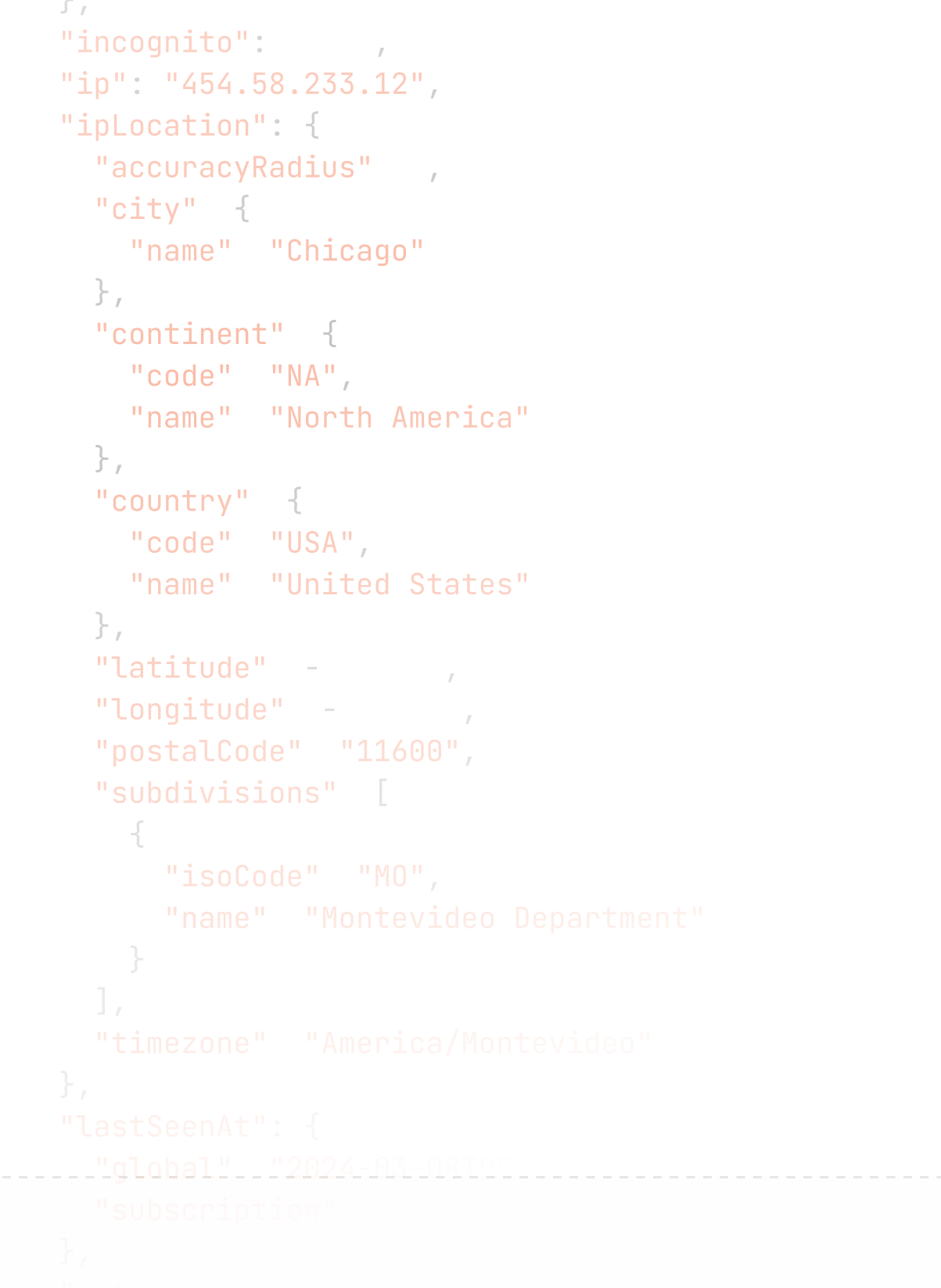
Fingerprint



A GUIDE FOR ONLINE MARKETPLACES & FINANCIAL SERVICES

The impact of payment fraud on UX, conversions & customer retention

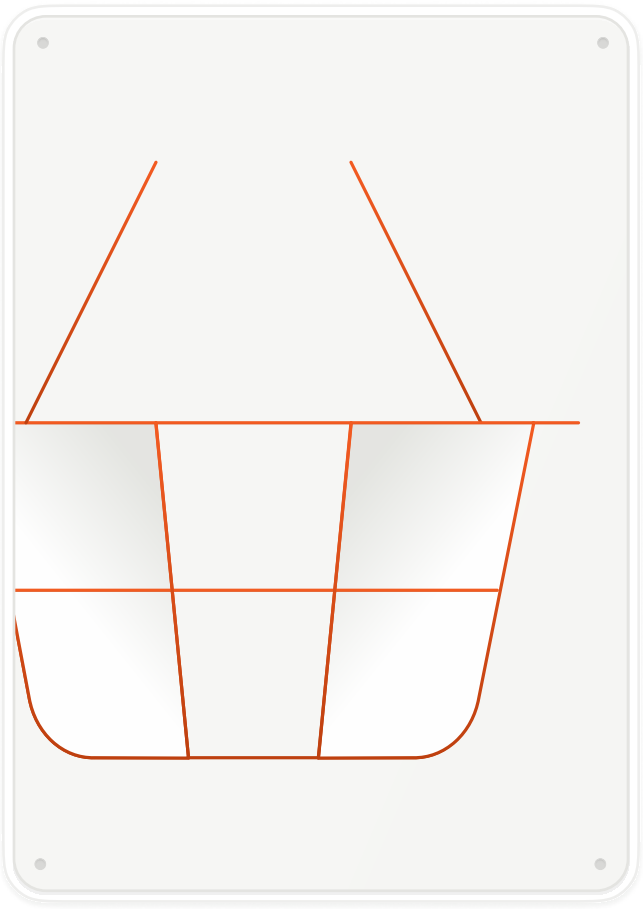
Table of contents

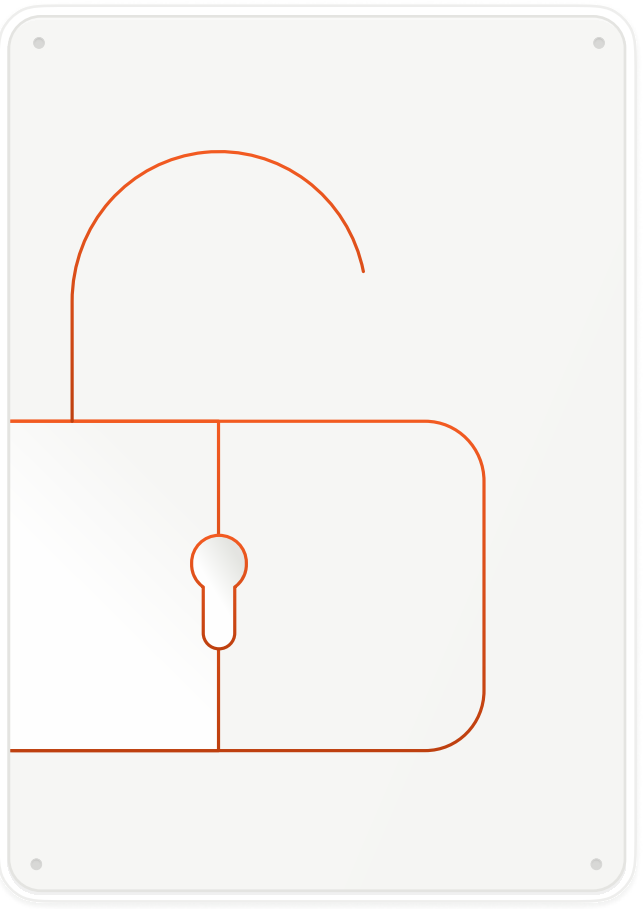
Introduction

It’s no secret: Consumers love convenience. From shopping for groceries to sending payments to friends using apps like Venmo, many are reaping the benefits of being able to run a lot of their errands without ever leaving the couch.

But with increased online services and convenience also comes an increase in fraud risk — more specifically, payment fraud. Fraudsters are taking full advantage of the shift consumers are making to online services and finding new ways to exploit weaknesses in different payment systems.

In this guide, we’ll dive into the most common types of payment fraud, how it impacts online marketplaces and businesses offering financial services, and recommended strategies for combating fraudsters without causing unnecessary friction for legitimate customers — so you can take control of fraud before it takes control of your business.





What is payment fraud?

Payment fraud comes in many different forms, and fraudsters are always looking for new ways to cause trouble. They use various techniques to access customer data or business financial information, including credit details, bank account information, usernames, passwords, and other personally identifiable information (PII). Once they have this information, they can then transfer money out of a bank account or go on a shopping spree, resulting in headaches and financial losses for both customers and businesses.

