ClearSale

Guide

Small Business Guide to Ecommerce Fraud Protection

For small ecommerce businesses, managing fraud is frustrating. It takes a lot of time, resources and expertise to effectively fight fraud on your own ... all while you're flat-out busy growing your business.

Ready to Get Started?

Call us at +1 786 888 4584 or email contact@clear.sale to speak with a fraud expert today!

www.clear.sale

But fraud prevention can't be a "when we have time" activity, especially in today's post-pandemic ecommerce environment

Online shopping has increased to the tune of $900 billion more in spending, with about 30% of that growth continuing to stay strong or increase.

And with more transactions come more fraud attempts: **Experts predict online payment fraud will cost small businesses more than $206 billion cumulatively between 2021 and 2025.**

This puts most small ecommerce businesses in a tight spot:

- If they ignore ecommerce fraud, they risk their revenue, their merchant account and their business reputation.
- If they try to handle it in-house, they're taking time and resources away from other, more strategic business activities.
- And if they turn their fraud filters up to 11 and call it a day? They risk a trail of angry would-be customers. False declines are a big no-no among consumers: 40% of customers won't shop with you again if their transaction is declined, and 34% will take their beef to social media.

To effectively fight fraud, you need to understand ecommerce fraud, how it affects small business, the prevention steps you can take and what steps will work best for your business.

When it comes to choosing a fraud prevention solution, the variety of options can make you feel like you're comparing apples to oranges. That's why we created this guide — to help you take the right steps to protect your business, your profits and your reputation.

About ClearSale

ClearSale is a global pioneer and proven leader in ecommerce fraud protection and prevention solutions. Founded in 2001, we offer innovative fraud solutions that combine advanced machine learning and expert manual review to provide convenient, cost-effective and accurate fraud management.

All Chapters

About this guide

This guide has everything small-business owners like you need to know to fight fraud in the most effective way possible.

You'll learn:

- How fraudsters attack small businesses and the signs of ecommerce fraud
- How to stop fraud attacks without inadvertently declining good customers
- How to select the right fraud management solution

Ready?
Let's dive in!

Part 1

The State of Ecommerce

Ready to Get Started?

Call us at +1 786 888 4584 or email contact@clear.sale
to speak with a fraud expert today!

www.clear.sale

Part 1

The State of Ecommerce

In 2020, ecommerce took a giant step forward. In fact, analysts estimate that the industry experienced about **five years of growth** in a single year—mostly because the pandemic forced people to shop online to the tune of over **$3.9 trillion in sales**.

And while the incline isn't as steep in recent months, ecommerce sales continue to grow.

In our original research report, **What Consumers Thought About Ecommerce, Fraud & CX in 2021**, we discovered that **45% of consumers shop online at least once a week.**

And those who were once uncomfortable with the idea of making purchases on their PCs, phones and even social media channels are now embracing it. So much so, nearly 66% of people told us they are more likely to use their mobile phone for purchases.

Related Reading

2021 Global Ecommerce Consumer Behavior Analysis

READ MORE

And what about younger consumers? They're already online in droves: 55% of millennials are shopping online at least once a week.

Have any of these ecommerce fans been burned by fraud? Sure, but it's still not stopping them: Although 68% of our study respondents had experienced some form of ecommerce fraud, most said they felt shopping online was as safe or safer than shopping in a store.

That's good news for small ecommerce businesses.

But there's a catch: Customers are forgiving of businesses if they're victims of a fraud experience, but not so if they're falsely accused of fraud.

Part 1

As a business owner, your job is to provide a great ecommerce experience … while protecting your online business from fraud … without declining legitimate orders. It's a lot to juggle, especially considering how rapidly ecommerce fraud is growing.

Ecommerce Fraud Is Growing Worse

Ecommerce fraud is expected to grow exponentially over the next five years. The Federal Trade Commission received 436,000 fraud reports from consumers between January 2020 and April 2021, equaling $399 million in losses. And the average fraud amount rose 35% in April 2020 — early in the pandemic.

A Juniper Research study entitled "**Online Payment Fraud: Emerging Threats, Segment Analysis & Market Forecasts 2021-2025**" estimates ecommerce payment fraud will exceed $206 billion cumulatively through 2025. China is projected to be hit the worst with over 40% of global losses equaling over $12 billion by 2025.

The biggest sources of fraud are related to credit cards and account takeovers (ATOs):

- In 2020, 115 million stolen debit and credit cards were posted for sale on the dark web, and over 75% of them were from U.S. consumers. Those cards and card data are sold to fraudsters who use them to attack retail businesses.

- The data breaches that have taken place in the last several years, including the massive Capital One, Marriott and Facebook data breaches, have provided fraudsters with a wealth of personal and financial data — increasing account takeovers by over 280%.

Fraudsters also found new areas of opportunity, thanks to the new ways consumers shopped during the pandemic. BOPIS (buy online, pickup in store) fraud increased by 55%, and buy now, pay later fraud schemes have popped up as well.

