dollar of fraud costs companies a total of $3.02.

How preventing payment fraud can lead to friction for consumers

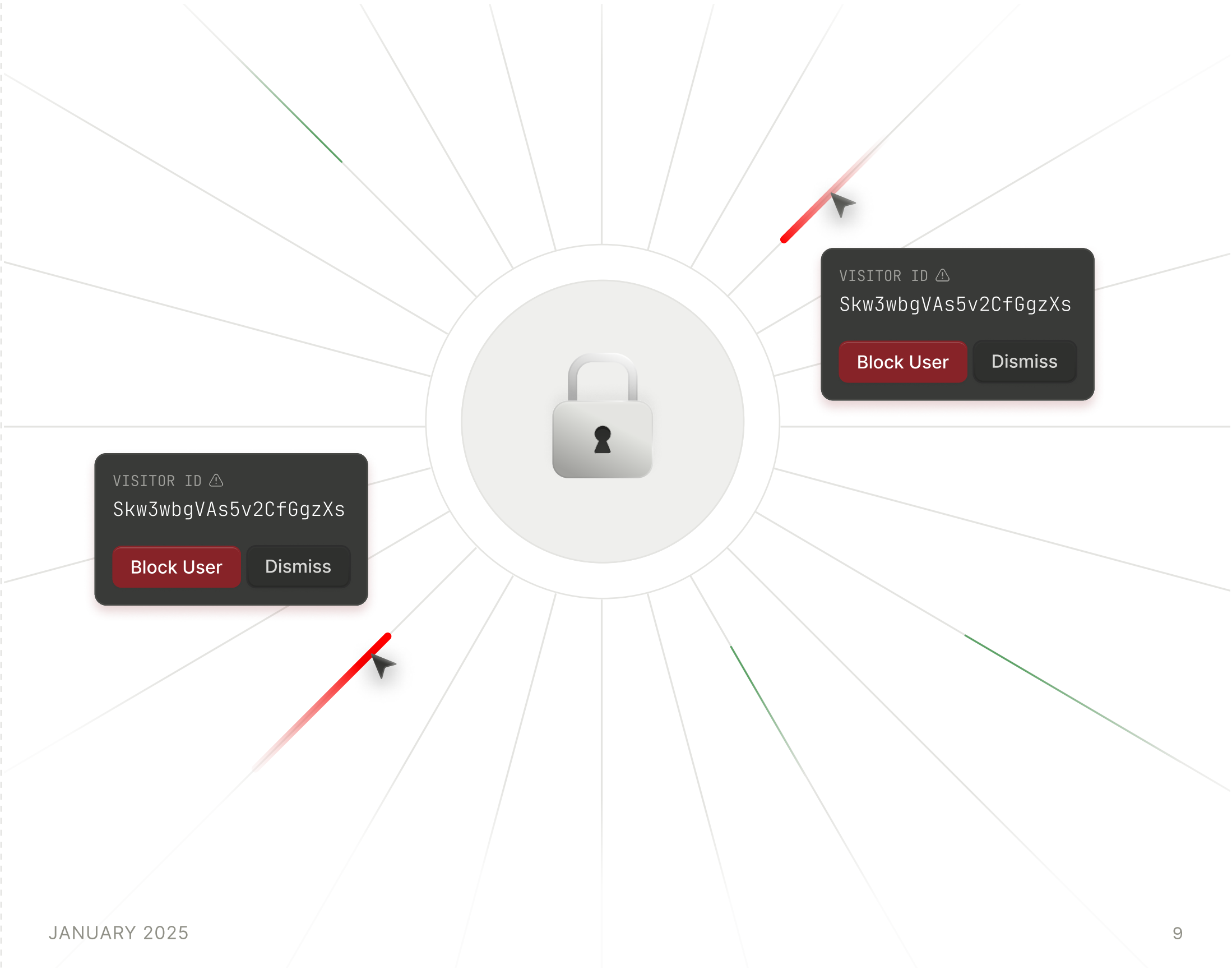
The chargeback system puts merchants in a pickle: On the one hand, they want to sell as much as they can, but on the other, they really don't want to lose the revenue in the form of chargebacks when they've already delivered the goods. As a result, they have to figure out how to make it easy and fast for honest buyers to spend their money while throwing up roadblocks for fraudsters.

We've all experienced the various ways that identity confirmation slows things down. All those codes to your email and phone to log into your account, pulling out your credit card to remind yourself of your CVV, and required verifications from your credit card create friction. These tedious processes are not only annoying, but also increase the likelihood that a shopper will abandon a purchase due to inconvenience or distraction. They also don't do very much to prevent friendly fraud.

Better ways to prevent payment fraud

There are many other ways to detect and prevent chargebacks that are less likely to annoy your buyer:

- Device identification can not only flag suspicious transactions to your risk and fraud team, but also identify repeat buyers so you can reduce authentication hassles. For instance, for chargebacks involving subscription services, the merchant can use device identification to prove that the consumer filing the dispute actually did authorize the subscription by tying their device fingerprint to the original authorization.
- Implement rules to restrict, limit, or invoke extra scrutiny on transactions from places or devices that are very unlikely to be the source of legitimate purchases.
- Keep an eye out for velocity — that is, many attempted logins or transactions from the same source in quick succession — because it's a strong signal of card cracking or testing.
- Use blocklists to reject any account, card, or device previously involved in fraud. Device identification comes into play here as well since it can help businesses see through many smokescreens, such as VPNs or incognito mode, that repeat offenders may throw up to evade detection.



