Payment Fraud Guide 2024: Detection and Prevention

Learn about the types of payment fraud out there, how they relate to money laundering, and how businesses can safeguard themselves.

Payment fraud is a challenge, and it's only going to get worse in the coming years. According to Statista, fraudulent transactions using payment cards alone are expected to increase to $38.5 billion by 2027.

Payment fraud detection and prevention, therefore, is paramount for businesses and their clients—not only for anti-money laundering (AML) compliance, but also to protect assets and business reputations. However, it isn't the simplest of tasks, since fraudsters are constantly looking for new ways to commit payment fraud—whether it's using social engineering or creating look-alike domains to pose as legitimate vendors.

Let's dive into payment fraud, ways to prevent it, how to ensure that your business—and your clients—can avoid malicious scams.

What is payment fraud?

Payment fraud is stealing payment information to make unauthorized transactions. There are two broad categories:

1. "Card-present" fraud, which occurs when criminals use stolen or counterfeit cards to make purchases in-person (say, at an ATM or brick-and-mortar shop). This has become less common, however, as criminals have mostly turned their attention to online fraud.
2. "Card-not-present" fraud, which occurs online. This kind of fraud usually involves unauthorized use of payment information (card number, billing address, CVV and expiration date) to purchase products online—for instance, through e-commerce websites.

What industries are most prone to payment fraud?

Industries that deal with high transaction volumes and sensitive financial data are most at-risk. Some of the most vulnerable sectors include:

- **Financial services.** Banks, neobanks, credit card companies, and other financial institutions are prime targets due to the large sums of money they handle.

- **iGaming.** Online gaming and gambling platforms face instances of stolen credit card information and fraudulent transactions. Continuous learning ensures these systems stay updated with emerging fraud patterns.
- **E-commerce.** With the rise of online shopping, e-commerce platforms are frequent targets for fraudulent activities like account takeover and card-not-present fraud.
- **Hospitality.** Hotels, restaurants, and travel agencies are susceptible to payment fraud, especially through unauthorized credit card use or fraudulent bookings.
- **Healthcare.** Healthcare providers are targeted for insurance fraud, prescription fraud, and billing scams.
- **Telecommunications.** Telecom companies often deal with fraudulent activities such as subscription fraud and SIM swapping.
- **Insurance.** Insurance companies contend with fraudulent claims and identity theft, impacting their profitability and operational efficiency.
- **Non-profit organizations.** Charities and non-profits face risks including donation fraud and misuse of funds. They are also especially vulnerable to money laundering.

How does online payment fraud work?

Step 1: Fraudsters steal your personal information

The first thing that fraudsters need to commit payment fraud is personal information. Here are some ways that they can get their hands on it:

- Social engineering

  This is a manipulation technique that involves tricking people into disclosing their sensitive data. This can be when a criminal calls their victim pretending to be a bank representative—using a technique called **spoofing**—and asks them to confirm their account details, including payment information.

- Phishing

  The most common method of social engineering is **phishing**, which uses emails, phone calls, texts, and social media to gather sensitive personal data from unsuspecting victims. This can be when criminals send an email pretending to be from a legitimate online service, containing a malicious link that fools the victim into entering their login credentials—which leads to **account takeover** and **identity theft**.

- Business email compromise (BEC)

  This is a complex form of phishing that targets a businesses' sensitive information and finances. Targets include HR, accounting departments,

or even high-level executives like the CFO. The goal is to use social engineering techniques to trick members of an organization into sharing highly-sensitive information or making unauthorized payments.

- Enumeration

  Fraudsters can also use a technique called enumeration. This is when hackers determine login credentials using brute-forcing software, which tests numerous combinations to pass the authentication process. Once an account is compromised, hackers can get their hands on sensitive personal information—especially payment details.

Step 2: Fraudsters use your personal information to make unauthorized purchases.

Types of payment fraud

Once fraudsters get their hands on personal information, they have multiple ways to commit payment fraud:

Credit card fraud

If someone's credit card information is leaked in full, fraudsters can simply commit credit card fraud, which is when unauthorized purchases are made using someone else's payment information—usually with the aim of obtaining and reselling products.

Card testing

Full payment details aren't always available to fraudsters, which opens the door to other payment fraud techniques—such as card testing. This is when fraudsters, in this case known as "carders", test stolen credit card numbers to see which can be used to make unauthorized purchases. This can either be done manually, where the fraudster checks card validity by making small purchases—or by using special special bots to test large numbers of cards within a short time span, which is known as carding. Proper transaction monitoring tools can help spot carding and card testing attacks ahead of time.