Related Reading

Learn how fraudsters mine social media for credit card and account information:
How Social Media Hacks Compromise Your Fraud Protection Efforts

READ MORE

ClearSale

Part 1

5 Small-Business Costs of Ecommerce Fraud Attacks

The repercussions of fraud for a small business can be serious, leaving you facing:

- The cost of lost merchandise
- The cost of shipping and handling on fraudulent orders
- Chargeback fees from the issuing bank
- Negative hits on your company's reputation
- Potential loss of your account

Stopping Fraud Can Boost Business Growth

Think about the time and resources you allocate to dealing with fraud and the cascading financial impacts. For small businesses, battling fraud can be so time-consuming, it may seem like a line of business in and of itself … except this one depletes your bottom line.

Implementing a fraud prevention solution can solve that problem, allowing you to focus on what's most important for your business growth. You'll have less churn, better use of resources and more time to spend on sales and fulfilling orders. Plus, you'll get to keep more of your hard-earned revenue.

But to successfully fight fraud, you need to start by understanding the types of ecommerce fraud attacks small businesses can face.

Part 2

Recognizing Ecommerce Fraud

Ready to Get Started?

Call us at +1 786 888 4584 or email contact@clear.sale
to speak with a fraud expert today!

www.clear.sale

Part 2

Recognizing Ecommerce Fraud

Not all fraud is created equal. Businesses experience ecommerce fraud in many ways — from deliberate card-not-present fraud to friendly fraud caused by miscommunication.

Additionally, while all industries (and countries) are vulnerable, some face a higher risk of fraud … and may be subject to different fraud patterns or types of attacks.

Types of Ecommerce Fraud

While you may be familiar with ecommerce fraud in general, you might not know there are several different types of ecommerce fraud — all of which can create big headaches for you and your business.

Card-not-present fraud

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

1. **Use of a stolen** credit card
2. **Theft of a consumer's** identity
3. **Use of stolen card data**, without presenting the actual card itself

Part 2

In CNP fraud, the following process takes place:

A fraudster makes a purchase at an online store using someone else's credit card information.

The acquirer (or issuing bank) checks if the card has enough balance and approves the purchase.

The transaction is completed, and the goods are delivered to the fraudster.

The actual cardholder does not recognize the purchase and notifies the merchant (or more commonly, their card issuer).

The online store reimburses the cardholder and is left with a loss.

In many cases, the store is also penalized with a chargeback fee.

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

Pharming — installing malicious code on a computer to steal personal data

And that's not even counting the identity theft resulting from 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, fraudsters have stolen thousands (or more) of dollars in merchandise and have moved on to the next victim.

Part 2

Alarmingly, CNP fraud is growing quickly. In the United States alone, CNP fraud is estimated to **increase by 14% and cost ecommerce businesses $130 billion by 2023**. Small ecommerce businesses experienced a 27% increase in successful fraud attempts in 2020, compared to 2019, likely due to the prevalence of online shopping throughout the year. Of the **2,450 fraud attempts in an average month**, 916 were successful.

Small ecommerce businesses experienced a 27% increase in successful fraud attempts in 2020, compared to 2019.

What does that mean for your business? **Fraudsters have gotten smarter, more skilled and more able to work around fraud prevention. Small businesses need to up their game in this new era of ecommerce.**

Account takeover (ATO) fraud

A type of CNP fraud, **ATO fraud** is one of the fastest-growing fraud risks in the ecommerce industry. Bank and social media data breaches combined with text and email scams enabled a **307% increase** in ATOs between 2019 and 2021.

ATO fraud happens when fraudsters purchase stolen customer data on the dark web and use it to make fraudulent purchases. In 2021, the cost of data breaches **grew to $4.24 million**, the highest level in 17 years.

Fraudsters commit ATO and CNP fraud using a similar process:

- A fraudster uses stolen credit card or bank information to make a purchase online.
- Once the purchase is approved by the payment processor, the transaction is completed.

Part 2

- The purchased goods are shipped to the fraudster.
- When the actual consumer doesn't recognize the purchase, they contact their bank or payment processor.
- The online business must reimburse the consumer, but the costs of shipping and goods sold are lost.
- Most often, companies also have to pay a penalty to the payment processor — known as a chargeback.

Another thing to consider when it comes to CNP and ATO fraud is the damage to your reputation. **In our 2021 Consumer Attitudes report, 84% of consumers reported they would never again shop with a business that approved a fraudulent order with their credit card.**

Social commerce fraud

With the rising popularity of **Instagram Shop**, **Pinterest Lens** and even TikTok as a source of online shopping, social commerce is booming. Experts expect it to reach more than **$604 billion by 2027**.

