Merchant Guide
for E-Commerce Fraud Protection

clearsale

Merchant Guide for E-Commerce Fraud Protection

Introduction

As e-commerce explodes in popularity, so does e-commerce fraud – and every e-commerce merchant, from tiny start-ups to massive chains, is vulnerable. There are multiple types of fraud and ways to prevent it — but managing fraud protection the wrong way can be costly and frustrating.

It's important, therefore, to understand exactly what e-commerce fraud looks like, what other risks merchants face, and what e-commerce fraud protection tools can help thwart these attacks without inadvertently turning away good customers.

That's why we've built this resource: to help you understand your risks, so you can take the right steps to protect your business, your profits, and your good reputation.
Let's dive in!

Shortcuts

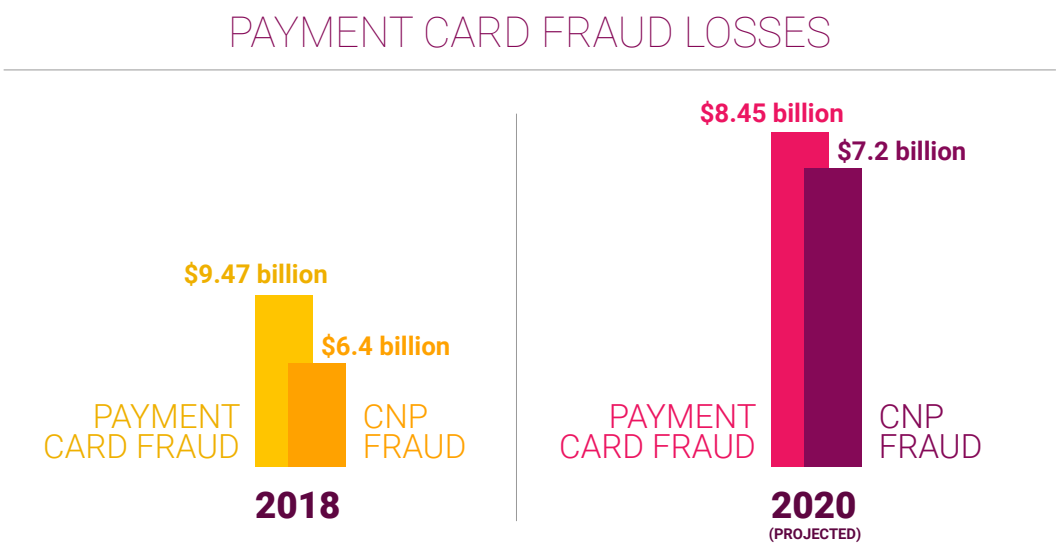
Introduction to E-Commerce Fraud

Whether you're a longstanding multichannel retail organization with millions of dollars in sales or a small retailer getting your business off the ground, e-commerce fraud is aggravating and expensive.

Growth in Fraud Attacks on Merchants

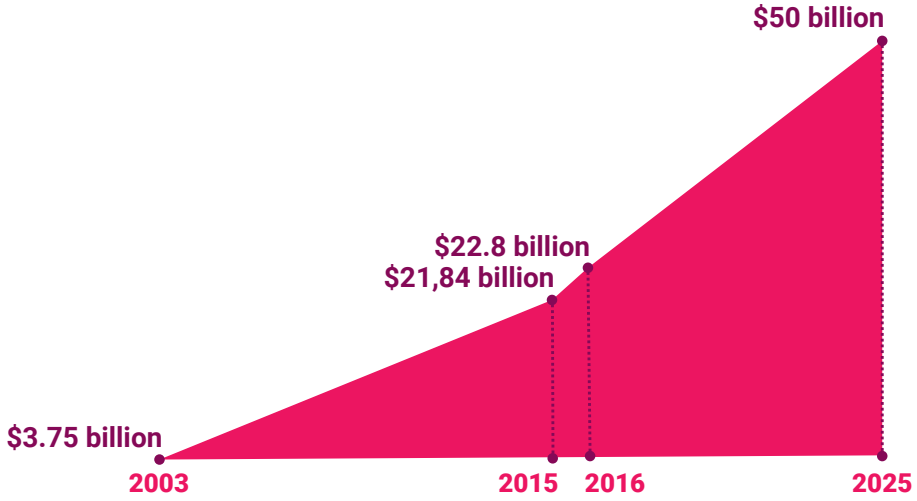
E-commerce fraud is on the rise. Fraud attack rates have **increased sharply** year over year.