The most common payment fraud types impacting marketplaces and financial services include:

Card-not-present fraud

Card-not-present fraud (CNP) has surged as online shopping became increasingly popular. Fraudsters use stolen credit card information for transactions where a physical card isn't required, such as when making purchases in online marketplaces. In 2023, CNP fraud losses in the U.S. alone totaled $9.2 billion and are projected to reach $28.1 billion globally by 2026.[1]

Chargeback fraud

Chargebacks are estimated to total over $12.8 billion in the U.S. by 2026,[2] and tackling chargeback fraud can help reduce that number.

One type of chargeback fraud is known as "friendly fraud," which is when customers dispute legitimate charges with their bank, claiming they didn't authorize the purchase when they actually did.

The other type of chargeback fraud is when a bad actor uses stolen credit card details to make a purchase. Here are couple of tactics they commonly use:

- **Card testing** is when a fraudster attempts a number of small transactions to see if the stolen credit card details they have — often purchased off the dark web or acquired through a data breach — are valid. If those transactions go through, then they proceed to make a big purchase.
- **Card cracking** is slightly different: The fraudster will have some of the details for a valid credit card, but not all. Generally, they'll write a bot script to test different combinations of numbers in quick succession to guess, for example, the CVV code and expiration date. Once they hit on a combo that works, they'll proceed with making fraudulent purchases.

Once the legitimate cardholder notices these unauthorized transactions, they will then file chargeback disputes. Both the friendly fraud and stolen credit card scenarios result in lost revenue, in addition to investigation costs and the cost of goods and services purchased.

Even worse, too many chargebacks can damage your business's reputation with payment processing providers and increase your payment processing fees — or cause them to drop you altogether as part of their merchant network.

[1] "The growing threat of CNP fraud," Finance Magnates

[2] "Chargeback trends and outlook: 2023 report," Ethoca by Mastercard

Account takeover fraud

Account takeover (ATO) fraud can be devastating for victims and happens when fraudsters gain unauthorized access to customer accounts, often using credentials exposed in data breaches or obtained through phishing.

Once they have access to an account, the fraudster can then transfer money to themselves, apply for loans, use stored credit cards to make purchases, or change mailing addresses and login information, the latter of which effectively blocks the legitimate customer from accessing their own account.

Buy now, pay later (BNPL) fraud

Buy now, pay later (BNL) services are experiencing widespread adoption and are on track to reach $687 billion in transactions by 2028.[3] Between that and the often too-easy credit check process, BNPL is a highly lucrative target for fraudsters.

A couple of the most common types of BNPL fraud include ATO and non-repayment fraud. In ATO situations, fraudsters will either obtain accurate login information or brute-force their way into the accounts of BNPL customers to take advantage of pre-approved credit and stored payment information to make unauthorized purchases.

Non-repayment fraud happens when a bad actor places an order with no intention to pay. They typically do this with a fake or stolen identity so they can't be traced or caught. (We cover BNPL fraud in more detail in this article.)

Coupon & promo abuse

Coupon and promo abuse can seriously impact an online business's revenues and involve a variety of tactics. For instance, fraudsters can hide their online identities to claim discounts or use coupon codes repeatedly. They may use bots or other tactics to bypass restrictions, exploiting promotions and exclusive offers meant to be used once, diminishing the effectiveness of your promotions and depriving legitimate customers of them.

[3] "Global buy now, pay later market: 2024-2028," Juniper Research

How payment fraud impacts online shops & marketplaces

More consumers than ever are spending their money in online marketplaces, from booking their next Airbnb stay and buying their Christmas tree on Amazon, to booking their flights on Kayak. These marketplaces have added over $1.7 trillion in consumer spending to the economy in 2019 and are projected to exceed $7 trillion in 2024.[4]

This massive growth has made digital marketplaces prime targets for online fraud attacks, with losses estimated at billions of dollars per year. Adding to the challenge are the diverse products these marketplaces offer which makes them vulnerable to different payment fraud attempts — for example, online travel booking sites may be targeted for account takeovers, where fraudsters use customer accounts to purchase tickets that they later resell. Online retailers selling clothing, on the other hand, may be targeted with credit card fraud, such as card testing and cracking.

Payment fraud impacts marketplaces in several ways, including:

Increased losses tied to fraud

First and foremost, payment fraud impacts every online seller's bottom line. It's not just the cost of the goods lost to fraudsters — online businesses also need to factor in shipping costs and the cost of refunds to the legitimate customer.