It only follows that social commerce fraud is booming as well. For starters, fraudsters create fake brand accounts to perpetrate a variety of fraud schemes, from phishing to triangulation fraud. In the fashion industry alone, impostor brands are promoted on as many as **65 million fake posts every year** and almost 20% of all fashion product posts from 50,000 on Instagram are fraudulent.

The other issue is with passwords. When the **most common password** used by consumers in the United States is "123456," it's not hard to hack into an account. And when you factor in how many people use the same passwords across their accounts, a single data breach can be a mother lode of opportunity for a fraudster.

Part 2

Friendly fraud

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

Friendly fraud happens when a customer makes a purchase with a legitimate credit card, was delivered the merchandise or service, but then disputes the charge.

While it is considered a form of fraud, it is usually not done maliciously and can happen for several reasons:

- The customer might believe their package was stolen, but it was just misplaced.
- The customer might not recognize the company's name on their statement.
- They might be disputing recurring charges, saying nobody notified them that these charges would take place.

The tricky part of friendly fraud is that without meticulous record-keeping, it's almost impossible 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 in shipping fees, staff time lost to dealing with the issue, and chargebacks.

Related Reading:
Friendly Fraud: What Ecommerce Merchants Need to Know
READ MORE

Part 2

Chargeback fraud

While chargebacks were initially developed by card issuers to protect consumers, the chargeback process has become so easy, some people game the system and knowingly commit chargeback fraud.

> The chargeback process has become so easy that some people game the system and knowingly commit chargeback fraud.

They 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

We'll dive much more deeply into chargebacks a little later on, so keep reading!

Related Reading:
Get more statistics, insights and tips on identifying ecommerce fraud: Ecommerce Fraud Protection for Online Merchants: The Ultimate Guide
READ MORE

Part 2

Channel-specific ecommerce fraud

Internet shopping has come a long way from the days of simply purchasing online using home-based computers. Consumers are now shopping with multiple types of devices in omnichannel environments. This includes but is not limited to:

- Voice commerce
- Mobile and tablet commerce
- Gaming consoles
- IoT devices such as watches
- Vehicles

Each of those channels presents a new fraud risk for small businesses.

Social commerce has exploded on apps like Instagram and Facebook, which creates a perfect opportunity for CNP fraud — the leading cause of ecommerce fraud today. Fake social media accounts lure consumers into making purchases that never materialize. Nearly **20% of the fashion product posts** on Instagram come from imposter brands that promote up to **65 million fake posts** each year.

Meanwhile, voice commerce using smart speakers like Amazon's Alexa, Apple's Siri, Google Assistant and Microsoft Cortana are expected to generate sales of **$80 billion by 2023**.

Related Reading:

Thinking about voice commerce? Make it easier for customers to voice search on your site: 4 Ways to Optimize Your Online Store for Voice Search Commerce

READ MORE

ClearSale

Part 2

Ecommerce Fraud and Risk Factors

While all ecommerce and multichannel retailers are at risk for fraud, some businesses tend to be more popular targets. These are referred to as **"high-risk"** businesses.

Being a high-risk business makes it even more difficult to fight fraud — not just because of the tactics fraudsters use, but because many payment processors shy away from high-risk businesses.

Add to that the risks of increased chargebacks, and you have a trifecta of challenges. Often, these businesses have no choice but to work with **high-risk credit card processors**, who tend to impose much higher fees and stricter conditions, cutting deeply into the company's bottom line.

A number of factors determine whether a business account provider will deem a business high-risk, but the two most common are industry and transaction types.

High-risk industries

The riskiest industries for fraud and chargebacks tend to be service providers and businesses that sell goods with a high resell value on the black market. **Service providers are considered high-risk simply because it's harder to prove that a service has been delivered.**

While **high-risk industries** vary based on consumer demand, here are some industries that typically struggle with fraud risk:

- XXX Adult **entertainment**
- Automotive **parts and accessories**
- Computer software, hardware and other **consumer electronics**
- Cannabis and **CBD products**

Part 2

- Dating services
- Financial services
- Firearms
- Gaming
- Health and wellness
- Luxury goods and jewelry
- Legal services
- Nutraceuticals and OTC drugs
- Online gambling or casinos
- Travel and hospitality

Want to learn more about your particular industry's ecommerce trends and fraud risk? Explore our in-depth industry guides.

Industry Insights

Fashion and Luxury

More than 18 years of experience with global leading luxury and fashion brands.

Automotive Parts

The auto parts sector has been growing along with general online retail sales, but not everything in this sector is sweet!

Travel and Airlines

The travel industry, especially airlines, faces unique additional challenges regarding card-not-present fraud.

Consumer Electronics

Your customers are always on the lookout for the latest electronic goods. Unfortunately, fraudsters are, too.

Part 2

High-risk transaction types

It's not only certain industries that are at risk. Some ecommerce businesses may find themselves at a higher risk of fraud simply because of how they do business. Transactions that tend to raise red flags with account providers include:

- Accepting **recurring payments**
- 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

High-risk geography

Another factor that small businesses don't always think about — but payment processors do consider — is geography.