In **2018**, payment card fraud losses incurred by merchants and card issuers in the United States alone totaled **$9.47 billion**, with **$6.4 billion** of that being **card-not-present fraud**. In **2020**, the U.S. total is projected to be more than **$8.45 billion**, with **$7.2 billion** being CNP fraud.



Globally, losses incurred by merchants and card issuers due to fraud **grew** from **$3.75 billion in 2003** to **$21.84 billion in 2015**. And from 2016 to 2025, these losses are projected to **nearly double**, rising from **$22.8 billion** to nearly **$50 billion**.

LOSSES INCURRED BY MERCHANTS AND CARD ISSUERS



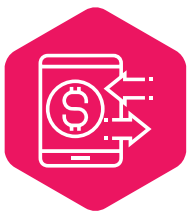
According to Experian, data breaches are one of the **biggest drivers** of credit card fraud. As private data is stolen, it gets sold to fraudsters who use it to attack retail businesses. Considering the number of data breaches that took place in 2019, including the massive **Capital One**, Marriot and Facebook data breaches, e-commerce retailers will need to batten down the hatches and prepare for a tsunami of fraud attempts in the near future.

Cost of Fraud Attacks

The repercussions of fraud are serious. Becoming a victim of fraud means dealing with:

The cost of lost merchandise

The cost of shipping and handing **on fraudulent orders**



Chargeback fees from the issuing bank

Negative hits on your company's reputation

Potential loss of your merchant account

Every dollar lost to fraud costs merchants **$3.13**. For mid to large e-commerce merchants selling digital goods, that number leaps to $3.50 per dollar of fraud.

Fraud can take a large bite out of a company's bottom line, and can even put the future of the company in jeopardy.

To fight it, the first step is to understand what types of fraud attacks merchants might face.

Understanding
E-Commerce Fraud

clearsale

Understanding E-Commerce Fraud

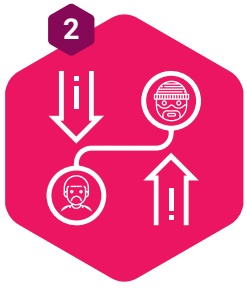
There are multiple ways in which a business can experience fraud, from deliberate card-not-present fraud to friendly fraud caused by miscommunication. All industries are vulnerable, but some industries have a considerably larger target on their backs.

Types of E-Commerce Fraud

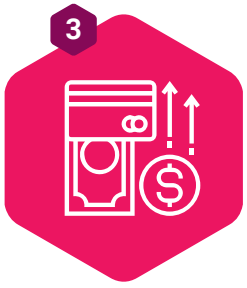
Card-Not-Present Fraud

Card-not-present (CNP) fraud can happen in three ways:

Use of a stolen credit card



Theft of a consumer's identity



Use of stolen card data, without presenting **the actual card itself**

In CNP fraud, the following process takes place:

1. **A fraudster** makes a purchase at an online store using someone else's credit card.
2. **The acquirer** (or issuing bank) checks if the card has enough balance and approves the purchase.
3. **The transaction** is completed and the goods delivered to the fraudster.
4. **The actual cardholder** does not recognize the purchase and asks for a chargeback.
5. **The online store** reimburses the cardholder and is left with a loss.
6. **In some cases**, the store is listed on credit card blacklists and may be penalized as well.