How payment fraud hurts consumers

Businesses feel the sting of fraud most directly since chargebacks directly impact their revenue. But consumers feel it, too, although in subtler ways, including:

- **Increased prices.**

  Consumers can figure that a portion of what they're paying is to cover lost revenue and extra salaries as a consequence of fraud, not to mention higher merchant account rates imposed on high-chargeback sellers. Certain types of sales have higher rates of friendly fraud, such as online subscriptions and airplane travel.

- **Transaction approval delays.**

  In addition to the various authentication codes and verification steps mentioned above, some merchants may choose to manually review certain transactions, especially for easily resold items like gift cards.

- **Negative user experience.**

  On top of transaction approval delays, legitimate customers may be subject to more authentication steps they deem unnecessary and frustrating, such as having to go through multifactor authentication processes again right before completing a payment.

- **Fewer payment options.**

  Sellers fed up with very low chargeback win rates from third-party payment platforms might simply drop them as payment mechanisms, leaving fewer payment options for consumers. And because they bear the costs of chargebacks, BNPL platforms may choose to drop merchants with particularly high fraud rates.

- **International frustration.**

  Cross-border payments are more likely to be fraudulent, so such transactions invite extra scrutiny. Legit consumers can get caught up and possibly even be unable to transact if the foreign company's risk management process doesn't see them and their payment as trustworthy. According to one study, international order rejection rates are nearly double that for domestic ones, across every region.

- **Market avoidance.**

  Relatedly, certain markets known for higher rates of fraud, such as West Africa and Latin America, are underserved by financial institutions that don't find the risk worthwhile. As a result, many consumers in those regions are missing out on some of the conveniences of modern e-commerce.

- **Restrictive return policies**

  Companies facing return fraud may decide to impose limitations on returns. Some of the many ways merchants fight back on wardrobing and other types of return fraud include removing free return shipping, charging fees, limiting return windows, imposing strict requirements on the condition of the returned item, or simply declaring all sales as final.

How payment fraud hurts businesses

You saw above that fraud costs much more than just lost revenue. We'll break down some of the specifics.

- **False declines.**

  Far outweighing the direct cost of payment fraud is all the transactions declined for fear of fraud. To add to the pain, frustrated consumers may leave poor reviews or tell others to shop elsewhere.

- **Chargeback fees.**

  Win or lose, merchants pay a hefty fee for each chargeback, generally between $20 and $60, but it potentially can be even higher. The exact amount is subject to the merchant agreement between the processor and the seller, but the fee can sometimes even exceed the original transaction amount.

- **Increased chargeback fees.**

  Chargeback fees are progressive: If you have a lot of chargebacks, your fees may increase, both in terms of the percentage you pay on every transaction, as well as each chargeback fee being higher than the baseline. If it worsens, you may be assessed hefty penalties, up to and including being banned by Visa, Mastercard, and/or other credit card issuers.

- **Operational diversion and distraction.**

  Fighting payment fraud has hard costs like fraud prevention software subscriptions, in addition to the costs tied to support staff investigating and responding to fraud and chargebacks.

How to detect & prevent payment fraud

Preventing payment fraud requires adopting new anti-fraud strategies and technologies as fraudsters change their tactics. We recommend:

- **Requiring multifactor authentication (MFA).**

  While requiring MFA at login or during the checkout process creates some friction for legitimate buyers, it also helps reduce the chances of unauthorized access and account takeovers by adding an extra layer of security.

- **Implementing device intelligence.**

  Using a device intelligence platform like Fingerprint can add another layer of security on top of a password and MFA — or even as an alternative for MFA for returning website visitors. Device intelligence works by collecting and analyzing a number of signals from the browser, device, and network, and assigning every device a unique visitor ID. Merchants can choose to configure their risk and fraud systems to bypass MFA requirements for returning customers who are using previously identified devices, which helps reduce friction for legitimate users — or require MFA for any new, unrecognized device.

- **Setting up automated alerts for high-risk transactions.**

  High-risk transactions, such as those involving large dollar amounts or originating from high-risk locations, should require special attention. Such transactions should be flagged for manual review so a trained analyst can assess whether they're legitimate.

- **Ensuring your business descriptor is recognizable on statements.**

  Reduce unintentional chargebacks by choosing an easily recognizable descriptor that will show up on credit card statements. For example, seeing "Spotify" as a recurring subscription charge is less likely to raise alarms and result in chargebacks than something vague like "8.5% Sales Tax" (this is a real-life example).

KEY TAKEAWAYS

Fighting fraud requires a multifaceted approach

The history of payment fraud is at least as long as that of commerce: Before chargebacks, card testing, and account takeovers, merchants worried about bad checks, forged currency, or people who simply skipped town after establishing store credit (the original BNPL!). The Internet has simply changed how it's committed.

As we've seen, payment fraud is widespread and multifaceted. The costs go far beyond lost revenue and lost goods, and it's tough to strike the right balance between reducing risk and increasing sales. It's also constantly evolving; as society and technology change, so do the approaches fraudsters take.

Fortunately, you're not alone. In fact, every company that sells things online has to deal with similar issues. While it requires concerted effort and investment, you have access to the tools, techniques, and people that can make for a comprehensive and successful payment fraud response.

Fingerprint offers one such tool: When you can identify individual devices, regardless of changes in browsers, logins, or IP address, you can overcome several of the techniques used for both first-party and third-party fraud. Sign up for a 14-day free trial or contact us for a personalized demo.