Within the United States, some **states have higher fraud rates**, and any online business in that state could be considered riskier for payment processors to take on.

Certain countries also face higher fraud rates, such as **Mexico**, or **China** with its particularly high mobile fraud rate. At the same time, both of those countries present **opportunities for cross-border** ecommerce, so there is a reward that goes along with the risk.

Expanding into new territory? Explore some of the most dynamic and promising ecommerce markets in the world, with our Country Profiles.

Country Profiles

United States
The United States has long enticed businesses as the land of opportunity.

Mexico
Everything you need to know about the market, buying habits and fraud to launch an ecommerce business in Mexico.

United Kingdom
Know the differences you must be prepared for if you plan to expand your business across the pond.

Canada
The logical next step for any ecommerce business merchant interested in growing its footprints in North America.

Part 2

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

One of the biggest ways ecommerce fraud hits small businesses hard is through chargebacks. Let's do a deeper dive into chargebacks, how they happen and what you can do to protect your business.

Part 3

Understanding Chargebacks

Ready to Get Started?

Call us at +1 786 888 4584 or email contact@clear.sale
to speak with a fraud expert today!

www.clear.sale

Part 3

Understanding Chargebacks

In addition to being aware of CNP fraud and friendly fraud, small businesses need to be aware of chargebacks themselves and how they work.

The Chargeback Process

As we touched on earlier, a chargeback happens when a customer files a dispute with their credit card issuer over a charge on their account.

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

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

Chargebacks can be devastating for businesses, especially small businesses. Not only do you often lose the value of a product plus shipping expenses, but chargeback fees can reach $100 or more per transaction.

And if a card issuer decides you incur too many chargebacks, they may raise your fees or remove your ability to accept credit cards entirely.

That can be the beginning of the end for a small business.

Part 3

Types of Chargebacks

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

Legitimate chargebacks

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

Friendly fraud chargebacks

As we mentioned earlier, friendly fraud is a gray area, where the reason for the chargeback isn't legitimate, but it's also not malicious. For example, the customer simply may not recognize a particular charge or business's name on their credit card statement.

Chargeback fraud

You've already learned that chargeback fraud happens when a customer files a chargeback with the express intent to defraud. For example, a fraudster may claim that an item was never received, when in fact it was. Or the customer 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.

Part 3

It takes a long time to process and adjudicate chargebacks. For small businesses, it is tedious and frustrating because the onus is on them to prove that the chargeback is invalid. To **win a chargeback dispute**, businesses need to produce meticulous records and have patience throughout the back-and-forth with the customer and credit card issuer.

Chargeback Fees and Chargeback Ratios

Not only do chargebacks cost time and effort, they can put a **significant dent** in a company's bottom line. In addition to lost inventory and shipping costs, chargebacks involve fees and other penalties. The fees vary by payment processor, but they can range from $50 to over $75 per dispute. Multiple chargeback fees can be the death knell for a small business.

In addition to chargeback fees, a bigger problem to worry about is your chargeback ratio.

Your chargeback ratio reflects the percentage of chargebacks relative to overall transactions. The industry standard has been 1% for years, but some payment processors have lowered that threshold, especially for high-risk businesses.

Once your chargeback ratio crosses that threshold, the fees increase and **the payment processor may freeze (or even terminate)** the company's account.

But that's not all.

Once a company's account is closed with one payment processor, word travels fast. You may have trouble opening an account with any of the other processors. That's when businesses are forced to accept sky-high processing rates to reopen their account ... if they can get approved for payment processing at all.

The best way to handle chargebacks is to prevent them as much as possible.

Part 3

Chargeback Solutions

Preventing excessive chargebacks from harming your business involves one of two solutions: chargeback protection or chargeback insurance. But **what is the difference** between these two options?

1. Chargeback Protection:
This solution offers tools to monitor transactions and identify/prevent fraud. It may also cover a portion of the potential losses related to chargebacks.

2. Chargeback Insurance:
This solution guarantees coverage if the fraud solution partner approves a transaction that turns out to be fraudulent and results in a chargeback.

These two solutions are markedly different, so it's critical to choose the approach that's best for your business. Not all vendors offer both options, which makes it even more important to carefully select your fraud prevention solution provider.

We'll help you navigate that important decision in Chapter 5. Before we do though, it's important to understand why relying solely on fraud filters can backfire ... and get you into trouble with your customers.

Part 4

Understanding False Declines

Ready to Get Started?

Call us at +1 786 888 4584 or email contact@clear.sale
to speak with a fraud expert today!

www.clear.sale

Part 4

Understanding False Declines

We've already provided a clear picture of what can happen if you rely on luck, hoping fraudsters will pass over your online business. (Spoiler: They won't.)

