CHARGEBACK GURUS

AN INTRODUCTORY GUIDE TO ECOMMERCE FRAUD AND PREVENTION

www.chargebackgurus.com

TABLE OF CONTENTS

AN INTRODUCTORY GUIDE TO ECOMMERCE FRAUD AND PREVENTION

Challenges in Today's Payments Environment

Fraud continues to be a significant and growing problem for merchants, especially in e-commerce. Payment fraud has escalated dramatically in recent years, and global annual losses are expected to reach $91 billion by 2028.

Worse yet, merchants can be hurt by their own fraud prevention efforts. Aite-Novartica estimates that the cost of false declines comes to $443 billion each year, several times the cost of payment fraud. Over 15% of consumers report experiencing false declines on attempts to make legitimate purchases.

The anonymity of e-commerce makes online fraud a low risk, high reward prospect for thieves, and improvements in card security for in-person transactions have had the effect of shifting fraud losses away from physical retail stores and into the card-not- present environment of e-commerce.

Where fraud goes, chargebacks follow, and it is vitally important for merchants to minimize the number of chargebacks that get filed against them. Aside from the huge revenue losses caused by transaction reversals, chargeback fees, and the resources spent on dealing with chargebacks, card networks impose limits on chargeback ratios that merchants can’t exceed without incurring penalties.

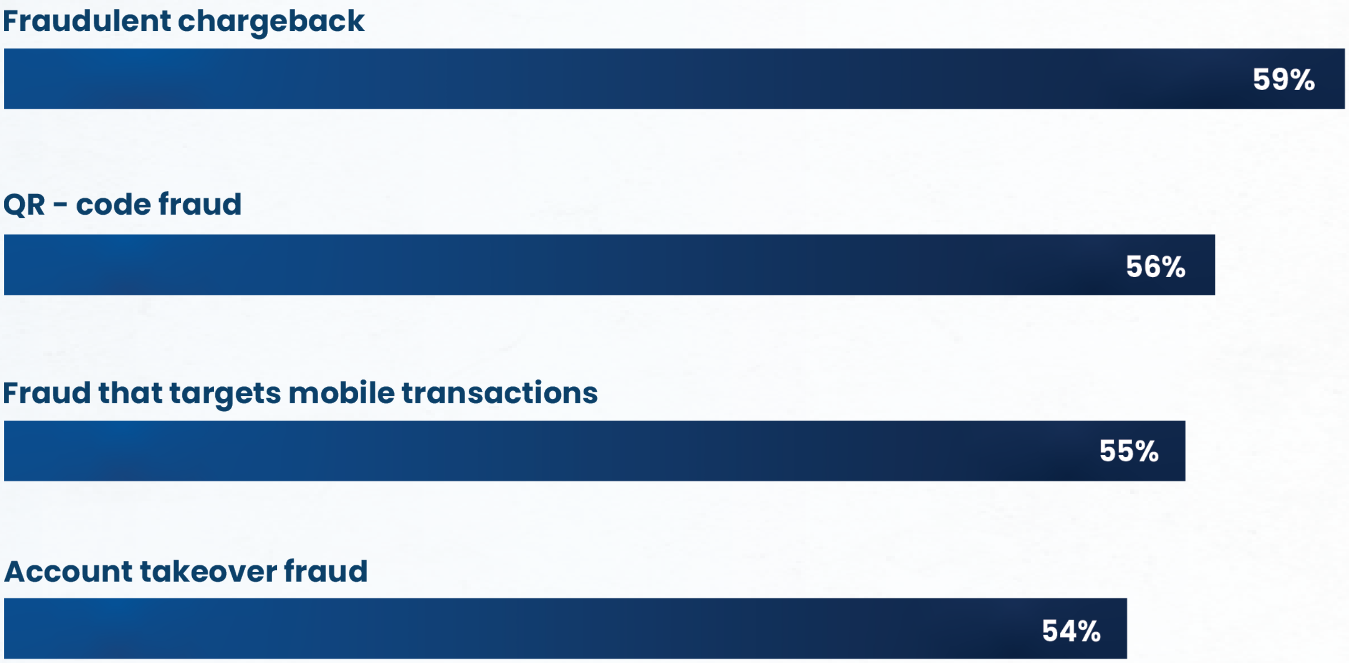
Prevention is crucial, but prevention can be costly. Merchants are stuck in a bind where they must make every effort to detect and avoid fraud and chargebacks, while being careful not to overzealously decline legitimate transactions or allow the costs of fraud prevention to harm their profitability.