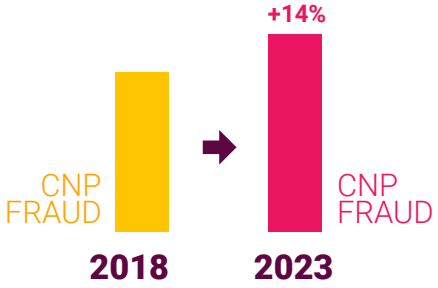
Preventing physical card theft can be relatively straightforward. Preventing identity theft and card data theft? That's more complicated.

Even if a consumer is exceedingly cautious with their own data, fraudsters are using increasingly sophisticated tools:

- **Skimming** — stealing card information at the point of sale
- **Phishing** — conning the cardholder out of their numbers either via email or over the phone
- **Account takeover** — hacking into a consumer's online session to steal the consumer's account numbers and passwords.
- **Pharming** — installing malicious code on a computer to steal personal data

And that's not even taking into account the huge amount of identity theft that is taking place as the result of large-scale data breaches. Unfortunately, many consumers have no idea their card data or identity has been stolen until they receive their bill. By that time, the fraudsters have received their thousands (or more) of dollars in merchandise and have moved on to the next victim.

Alarmingly, CNP fraud is growing quickly. In the United States alone, CNP fraud is estimated to **leap by 14%** between **2018** and **2023**, and businesses are at risk of losing an average of **5%** of their gross revenues to fraud. **In fact, mid to large retailers selling only physical goods experienced 606 successful fraudulent transactions monthly, while those selling digital goods reported an astonishing 1,242 fraudulent transactions monthly**.



That's bad enough, but the **average number of fraudulent transactions** per month have risen every year and show no signs of slowing down, meaning losses are expected to rise as well.

Friendly Fraud

Despite its non-threatening name, friendly fraud is no friend to your business.

Friendly fraud is when a customer makes a purchase with a legitimate credit card, is issued the merchandise or service, and then contacts their credit card company to dispute the charge.

Friendly fraud is a form of fraud, but it is not done maliciously. There are many reasons why friendly fraud could occur:

The customer might believe their package was stolen.

They might believe they returned the item, but that a refund was never processed.

The customer might not recognize the merchant's name on their statement.

They might be disputing recurring charges, saying nobody notified them that these charges would take place.

The tricky part is that without meticulous record-keeping, it's difficult to know if the customer is telling the truth or trying to defraud you. Nonetheless, friendly fraud is a growing concern, and the losses can be significant. When the credit card issuer processes the chargeback, the merchant is on the hook for chargeback and processing fees, shipping fees, penalties, and staff time lost to dealing with the issue.

Chargeback Fraud

While **chargebacks** were initially developed by card issuers to protect consumers, the chargeback process has become so easy that people often game the system and knowingly commit chargeback fraud. In these cases, customers intentionally file fraudulent chargebacks with the goal of keeping the product or service they ordered while also receiving a refund of the full transaction amount.

Chargeback fraud can take place in a variety of ways, including when the customer:

- Places an order with the explicit intent to get free products
- Experiences buyer's remorse and regrets a high-priced purchase
- Hides a purchase from a spouse or joint account holder
- Tries to lower their credit card balance

E-Commerce Fraud and Industry Risk

While virtually all e-commerce and multichannel retailers are at risk for fraud, some industries tend to be popular targets.

Being in a **"high-risk"** industry makes fighting fraud particularly difficult. Not only do companies face more than their fair share of fraud attempts, but in many cases, traditional merchant account providers will steer clear of these businesses and refuse to open accounts for clients in these industries. In those cases, businesses must resort to **high-risk credit card processors**, who tend to impose much higher fees and stricter conditions, cutting deeply into the merchant's bottom line.