On the opposite end of the spectrum, you don't want to wantonly block every transaction that gives even a hint of being fraudulent. That's where you risk damaging your reputation with too many false declines.

The Dangers of False Declines

False declines happen when a legitimate transaction is mistaken for fraud and denied. About 90% of declined transactions are actually valid customers just trying to give you their money.

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 traveling 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 business 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 in the hundreds of billions. In addition, false declines can have a nasty ripple effect: If you recall, we stated earlier that your cost per $1 of fraud is just under $4.

Part 4

Your **cost per $1 in false declines is a whopping $13.**

That's because when you falsely decline a customer, you're likely saying goodbye to that customer forever: In our **2021 Consumer Attitudes study**, we learned consumers are not forgiving when it comes to being denied what they want to purchase.

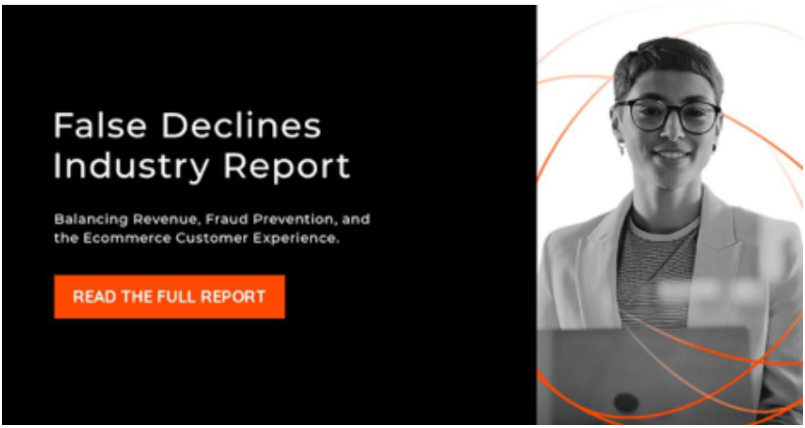
When asked if they would return to the same company after being declined, 40% of respondents said they would not.

If you sell low-volume, high-dollar offerings, that spells trouble.

It gets worse: **34% of respondents** reported that not only would they never shop with the company again, **they would take to social media to share their displeasure.**

When it comes to false declines, millennials are the least forgiving age group, with 56% saying they would never place another order with the business again and a whopping 64% saying they would complain on social media.

Given how much millennials dominate social media consumption, small businesses simply cannot afford to let their false declines get out of control.



Part 4

Small businesses in Latin America should be very wary of false declines

If you have a small business or are considering starting a small ecommerce business in places like Argentina, Chile, Peru, Ecuador or any other Latin American country, false declines are most likely going to be your biggest obstacle. Solve that problem and you'll be head and shoulders above your competitors when it comes to revenue and the all-important customer experience!

False Declines' Ugly Stepsister: The Deny List

Some companies try to circumvent chargebacks and false declines by trying to identify "repeat offenders" or extreme fraudsters and place them on what's called a **fraud prevention deny list**.

A deny list is essentially a database with credit card numbers, names, addresses, emails, phone numbers and IP addresses for the fraud filters to use to automatically decline transactions.

Here's why these types of lists are a bad idea: If the customer's credit card was stolen, the customer's name could end up on a deny list, even though the customer is actually the victim. Another problem with lists is that IP addresses are constantly exchanged. A valid customer could end up on a list completely in error.

Like we said, many small ecommerce businesses feel stuck: Either they risk losses to fraudsters, spend all day verifying transactions, or risk turning away much-needed business because of a ham-handed deny list.

As it turns out, though, there are more fraud prevention options than most small businesses realize. The key is to find the one that works with your business … and your customers.

Part 5

Comparing Fraud Prevention Options

Ready to Get Started?

Call us at +1 786 888 4584 or email contact@clear.sale
to speak with a fraud expert today!

www.clear.sale

Part 5

Comparing Fraud Prevention Options

There are a wide range of options out there to help you protect your small ecommerce business from the types of fraud we've discussed in this guide.

The question is, what will be the best option for your business? Let's examine each in detail.

Fraud Filters

When we talk to small businesses about fraud prevention, the most common response we hear is that they already have fraud filters in place.

How fraud filters work

Fraud filters are usually built into your ecommerce platform. They're designed to identify potentially fraudulent orders and prevent them from being processed, and they function differently, depending on 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 all of them by flooding your site with orders.

Address verification service (AVS) is a filter that declines or flags transactions when the billing and shipping addresses don't match. These are intended to keep credit card thieves from having merchandise delivered to another address.

Part 5

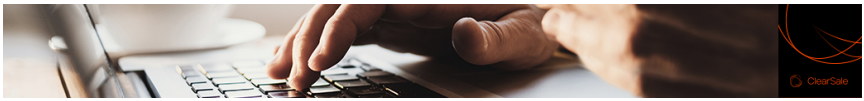
Time-of-purchase filters are used to flag or block transactions during a specific timeframe — usually when fraudulent transactions are more likely to occur, such as holidays and special sales.