The exponential growth of e-commerce, set to reach $7.9 trillion by 2027, underscores the need for robust fraud prevention strategies. As business accelerates, so does the risk, with fraud losses potentially rising by 16% annually. Proactive measures are essential to mitigate losses amidst this rapid expansion.

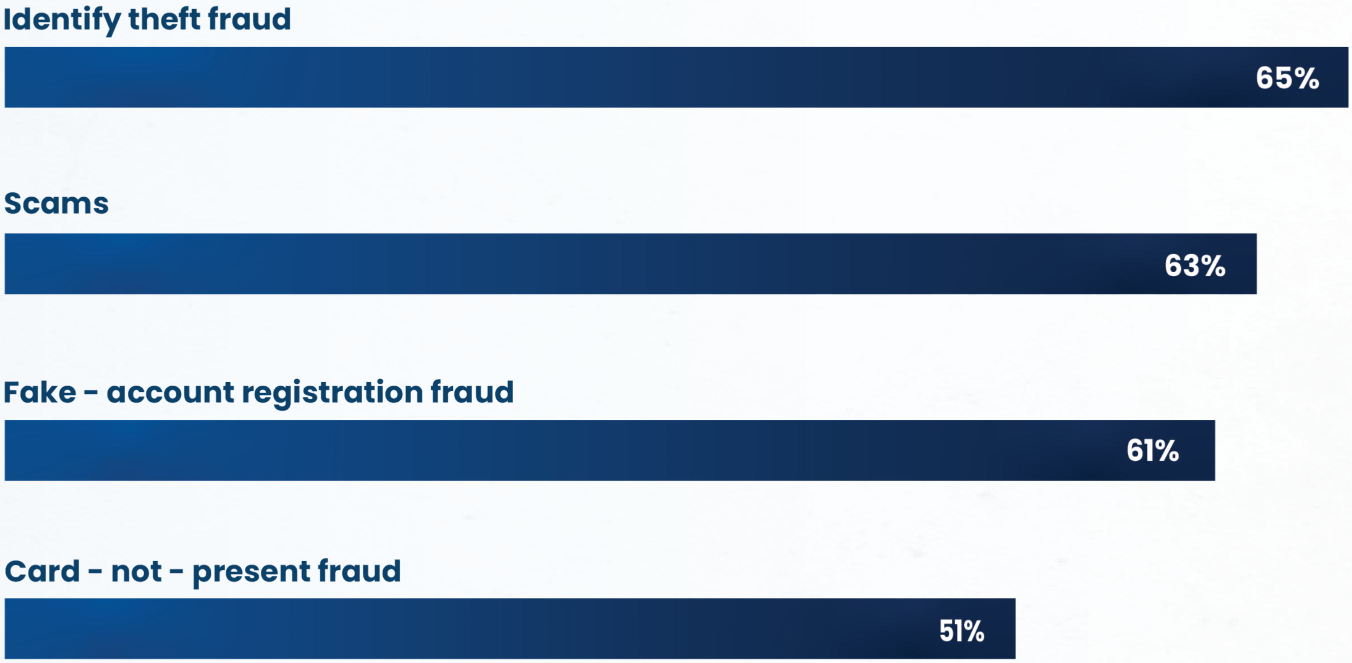
The latest findings from the LexisNexis “True Cost of Fraud” study reveal asignificant surge in both the frequency and complexity of fraudulent activities. Most merchants reported an increase in overall fraud levels in 2023 as well as increases in a variety of specific types of fraud.

Fastest Growing Fraud Types in Last 12 Months

RETAIL



ECOMMERCE



AN INTRODUCTORY GUIDE TO ECOMMERCE FRAUD AND PREVENTION

Common Types of Fraud

Fraudsters are creative. There are a variety of different ways to perpetrate fraud, and new schemes and techniques seem to crop up every day. Nevertheless, most fraud will fit into one of five different categories:

Payment Card Fraud

This is the relatively straightforward form of fraud most of us associate with the term, where a third party uses stolen payment credentials to make a purchase. The implementation of EMV technology made this type of fraud more difficult in card-present environments, but preventing credit card fraud online is still a challenge.