Two factors determine whether a merchant account provider will deem a business high-risk:

The **industry** that it's in

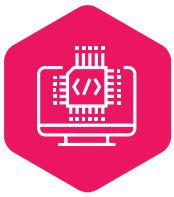
The **types of transactions** it does

High-Risk Industries

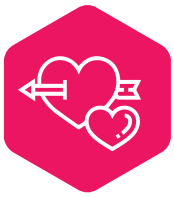
The riskiest industries for fraud and chargebacks tend to be those that provide services (which are hard to prove as being delivered or not delivered) or those that provide goods with a high resell value on the black market.

Across the board, high-risk industries typically include:

Adult entertainment



Computer software or hardware



Dating services

Electronics

High-Risk Industries

Across the board, high-risk industries typically include (cont.):

Financial services

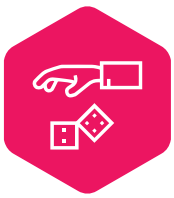
Firearms

Gaming

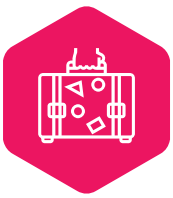
Health and wellness

Jewelry

Legal services



Online gambling or casinos



Travel and hospitality

High-Risk Transaction Types

Transactions that tend to raise red flags with merchant account providers include:

- Accepting **recurring payments**
- Conducting transactions in multiple currencies or countries with **traditionally elevated levels** of fraud
- Having high monthly sales volumes or individual transactions
- Having cyclical sales
- Being in an industry with historically high **chargeback ratios**
- Offering subscription-based products or services
- Having not yet established a payment processing history

Even if your industry is considered low-risk, it doesn't mean you're immune. Some fraudsters like to target lower-risk industries, figuring their guard is down and they'll be easier to scam.

One of the biggest ways e-commerce fraud hits merchants hard is the chargeback. What are chargebacks, how do they happen and what can merchants do to protect themselves?

Understanding Chargebacks

clearsale

Understanding Chargebacks

In addition to being aware of CNP chargeback fraud and friendly fraud, merchants need to be aware of chargebacks.

The Chargeback Process

A **chargeback** is when a customer, faced with a charge on their credit card, files a dispute with their credit card issuer.

Once a chargeback request is filed, a series of steps takes place:

1. **The credit** card issuer contacts the business's merchant account provider.
2. **The merchant** submits documents to prove the chargeback is invalid.
3. **If the merchant loses the chargeback,** the merchant account provider reverses whatever payment was made to the merchant and charges an additional chargeback fee.

Types of Chargebacks

Chargebacks can fall into **three categories**: legitimate chargebacks, friendly fraud and chargeback fraud.

Legitimate Chargebacks

Legitimate chargebacks occur when the merchant is genuinely at fault – for example, if the merchant charged the customer without fulfilling the sale or if the merchant shipped a different product from what the customer ordered.

Friendly Fraud

Friendly fraud is a gray area, where the reason for the chargeback isn't legitimate, but it's also not malicious. **In some cases,** the customer doesn't understand the company's return process. Or the customer may not recognize a particular charge or merchant's name on their credit card statement.

If a company is hard to contact, has unclear return policies, or doesn't work with the customer to resolve an issue, they're highly likely to see more friendly fraud chargebacks than average.

Chargeback Fraud

In other cases, the chargeback is entirely fraudulent. For example, a fraudster may claim that the item was never received, when in fact it was. Or the fraudster may place an order with their own card but then claim that the card was stolen and the transaction was fraudulent, all while they're sitting with the merchandise in hand.

Because of the time it takes to process and adjudicate chargebacks, and because the onus is on the merchant to prove that the chargeback is invalid, chargeback fraud can be extremely time-consuming and frustrating, requiring a lot of **records retrieval** and back-and-forth with the merchant account provider and credit card issuer.

> And in addition to costing time and patience, chargebacks can put **a significant dent** in a merchant's bottom line.