Card verification value (CVV) filters look for errors in the CVV number being submitted.

Purchase amount filters flag high-dollar transactions that fall outside a typical transaction amount.

IP address mismatches can flag transactions where the customer's IP address and shipping address don't match, a potential fraud indicator.

Fraud filters are commonly included in **ecommerce platforms (the ecommerce platforms for small- and medium-sized** businesses that integrate with ClearSale all offer fraud filters).



Fraud filters do have a downside

While fraud filters have value and can provide insight into what is happening on your ecommerce site, they can also **create more problems than they solve.**

Some businesses try to solve any issues with fraud by layering multiple levels of fraud filters. But without intimate knowledge of fraud trends, cues and other factors, those businesses end up with filters that either negate each other or completely block all sales.

For example, your best customer might be on vacation when she remembers that her friend's birthday is coming up, so she places an order from her phone while in her hotel room. A fraud filter might identify that the geographic location of the device is different from the credit card account address and therefore decline that transaction — even though it is in fact legitimate.

Part 5

The bottom line: Fraud filters are an important part of a fraud solution.

While fraud filters do put ecommerce businesses at risk of increasing false declines and lowering your approval rate, they are very effective for identifying which transactions should be flagged for further analysis and manual review.

Pros:

- **Inexpensive:** Fraud filters come standard on most ecommerce platforms.
- **Easy to set up:** Ecommerce platforms like Shift4Shop, Shopify, PrestaShop and OpenCart are incredibly easy to set up.
- **No integration required**

Cons:

- **High risk of false declines:** Fraud filters don't have the artificial intelligence to "learn" behavior, so a transaction that looks fraudulent is assumed to be fraudulent, whether it is or is not.
- **No option for secondary review:** If a valid transaction is declined, businesses will likely anger the customer, lose the sale and risk a bad review on social media.
- **Few options for customizing:** Ecommerce businesses would need to have their developers or a consultant customize standard filters.
- **Potentially lower approval rate:** The order in which fraud filter rules are applied can result in some rules contradicting others, which can reduce the number of approved transactions.

Related Reading:

Selecting the right combination of fraud filters can be overwhelming. Learn more about each type of filter and how filters fit into your larger fraud prevention program: The Beginner's Guide to Fraud Filters

READ MORE

ClearSale

Part 5

Secondary Fraud Review

Secondary fraud review involves a team of individuals manually 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 an external third party, where the **business sends orders that seem "iffy" to a fraud protection vendor** to analyze.

Secondary review is better than just fraud filters

Expertly trained humans are generally better at understanding context than automated fraud filters. These fraud experts can look at each situation individually to assess the fraud risk, 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.

Secondary review takes time

On the other hand, secondary review is very time- and resource-intensive. Even the best human reviewer can't work as quickly as a computer program, so customers may have to wait slightly longer to be approved for their orders. (However, most small businesses who've worked with a fraud prevention solution will say the **secondary review is worth the wait.)**

Also, the effectiveness of a manual review is only as good as the expertise of the employees performing the review.

Part 5

If you want to keep your review team in-house, you'll need to hire experienced staff or pay to train them. This can be a solid approach if your volume and business are stable, but a sudden (or seasonal) increase in business could add strain. In those cases, **outsourcing secondary fraud review** can provide better flexibility.

The bottom line: Secondary review by analysts is essential to decisions about potentially fraudulent transactions.

Secondary review on its own can be costly — and not as fast as filters — but is an ideal way to evaluate potentially fraudulent transactions instead of simply declining them.

Pros:

- **Thorough fraud review:** Every transaction is carefully examined.
- **High level of accuracy:** Reviewers can be trained to apply new knowledge about fraud trends to their decision-making process.

Cons:

- **Not scalable for sudden changes in transaction volumes:** Sudden spikes in sales volume will slow down the review process and could result in customer service issues if the reviews take too long.
- **Not cost-effective:** Small businesses have to incur the expense of recruiting, hiring and training enough staff to handle the maximum volume of transactions.
- **Potential loss of institutional knowledge:** If staff members leave, their expertise and knowledge leave with them.

Related Reading:
Guidance for In-House Fraud Management Teams
READ MORE

Part 5

Outsourced Automated Solutions

Outsourced automated solutions allow small ecommerce businesses to offload all of their fraud protection onto a third party. Transactions are processed through automated systems and are approved or declined based on preset parameters and filters.

This type of machine learning and AI are fast and reliable because they use mathematical algorithms and data to identify fraud trends and patterns. And because no humans are involved in this form of fraud detection, machine learning is scalable and consistent. Every transaction receives the same level of scrutiny.

But, if you recall from Chapter 4 where we discussed false declines, making decisions about transactions purely because they **appear** to be fraudulent increases the risk of declining legitimate transactions. And that can have a serious negative impact on customer experience.