Operational costs also come into play when we're talking about disputing "friendly fraud" chargebacks due to the time required to research and submit evidence to payment processors (18% of merchants spend more than 20 minutes per chargeback dispute).[5]

Additionally, having too many chargebacks filed can increase payment processing fees for the merchant or — even worse — cause a payment processor to drop a business altogether from its merchant network, which could negatively impact future sales.

Loss of customer trust

Customers need to be able to trust that a brand will provide the best services and goods possible while keeping their personal and financial information safe. For example, when big names like Ticketmaster suffer data breaches[6] or when smaller brands fail to protect customer information, it can negatively impact the company's reputation, resulting in lower customer retention and lower sales.

In fact, a survey found that 65% of customers would stop purchasing from a brand where their account was breached, and 30% said that they would discourage friends from shopping from that brand as well.[7]

[4] "Online marketplaces set to exceed $7 trillion in sales by 2024," Payment Industry Intelligence: Payments Cards & Mobile

[5] "Three surprising costs of chargebacks and their impact on e-commerce," Riskified

[6] "Ticketmaster confirms customer data breach," Malwarebytes

[7] "Fighting payments fraud in online marketplaces," Payoneer

Increased friction leading to abandoned carts

In their efforts to stop payment fraud, many online marketplaces have implemented additional security measures like multifactor authentication (MFA), one-time passwords (OTP), and CAPTCHA tests.

While additional authentication steps can help, they can also cause friction for legitimate customers who simply want to log in and complete their purchase as smoothly as possible — and when faced with additional, what-may-seem-unnecessary steps, they may abandon the transaction completely.

Losing customers to false declines

Another way of losing customers is having a risk engine trained with poor data that inadvertently results in a high number of false declines (also known as false positives). For example, if a customer has traveled to another country for work and places an order online, a merchant might flag that transaction as fraudulent and decline to process the payment, despite it falling within the usual purchase patterns for that particular customer.

Why does this matter? Because in 2022, a survey found that 19% of customers in the U.S. won't attempt the same purchase again after a false decline[8] and may choose to shop elsewhere permanently, resulting in not just a lost sale now, but also potentially future sales as well.

[8] "False declines explained," Checkout.com

Preventing payment fraud for online shops & marketplaces

We recommend a few techniques that online businesses and marketplaces can use to help prevent payment fraud without adding unnecessary friction for legitimate customers.

Use a reputable payment processor & require CVV input

Using a reputable payment processor and system is table stakes for operating an online marketplace. Unsecured payment systems are a target for fraudsters who can exploit weak defenses to steal sensitive information, such as credit card numbers, bank account details, and other personally identifiable information (PII).

Additionally, to help prevent ATO and CNP fraud, consider having customers input the CVV code from their credit card every time they check out.

Regularly monitor & audit transactions

Define normal and abnormal transaction behavior based on historical data and industry benchmarks. Automated monitoring protocols can then be set up to alert your risk and fraud team whenever a transaction falls outside defined parameters.

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

Additionally, conducting routine audits that involve a comprehensive review of transaction records is highly recommended. Doing so can help identify patterns or trends that automated systems may miss, such as repeated attempts at small transactions (which is a common sign of card testing) or a sudden increase in transactions from a specific location.

Consider adopting reliable & accurate visitor identification

Identifying website visitors should be an important part of your payment fraud prevention strategy. By using a device intelligence platform like Fingerprint, online businesses and marketplaces can, for example, detect in real time when users are attempting to conceal their identity or location via a VPN and quickly flag potentially suspicious visitors.

How payment fraud impacts banking & financial services

Banks and the financial services industry overall serve as stewards of everyone's money. So it's no surprise that they are commonly targeted by fraudsters. A recent report released by the European Central Bank and the European Banking Authority found that money lost to payment fraud in the European Economic Area totaled €2.0 billion in the first half of 2023.[9] In the United States, 42% of financial institutions saw an increase in fraud in 2024, with a corresponding increase in the total dollars lost to fraud.[10]

Payment fraud can have far-reaching consequences for financial institutions, including:

Significant financial losses

Just one fraudulent transaction (or even 10) doesn't seem like much, but they add up. Surprisingly, check fraud is still a big issue, even as people give up paying with physical checks in favor of more convenient payment methods. With physical checks, criminals can easily alter the payee or payment amount, forge account holders' signatures, or print counterfeit checks.