Friendly Fraud

So-called "friendly" fraud, also referred to as first-party misuse, occurs when a customer disputes a legitimate transaction, resulting in a chargeback for the merchant. This type of fraud can be committed unknowingly by a misguided customer or maliciously by a bad actor intent on defrauding the merchant.

Account Takeover

Account takeover occurs when a fraudster gains access to someone else's account and uses it to make purchases with saved payment credentials, transfer stored funds, etc. Fraudsters can gain access to both customer and employee accounts through a variety of means, including phishing, data breaches, identity theft, and more.

Return Fraud/Policy Abuse

There are a variety of ways for fraudsters to abuse a merchants return and refund policies for financial gain, such as false claims of non-delivery, returning a counterfeit or lower-value product instead of the one originally purchased, or returning items that were purchased fraudulently.

Card Testing

A sub-type of payment card fraud, card testing occurs when a fraudster attempts to make small purchases with stolen payment credentials to test whether they are still valid. Card testing can scale up in a big way, with organized criminals using bot networks to test thousands of stolen cards at once.

AN INTRODUCTORY GUIDE TO ECOMMERCE FRAUD AND PREVENTION

Effective Prevention Tools & Strategies

Different types of fraud require different strategies and tools to combat them effectively. As such, mitigating overall fraud risk requires a multi-layered strategy that encompasses every stage of the pre- and post- transaction process.

Coming up with an effective fraud prevention plan requires you to understand what types of fraud are occurring most often, what your biggest vulnerabilities are, and how the prevention methods you're considering will affect the overall financial health of your business.

In this section, we'll talk about in-house strategies, external tools, and ways to measure fraud prevention effectiveness for each of the major types of online fraud.

Payment Card Fraud

In-House Strategies

1. Activate AVS and CVV matching features in your payment gateway. Most low-effort methods of credit card theft won't include both of these pieces of information. This is one of the easiest ways to screen out charges from stolen cards, and every payment processor should offer these options.

2. Review orders that request rush or overnight shipping manually before fulfilling them or assign them a higher risk score in automated tools, especially if they have different billing and shipping addresses. Fraudsters often ask for expedited shipping to ensure the purchase is shipped before the cardholder notices the charge.

3. Trace IP addresses to identify the geographical origin of suspicious transactions. Some countries have higher rates of fraud than others, and any time you get an order from a country you don't normally do business in, that should be a warning sign.

4. Use velocity checking to identify suspicious patterns of behavior, such as multiple transactions with the same shipping address, IP, or device fingerprint in a short period of time.

5. Use an order management system compliant with the Payment Card Industry Data Security Standard to store order information. This standard was established by the major card brands to reduce credit card fraud by mandating extra layers of protection for cardholder data.

External Tools

1. Artificial intelligence and rule-based fraud detection software.
2. 3-D Secure 2.0.
3. AVS & CVV matching.
4. EMV Chips.
5. Device fingerprinting.

Measuring Effectiveness

The major concerns for merchants when using fraud prevention tools are:

1. An increase in false positives that causes your order rate to decline.

2. The time and resources required to learn how to use the tools and manage them properly.

3. Increasing fraud management costs that yield a negative return on investment.

Here are some solutions that address those concerns:

1. Specify benchmarks for the following before implementing fraud prevention tools:
   a. True fraud chargeback rate
   b. False positive rate

2. Incorporate one tool at a time and compare the results against the benchmark for at least 60 to 90 days to determine the true ROI.

3. If the ROI is positive, incorporate the next tool and repeat the steps above.

4. If the ROI is negative, talk to the company providing or servicing the tool and adjust the settings to see if you can get a positive ROI.

5. If you can't get positive results with a tool after making adjustments, discontinue using it and move on to testing out the effectiveness of the next tool.

Friendly Fraud

In-House Strategies

1. Make sure your merchant descriptors are easy for customers to recognize. Many chargebacks occur because customers don't recognize the charge on their bank statement. To minimize this, include a business name customers will recognize in the descriptor so that customers can easily identify the origin of the charge. Additionally, consider adding a support phone number to the descriptor, or make the descriptor dynamic and include relevant details such as the product name. This approach can help reduce confusion and further prevent chargebacks.

2. Set realistic expectations about your products and/or services. A customer who feels misled or deceived by your marketing materials may not trust you enough to go back to your company to resolve whatever issue they're having. Don't make promises you can't keep.

3. Maintain honest and ethical business practices. Fraud goes both ways—you can't expect your customers to behave ethically toward you if you're trying to take advantage of them.