Without human intuition, analysis or interaction, you can't contact a longtime client to get more information about a suspicious purchase. The last thing you want to do is have an algorithm drive away your best customers.

The bottom line: Outsourced automation is a great part of the solution.

Outsourced automated fraud protection using machine language and AI can detect most fraudulent transactions and identify transactions that require further review.

Pros:

- **Fast processing time:** Automated rules allow for immediate decision-making and transaction disposition.
- **Hands-off fraud protection:** With their fraud protection handled by a third party, ecommerce businesses don't have to understand the nuances of fraud and fraud risk.
- **Better fraud identification:** With more sophisticated options that offer machine learning and AI, outsourced automated solutions "learn" buying patterns.

Part 5

Cons:

- **Limited variability:** Outsourced automated solutions can't account for variations in consumer behavior, such as vacation purchases.
- **High risk of false declines:** Automated solutions treat potential fraud like actual fraud.
- **Slow adoption of new fraud trends:** Automated solutions require programming with new data, which can take time to integrate into its intelligence.

Related Reading:
Should My Fraud Management Solution Screen Every Online Transaction?
READ MORE

Fraud Managed Services

Fraud managed services incorporate a two-pronged approach: **Prevent fraud** from happening … and **protect the small business** if a fraudulent transaction does slip through.

A 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 internal fraud team or to augment an in-house team, especially during times of increased sales volumes or periods of rapid growth.

Here's how it works:

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, even if the order looks like it might be fraudulent, the order is not automatically declined.

Instead, **any order that fails to pass the initial screening is sent to a secondary review team for analysis.** There, a team of expert analysts reviews the order to see if data is missing, compares the order to that cardholder's typical ordering or store behavior, and contacts the customer for further authentication if needed.

Part 5

Why a fraud managed services approach works.

- Because no transaction is automatically declined, you have fewer false declines.
- Expert fraud analysts can quickly spot new **fraud trends and flag them for insertion into the AI's algorithms.**
- The analysts **can work alongside** a company's in-house team, or in consultation with the client, bringing specific business/industry insight to their fraud screening.
- The solution **easily scales** to accommodate peak sales times, while still ensuring each flagged transaction is reviewed by a human analyst.

The bottom line: A fraud managed solution offers the best of all worlds.

By combining all the options available for fraud protection, a fraud managed solution offers ecommerce businesses a reasonably priced way to protect themselves from fraud without risking turning away good customers. Plus, you'll still have control over the process without having to manage every aspect of the process.

Pros:

- **Fewer false declines and higher approval rates:** The combination of AI and manual review distinguishes between clearly fraudulent and potentially fraudulent transactions
- **Fewer chargebacks:** AI "learns" customer behavior and takes into account fraud trends to quickly spot fraud patterns.
- **Fast processing:** Approved transactions are automatically processed, which adds to the customer experience.
- **Full transparency:** Data analysis provides the company with information about why a transaction was flagged.

Part 5

- **Peace of mind:** Ecommerce businesses don't need to be fraud analysts, and if available, they can provide the vendor with historical customer and transactional data that helps improve the accuracy of the solution.

Cons:

- **Longer process for declining transactions:** Reviewing suspicious transactions will take more time to determine if those transactions are fraudulent. So if a good customer's transaction is flagged, they may need to wait a little longer before shipping — and may be asked to provide some verification information.

- **More costly than ecommerce platform fraud filters:** The cost of a hybrid solution is higher than simply relying on your ecommerce platform fraud filters. However, when you consider the cost of losing customers and negative reviews, the cost difference may easily be justified.

If you've settled on what type of fraud protection you want, great! But now comes the tricky part — making a decision. There are a lot of fraud prevention solutions out there. What questions should you ask to find the perfect match for your business?

Part 6

Important Factors to Consider

Ready to Get Started?

Call us at +1 786 888 4584 or email contact@clear.sale
to speak with a fraud expert today!

www.clear.sale

Part 6

Important Factors to Consider

When selecting the best fraud solution, many factors come into play. We've compiled the questions you should ask to make sure you get the right fit.

How Well Does the Solution Balance CX, UX & Fraud Protection?

Customers can shop anywhere, and they know it. So, the customer experience (CX) and user experience (UX) of your ecommerce store are incredibly important.

Your fraud protection solution should make it easier for customers to purchase from you — that means speedy approvals where possible and few to no false declines.

When considering a solution, here are questions to ask about CX and UX:

- Does the solution require updates to your website?
- How do those updates impact the customer experience?
- Does the solution approve/decline orders on its own or send them to you for the final decision?
- Will you be kept informed about declined orders and why they were declined?
- What skills or training will you need to have in-house for this solution to work?

Part 6

How Easy Is the Integration Process?

The best fraud protection solution will work seamlessly with your existing ecommerce platform and integrate with limited steps. At ClearSale, most of our integrations are plug-ins; several of our ecommerce platform integrations can be completed in three steps.