In total, payment fraud, credit card fraud, and check fraud contributed $137.2 billion in losses for financial institutions in the Americas in 2023. Globally, that number increases to $442 billion.[11]

Loss of customer trust & reputational damage

Imagine being a customer of a bank, and someone accessed and emptied your account. You're now responsible for reporting the theft and filing a complaint with the bank. Then you have to wait for the investigation to be completed, and in the end, you may not get all your money back.

Even though it was a fraudster who stole the money, customers will blame the bank for failing to protect them. And if it happens often enough or on a large enough scale, customers will move their accounts to a competitor that is perceived to have better anti-fraud security measures in place. In fact, 50% of customers are willing to switch banks if they're not getting the services they want and expect. [12]

Being subject to regulatory fines & legal action

Morgan Stanley, a global financial services company, was fined $60 million by the U.S. Treasury Department for potentially exposing customer PII data.[13] Additionally, a $5 million class action lawsuit was filed by affected customers soon after.

Ally Bank is another example. A proposed class action lawsuit was filed in 2024 against the bank for failing to protect its customers against a data breach.[14] Customers' PII, including Social Security numbers, dates of birth, addresses, and more were exposed on an unspecified date, and allegedly are now for sale on the dark web.

[9] Press release, "ECB and EBA publish joint report on payment fraud," European Central Bank

[10] "The state of fraud and financial crime in the U.S. 2024: What FIs need to know. November 2024 Report," PYMNTS.com

[11] 2024 Global financial crime report: Insights at the intersection of financial crime data & real survivor stories," Nasdaq Verafi

[12] "Chargeback trends and outlook: 2023 report," Ethoca by Mastercard

[13] "Morgan Stanley fined $60 million for data protection mishaps," GDPR register

[14] "Ally Bank faces class action lawsuit over data breach," National Mortgage Professional

Preventing payment fraud in banking & financial services

Preventing payment fraud is a continued challenge for banks and other businesses providing financial services, from fintechs to credit card providers, as fraudsters use technologies to find new ways of bypassing online security checks. To help prevent payment fraud, we recommend incorporating the following into an overall risk and fraud prevention strategy:

Empower customers with ongoing education

Providing information to customers on how they can recognize phishing attempts — such as suspicious emails full of typos or text messages asking them to log into their bank account — can help empower them to protect their own money and data.

Require multifactor authentication (MFA)

If you're a financial institution or a business providing financial services, implementing MFA is a must, not a nice-to-have. While it adds a bit of friction for the customer, adding this extra layer of security is worth the extra hurdle for legitimate users because it helps reduce the changes of unauthorized access (and, by extension, account takeovers).

Set up automated alerts for potentially suspicious transactions

We recommend configuring your risk and fraud detection systems to monitor transactions in real time and send alerts for any anomalies, such as transactions in unfamiliar locations or an unusually large purchase.

Implement device intelligence

Device intelligence can be an invisible, added layer of security on top of a password and MFA — or even be used as an alternative to MFA in certain instances. For example, Fingerprint's device intelligence platform collects and analyzes a number of signals from the browser, device, and network, and assigns every device a unique visitor ID to help risk and fraud teams better differentiate legitimate users from suspicious ones.

With device intelligence in place, you can choose to configure your systems to bypass MFA for returning customers who are using previously identified devices, which reduces friction for legitimate users — or require MFA every time for any new, unrecognized device.

Key takeaways

Preventing payment fraud without negatively impacting the user experience is a challenge that online marketplaces, banks, and financial services are continuously trying to solve.

By taking a multifaceted approach that combines new technology like device intelligence with other, traditional security checks like MFA, your risk and fraud teams can shore up fraud detection and prevention efforts to better protect customers and your bottom line.

Interested in learning more? Reach out to our sales team today for a personalized demo.

About Fingerprint

Fingerprint, the world's most accurate device intelligence platform, enables companies to prevent fraud and improve user experiences. Fingerprint processes 100+ signals from the browser, device, and network to generate a stable and persistent unique visitor identifier that can be used to understand visitor behavior. Fingerprint is ISO 27001 certified, and SOC 2 Type II, GDPR, and CCPA compliant. Fingerprint also meets the Strong Customer Authentication (SCA) requirements as outlined by PSD2. Fingerprint is trusted by over 6,000 companies worldwide, including 16% of the top 500 websites, to help catch sophisticated fraudsters and personalize experiences for trusted users.

Learn more at fingerprint.com