Chargeback Fees and Chargeback Ratios

In addition to the lost inventory and shipping costs, merchants who lose a chargeback also face **chargeback fees** and other penalties.

The fees vary by merchant account provider, but they can range from $50 to over $75 per dispute. For a small merchant, this can be disastrous.

If you're a larger e-commerce or multi-channel business, $50 to $75 here or there might be a drop in the bucket and not worth worrying about.

However, there's another problem: the **chargeback ratio**. If a business experiences a high percentage of chargebacks relative to overall transactions (over 1%, as a general rule), **the merchant account provider may freeze (or even terminate)** the merchant's credit card account. And if the account is closed due to excessive chargebacks, the merchant may be forced to accept sky-high processing rates to reopen their account … if they can get approved for payment processing at all.

Chargeback Solutions

To prevent excessive chargebacks from harming their business, many merchants look into either chargeback protection or chargeback insurance as a solution. But **what is the difference** between these two options?

Chargeback Protection: Typically offers tools to help you monitor transactions and identify/prevent fraud, and may cover a portion of the potential losses a business might incur due to chargebacks.

Chargeback Insurance: Provides a guarantee that covers the merchant if the fraud solution partner approves a transaction that turns out to be fraudulent and results in a chargeback.

These two solutions are very different, so it's critical for merchants to understand which approach is right for them, and which approach is offered by the vendors they're considering.

To see how the two types of chargeback solutions fit into a broader fraud protection strategy, let's explore how e-commerce fraud protection works and the different options available to merchants.

Fraud Detection, Fraud Prevention and Fraud Management

clearsale

Fraud Detection, Fraud Prevention and Fraud Management

When it comes to fraud, the worst mistake is to stick your head in the sand and hope it won't affect you. When looking for a way to guard against fraud, however, there are several different options from which you can choose and a number of things to keep in mind when making a decision.

Fraud Filters

The first typical line of defense against fraud is the **fraud filter**.

Fraud filters are provided by your e-commerce platform and designed to identify potentially fraudulent orders and prevent them from being processed. They work in multiple ways, depending upon which one you use:

- **Velocity filters** limit how many sales can be submitted to your website during a given time period. This prevents fraudsters with lists of stolen credit card numbers from testing them all on your business.
- **IP Address** mismatches can flag transactions in which the customer's IP address and shipping address don't match, a potential fraud indicator.
- A **card verification value (CVV) filter** looks for errors in the CVV number being submitted.
- A **purchase amount filter** flags high-dollar transactions that fall outside the business's typical range.
- An **address verification service (AVS)** declines or flags transactions when the billing and shipping addresses don't match, to keep card thieves from having merchandise sent anywhere but to the cardholder.
- A **Time-of-Purchase** filter can flag or even block transactions that happen during timeframes when fraudulent transactions are more likely to occur.

While these filters can offer a fair amount of protection, they're **far from perfect**. For example, during peak sales times like Black Friday, velocity filters can slow sales down and result in customers being turned away. Similarly, during the holidays, AVS filters can create a large number of **false declines**: If a customer purchases a gift item, or if they request an order be shipped to their work address instead of home, the AVS filter might decline the legitimate transaction.

Some merchants try to solve these issues by layering multiple levels of fraud filters. However, if the filters aren't applied in the correct order, some rules could wind up being contradictory to other rules, and the merchant may end up exposed to even more levels of fraud or false declines.

The Dangers of False Declines

The topic of false declines naturally comes up when talking about fraud filters, but **what ARE false declines?**

False declines take place when legitimate transactions get caught up in the merchant's (or e-commerce site's) fraud filters and are inadvertently declined. Examples of false declines include:

- **A grandmother** buys gifts and has them shipped directly to her grandkids, but the AVS filter flags the orders as fraudulent.
- **A couple is travelling** out of the country, and while ordering something online to be delivered to their home, the fraud filter declines it based on their current location.
- **A merchant has the good luck of a product going viral online,** but the sudden influx of sales triggers the velocity filter, turning away scores of customers.