4. Provide helpful, easily accessible customer service. A customer who can't reach you when they're having a problem is likely to lose patience and call up their bank's customer service line instead. If your customer service staff is easy to reach and trained to provide comprehensive assistance, customer complaints are less likely to turn into chargebacks.

5. Blacklist customers who file chargebacks. We estimate that customers who file chargebacks will do so at least two or three times against the same merchant if no preventative actions are taken. Blacklisting these customers will prohibit them from taking advantage of you more than once, but you have to weigh the cost of losing potential future sales against the likelihood of getting more chargebacks from them.

6. Fulfill orders on time and track return shipments. Delays can happen, but customers who give up on ever receiving their order have a high likelihood of requesting a chargeback. Ship promptly, track all outgoing and incoming packages, notify your customers about any unforeseen delays, and issue refunds immediately when a return shipment arrives.

7. Notify customers when you process their order. For recurring payments, send a notification before and after you process them. Any time there's a delay between an order being placed and a card being charged, it's a good idea to remind the customer what they're being charged for.

8. Have a rigorous, reliable process for identifying and fixing merchant errors. More than a quarter of all chargebacks happen because of merchant error—duplicate order entry, shipping to the wrong address, incorrect refunds, etc. If your internal processes are designed to fix these errors on the fly, you can eliminate these costly chargebacks.

External Tools

1. Reporting tools that can analyze and identify the root causes of your chargebacks.
2. Third-party chargeback management companies.
3. Order management software that can flag and block problematic customers.
4. Visa's Order Insight or Ethoca's Consumer Clarity.
5. Chargeback alert services.

Measuring Effectiveness

The major concerns merchants have about third-party analytical tools or chargeback management companies are:

1. The time and resources needed to learn how to use the tools effectively and do any custom programming necessary to facilitate the identification of chargeback root causes.

2. The licensing costs of third-party tools and the costs involved in customizing them to get the desired analytics.

3. The costs of hiring third-party chargeback management companies to identify root causes and handle chargeback disputes on the merchant's behalf.

4. The risks of exposing customer data to third parties.

Here are some possible solutions:

1. Before deciding on an analytical tool, prepare the list of reports you'll need to identify the root causes of your chargebacks, and discuss the scope of this analysis with the tool provider. Identify the cost of custom report programming and any maintenance costs and compare the total cost of the tool with your current chargeback revenue losses.

2. Hiring a chargeback management company might be expensive when compared to handling chargebacks yourself, but working with a skilled and specialized team can get you the proper analytics, ensure you're in compliance with the ever-changing payment and chargeback regulations, increase your win rate in chargeback disputes, and help you reduce the overall number of chargebacks you get. This can mean an overall higher ROI than lower-cost solutions.

You can measure the effectiveness of a chargeback management company in the following ways:

a. The amount of revenue they recover by fighting your chargebacks.

b. The time they save you by managing chargebacks.

c. Whether the analytics they provide help you identify your vulnerabilities and reduce your overall chargeback rate.

d. Experienced chargeback management companies will provide you with a profitability and service effectiveness review every three to six months—you shouldn't need to specifically request these reviews.

Account Takeover
In-House Strategies

1. Use strong password requirements for your database and CRM system. Many employees wrongly assume that their internal computer systems are reasonably safe from hackers and choose easy-to- remember passwords. Don't give them that option.

2. Make your customers create complex passwords with a long minimum length. If you require them to answer security questions for a password reset, make sure those questions don't ask for information that criminals could gain access to via social media.

3. Prohibit your employees from using open Wi-Fi networks to log into admin accounts. When you use somebody else's Wi-Fi, you have no idea how secure it is, and there are tools that can sniff out and record all the data that passes through an unsecured Wi-Fi network.

4. Require two-factor authentication for customer accounts with stored payment credentials. This can help prevent unauthorized purchases even when a customer uses an insecure password or re-uses one that's been compromised. While two-factor authentication was once seen by consumers as an annoying hassle, it has now become common enough that most customers won't balk at being asked to authenticate themselves when logging in from an unrecognized device.

5. Limit repeated login attempts. Brute force attacks still happen, and limiting the number of unsuccessful login attempts is an easy way to prevent them that will rarely affect ordinary customers.

6. Encrypt customer account login credentials at the database level. Bad database security procedures could mean that a hacker could gain access to every single one of your customers' passwords if they obtain a copy of your database file. Proper encryption and decryption procedures can eliminate this possibility.