When considering a solution, here are questions to ask about integration:

- How long does the implementation process take?
- What level of expertise do we need to have in-house to get this solution integrated?
- What technical support is available to us if things go wrong?

Keep Geography in Mind When Looking at Integrations

When it comes to chargebacks — or any kind of fraud — it's important to remember not all countries operate in the same way. The banking systems in some countries, such as many LATAM countries, operate with fewer checks and balances.

As you're narrowing down your fraud protection options, ask whether those providers integrate with solutions that are tailored toward the market (or markets) in which you'll be operating.

For example, ClearSale partnered with ecommerce company VTEX to offer a two-step authentication process that mimics the type of authentication you find in the United States and other countries. As a result, ecommerce businesses in LATAM countries can significantly reduce their fraud risk.

Part 6

How Accurately Does the Solution Detect Fraud?

If your fraud protection solution is too rigid, you run the risk of declining valid transactions.

PRO TIP: Ask vendors what mechanisms they use to ensure accuracy and reduce the risk of false declines.

When considering the accuracy of a solution, ask these questions:

1. How are the models trained for accuracy?
2. How quickly is information about new fraud trends integrated into their processes?
3. How do they reduce the risk of false declines?
4. What is the typical approval rate among its customers?

For every $1 in losses due to credit card fraud, businesses lose $13 to false declines.

And 40% of U.S. customers will refuse to shop with a company after a false decline.

Does the Solution Protect You From Chargebacks?

You now know how important it is to avoid chargebacks: They are the single biggest threat to your small ecommerce business. Too many chargebacks will put your business in jeopardy of paying high penalties, which can drain your profits quickly.

Many fraud solutions address only CNP fraud and don't have the capability or expertise to prevent ATO, chargeback and friendly fraud. All these types of fraud can lead your business down the path to high chargeback rates. And what about chargeback protection, chargeback insurance and chargeback alerts?

Part 6

When considering how a solution addresses chargebacks, ask these questions:

- How does this solution protect you from chargebacks?
- How much in-house work do you need to do to manage chargebacks?
- Does this solution handle chargeback disputes on your behalf?
- Does the solution offer chargeback protection or a guarantee? How does it work?
- What types of fraud does the solution detect?
- How is questionable fraud handled?
- Does the solution also assist with investigation of/response to chargebacks?

Is Your Business and Customer Data Safe?

When considering data safety, ask these questions:

- Are they PCI-DSS compliant?
- Do they have external penetration tests done? How often?
- How is their solution/application hosted? Local? Remotely? The cloud?

Reminder: By making sure your customers' data is protected, you'll be protecting yourself and other businesses from the increase in CNP fraud that tends to follow data breaches.

Part 6

What Fraud Solution Costs Are Involved?

A fraud solution needs to give you the best return on investment. Some "bargain" solutions may offer none of the features you truly need, making them no bargain at all.

At the same time, other solutions offer more bells and whistles than you'll ever use ... and will charge you a small fortune for them.

When considering costs, ask these questions:

- Do they charge monthly management/support fees?
- What is the estimated cost per transaction? How will this change as you grow?
- What are the contract terms, and are there any fees outside of the contract?

You *Can* Prevent Ecommerce Fraud & Grow Your Business

As a small ecommerce business, you can't ignore fraud. It's an exponentially growing concern. And the stakes are high:

- Too much fraud will trigger chargebacks that siphon away your profits.
- Too many chargebacks will make payment processors question your business relationship and charge higher fees.
- Too-strict fraud rules will decline valid transactions and turn away loyal customers.

You have a lot to consider when choosing a fraud protection solution, and it has to work with your business to keep you on the path of success.

Now that you're much more informed about ecommerce fraud, you can be more confident making a choice that will protect your business from fraud, save you time and money and keep your customers happy — so they'll come back to you again and again.

Part 7

Ecommerce Fraud FAQs

Ready to Get Started?

Call us at +1 786 888 4584 or email contact@clear.sale
to speak with a fraud expert today!

www.clear.sale

Part 7

Ecommerce 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.

Part 7

What should merchants know about preventing fraud for online sales?

The **key to your success**? Minimizing financial losses due to fraud while boosting your ability to approve the largest number of orders in as short a time as possible.

So, a good anti-fraud service should include a risk management system that ensures high rates of approved sales while minimizing chargebacks, in as short a response time as possible.

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.

More questions? Check out our comprehensive **Knowledge Base** with answers to the most frequently asked questions about fraud definitions and terms and fraud prevention topics.

Part 7

We did say that reviews and consumer feedback matters. Here's how we've helped our clients succeed in fighting fraud and increasing revenue.

Ready to Get Started?

Let's Talk!

Find out how to prevent chargebacks and sell more.
Talk with a ClearSale CNP fraud expert today!

GET STARTED NOW