False declines are a massive concern, with losses due to false declines predicted to grow to **$443 billion by 2021**, dwarfing the estimated $6.4 billion in e-commerce fraud losses.

In addition, false declines can have a nasty ripple effect. They're embarrassing and inconvenient for customers, who in turn react negatively:

They walk. 19% of cardholders **will refuse** to shop with a merchant after a false decline, while 24% decrease their purchase levels with the merchant. For businesses that sell high-end goods that typically have a smaller sales volume, like cars, travel or luxury goods, losing even one customer can be devastating.

They talk. According to an **American Express study**, U.S. consumers tell an average of 11 people about good customer service experiences, but they tell 15 about poor experiences. And if they do their talking via **social media**, complaints can easily be seen by thousands of people.

Many merchants, when trying to protect themselves against fraud, can find themselves implementing fraud rules and filters that are too strict and inflexible. In trying to protect themselves from fraud losses, they end up incurring even greater losses due to false declines.

For this reason, many e-commerce and multi channel merchants choose a more sophisticated fraud management solution.

Manual Fraud Review

Manual fraud review is just that: a team of individuals reviewing each transaction (or a selection of transactions) to detect fraud. This can be done in-house through a fraud-review team that analyzes orders, or through a third party, where the merchant sends orders that seem "iffy" to a vendor for them to analyze.

Manual fraud review has pros and cons:

Advantages of Manual Fraud Review

On one hand, people tend to be **better at understanding context** than automated fraud filters. Trained fraud experts can look at each situation individually instead of blindly adhering to preset rules.

These experts can also **dig quite deep** while investigating, for example, by performing reverse lookup searches on addresses and phone numbers, calling a bank to verify records, and even calling the customer to ask authentication questions.

Disadvantages of Manual Fraud Review

On the other hand, manual review is very time – and resource-intensive. Even the best manual reviewer can't work as quickly as a computer program, so customers may have to wait slightly longer to be approved for their orders.

Also, the effectiveness of the review is only as good as the expertise of the individual staff members performing the review. If you want to keep your manual review team **in-house**, you'll need to hire experienced staff or pay to train them. And if you have a high turnover of employees, your results with manual review may be inconsistent. **Outsourcing** your manual fraud review may solve these issues.

Machine Learning/AI

Because of the increase in both the quantity and sophistication of fraud attempts, many companies are turning to technology. Software that relies on machine learning or artificial intelligence (AI) can provide a fast and reliable way to screen out fraud. These programs rely on mathematical algorithms and data to identify fraud trends and patterns.

Because no humans are involved in this form of fraud detection, machine learning is scalable and consistent, applying the same level of scrutiny to every transaction.

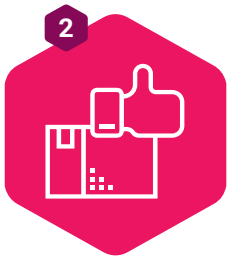
Unfortunately, this consistency **can be a double-edged sword**. Fraud solutions that rely solely on machine learning can be inflexible. Different industries, and even different merchants within the same industry, may experience different fraud attempt patterns that **slip under the AI's radar** – not to mention new types of fraud that won't be part of the algorithm's database until it's updated.

Lastly, **false declines tend to increase** when using only AI/machine learning, since there is no human intuition or analysis. A program won't be able to call a long time client to get more information; instead, it will instead simply decline the purchase. But what if this client was simply shopping online while travelling abroad? You'll lose the sale and possibly the customer, too.

Fraud Managed Services

Fraud managed services incorporate a two-pronged approach:

Prevent fraud



... and protect the merchant
if a fraudulent transaction
does slip through

The **managed services solution** does this by blending a fraud protection strategy, chargeback management strategies, and a **team of trained fraud analysts**. The solution can be used in place of an expensive internal fraud team or to supplement an in-house team, particularly during times of increased sales volumes.