Triangulation fraud

Triangulation fraud involves three parties—an unaware customer, an online shop, and a fraudster as a middleman. It usually happens as follows: an unsuspecting customer places an order with a fraudulent seller at a legit marketplace (such as Amazon). The fraudulent seller then places an order for the actual product from a legitimate seller using a stolen credit card.

Online gaming scam

Fraudsters can develop an online game that gets listed on the App Store or Google Play. The players of the game are then asked to pay a small fee in order to continue playing, which enables the fraudsters to eventually extract a much larger amount from the card linked to their Apple ID.

To offer a game on the App Store, it's necessary to have a bank account. In this case, fraudsters open bank accounts with neobanks and MSBs, rather than with traditional financial institutions. Therefore, fintech companies need a high-quality business verification service.

Chargeback fraud (aka "friendly fraud")

Not all payment fraud involves stealing personal information through social engineering and so on. **Friendly fraud** is when someone makes an intentional purchase online, and then contacts their bank to dispute the charge by falsely claiming that the transaction was invalid. To recognize this kind of fraud, it's important to monitor customers' behavioral patterns.

A reliable transaction monitoring tool lets businesses set triggers that detect suspicious transactions and anomalies, such as purchases made by the same client simultaneously, unusually large transactions (above the AML threshold), and high-risk countries.

How does payment fraud affect businesses?

Online payment fraud statistics

According to the AFP 2022 Payments Fraud and Control Report:

71%
of survey respondents reported their organizations falling victim to payment fraud attacks in 2021.

68%
of organizations were targeted by business email compromise (BEC) in 2021.

66%
of all payment fraud was committed using checks, with 37% committed using ACH debits.

58%
of survey respondents stated that their Accounts Payable departments fell victim to payment fraud through email scams. AP departments continue to be the most susceptible to BEC.

According to Statista, e-commerce losses to payment fraud were estimated at $41 billion globally in 2022, up from the previous year. This figure is expected to grow to $48 billion by 2023.

Sources: AFP 2022 Payments Fraud and Control Report, Statista

Payment fraud is devastating for businesses, causing enormous losses which are expected to grow.

Juniper Research recently predicted that merchant losses from online payment fraud would exceed $362 billion globally between 2023 to 2028, with losses of $91 billion in 2028 alone.

Therefore, all businesses that deal with high transaction volumes and sensitive financial data should implement robust anti-fraud measures to stay ahead of fraudsters.

How to detect payment fraud

The following red flags often signal payment fraud:

- Unusual transaction amounts
- Unusual cross-border or international transactions
- Unusual frequency of transactions

- Unusual transaction types
- Change of payment method
- Mismatch of username and payment method
- Recurring refunds
- Unknown chargebacks
- Unfamiliar shipping addresses
- Shipping addresses too far from the IP address
- Errors in ID documents
- Transactions exceeding the account balance or credit limits.

How to prevent payment fraud

There are steps businesses should follow to effectively prevent payment fraud:

- Taking a risk-based approach towards customers, partners, and vendors
- Cyber-security measures and policies, like secure VPNs, etc.
- Using AI-based behavioral fraud detection
- Conducting regular employee training
- Using a reliable KYC solution to onboard only trustworthy users
- Requesting face authentication in case of unusual activity
- Using a reliable business verification solution to know and trust the partners and corporate customers you work with
- Using a transaction monitoring tool to quickly detect unusual transactions
- Encrypting transactions
- Using up-to-date software.

FAQ

What is considered payment fraud?

Payment fraud is any unauthorized or deceptive activity aimed at obtaining money or valuables through illegitimate means during a transaction or payment process.

How common is payment fraud?

Unfortunately, payment fraud is common and keeps growing. Businesses lose billions of dollars annually globally due to various fraudulent schemes and tactics across multiple industries.

What is transaction fraud detection?

Transaction fraud detection involves the use of algorithms and technologies to identify and prevent fraudulent activities in real-time.

How can you avoid online payment fraud?

- Be aware of the latest fraud trends and red flags
- Protect your personal data and online accounts with multi-factor authentication
- Use KYC, KYB, and transaction monitoring tools

sumsub

Start exploring Sumsub today.

Get started