Typically, as an order comes in, it is screened in real time using **automated technology** that may include geolocation, email validation, fraud filters, machine learning, and fraud score.

However, at no point is an order automatically declined. Instead, any order that fails to pass the initial screening is sent to human analysis. There, a team of expert analysts reviews the order to see if data is missing, compare the order to typical cardholder or store behavior, and contact the customer for further authentication if needed.

There are **major advantages** to this approach:

- **Because no transaction** is automatically declined, the merchant's rate of false declines is greatly reduced.
- **Expert human analysts** can quickly spot new **fraud trends** and flag them for insertion into the AI's algorithms.
- **The human analysts** can **work alongside** an in-house fraud team, or in consultation with the client, bringing specific business/industry insight to their fraud screening.
- **The solution is easily scalable** for peak sales times, while still providing specific review of each flagged transaction.

Conclusion

With increasingly clever attack tactics and a wealth of stolen personal data at their fingertips, the number of people attempting to defraud merchants will only grow in coming years.

Companies stand to lose billions of dollars, both in fraudulent transactions and in lost revenue from false declines.

When it comes to e-commerce fraud protection, there are many factors to consider. In addition to making sure your customers' data is as secure as possible, you also want to make sure fraudsters aren't slipping past your defenses and cutting into your profits.

By becoming better informed about the types of fraud out there and how it can be stopped, you'll be better protected from fraud damaging or even destroying your business.

clearsale

E-Commerce Fraud FAQs

My online store is "low-risk." Even so, should I add a risk management tool?

There are two reasons why your company might be low-risk:

1. Your company cancels any order it finds suspicious. This solves the fraud problem, but you are likely losing numerous safe purchases made by good customers who, for some reason, fit the risk profile or have made a small error during the transaction. This can lead to the **loss of a future loyal customer**.

2. Your company has yet to be discovered by fraudsters. This is just a question of time and market exposure. Once a merchant is protected from fraud, fraudsters migrate to other stores that offer an easier target.

What are the losses resulting from fraud?

Losses can extend far beyond the value of the goods lost due to fraudulent purchases. If fraud management is not properly handled, high levels of unauthorized purchases due to suspected fraud or lengthy analyses can lead to lost sales, loss of any marketing investment, an adverse effect on the merchant's image and, most importantly, lost customers.

Merchants may not realize that transactions can be declined for the smallest errors. This may lead to loss of immediate revenue from the purchase or, more importantly, loss of a future loyal customer. As data breaches and fraud rises security restrictions are becoming tighter. The need for hands-on fraud management for every merchant is now vital.

clearsale

E-Commerce Fraud FAQs

What should merchants know about preventing fraud for online sales?

The survival of a company that operates in the virtual world depends in part on minimizing its **financial losses due to fraud** and on its ability to approve the largest number of orders in as short a time as possible.

Therefore, a good anti-fraud service will include a thorough risk management system that ensures high rates of approved sales while minimizing chargebacks, all of this in as short a response time as possible. Companies that do not practice fraud risk management run the risk of **turning down good orders** because fraud is suspected and delaying order approvals as they lack the analytical skills and resources required.

What is a chargeback?

A **chargeback** occurs when a customer disputes a charge on his/her credit card bill. If the true owner of the card does not recognize the purchase, he or she will ask for their money back by filing a complaint regarding a non-authorized transaction with the issuing bank. This is known as a chargeback.

In practice, the card administrator in the process of financial settlement between the parties debits the amount that would be transferred to the merchant.

clearsale

E-Commerce Fraud FAQs

To learn more about e-commerce fraud protection, please visit our selection of **videos** and **e-books** that go into more depth on these issues.

Ready to start empowering your business with ClearSale's fraud protection solutions? **Let's get started.**

www.clear.sale/getstarted

clearsale


clearsale