7. When using a third-party CRM system, make sure it's PCI-compliant and that you regularly update it with the latest security patches. The PCI standards are fairly extensive and should give you some peace of mind that your customers' data is protected However, security features are only as good as their latest patch, and hackers are always finding new exploits and looking for out-of-date systems to try them on.

8. Use Google Alerts to find out if any other companies or individuals are trying to use your business name on the internet. Lots of phishing is done the old-fashioned way by pretending to be someone you're not. Be vigilant about protecting your name and reputation online.

9. Protect your systems by regularly installing the latest security patches for any devices you and your team use— desktop computers, notebooks, tablets, phones, and anything else network- connected. New bugs and hacks are discovered every day, and leaving your systems unpatched is like rolling out a big welcome mat for online thieves.

External Tools

1. Bots that perform vulnerability assessment tests on cloud-stored data.
2. Tools like PasswordPing that identify compromised credentials (MFA).
3. Automated account takeover prevention tools.
4. Transaction Monitoring Systems.

Measuring Effectiveness

Account takeover fraud generally targets medium-sized or larger e-commerce businesses. For cyber criminals, the payoff is better from businesses at this scale. Smaller merchants will often see more cost-effective benefits from implementing in-house strategies, as the cost of using external tools may exceed the ROI. No tool can provide complete, failure-proof protection against this type of fraud, but the vast majority of hackers and phishers will focus their efforts on soft targets that have minimal or non-existent security measures in place, rather than expending time and energy trying to find a weak spot in a well-protected website.

Return Fraud/ Policy Abuse

In-House Strategies

1. Get a tracking number for every order you ship. The most common reason customers request refunds is for products that were never delivered. Shipping physical goods with a tracking number can greatly reduce refund fraud.

2. Make sure the specifics of your refund policy and terms are clearly communicated to your customers before they make a purchase. “Hassle-free” refunds can help you drum up business, but they can also attract customers who intend to take advantage of it.

3. Track how many refunds a customer requests, and their reasons for requesting them. Analytics can help you identify the internal issues that are causing your refund rates to spike and can also help you identify customers who are abusing your refund policy.

4. Create a process and policy document for your customer service team. Refund abuse often happens when merchants use third-party call centers to handle customer service requests. Provide your team with clear directions on the qualifying criteria for returns and refunds.

5. Prevent double refund fraud by creating a database for chargeback abusers. Fraudsters can sometimes score a double refund by requesting a refund from the merchant at the same time they’re asking their bank for a chargeback. Merchants who aren’t experienced with fighting chargebacks will often end up losing the revenue twice. Blacklisting these customers can help your customer service team avoid issuing refunds to known chargeback abusers.

External Tools

Your best weapon against return fraud is a CRM system with PCI compliance that can blacklist chargeback abusers, block future transactions from blacklisted customers, and manage tracking and record keeping for returns and refunds.

Measuring Effectiveness

You can gauge the effectiveness of your in-house strategies and third-party tools by comparing their results with the following benchmark attributes:

1. Overall order refund rate.
2. Product return rate by item.
3. Chargeback rate for orders that have been refunded.
4. Order refund rate by cause (product quality, fulfillment, customer service, marketing).
5. Order return rate by season (holiday season rate vs the rest of the year's rate).

Card Testing

In-House Strategies

1. Activate AVS and CVV matching features in your payment gateway. The resulting error messages will dissuade fraudsters from making further purchase attempts at your online store.

2. Use velocity checking tools. Fraudsters often try to place multiple small orders within a short span of time in order to test different card numbers they've stolen. Velocity checking can be used to set alerts for sudden spikes in small orders or block repeated orders with matching information such as IP address or device fingerprint.

3. Watch out for incoming orders from foreign IP addresses. Most card testing fraud originates from outside the United States, so if doing business internationally isn't important for your overall sales, consider automatically declining all orders that come from foreign IP addresses.

4. Be extra vigilant during the holiday season. Fraudsters know that during this time, merchants are busy and multiple orders from a single customer aren't uncommon. Since merchants have less time during the holidays to scrutinize suspicious orders, this is the best time for criminals to test out stolen credit cards.

5. Blacklist accounts or IPs you suspect of attempting card testing schemes so that they can't place orders with you anymore. It's estimated that once a fraudster finds a vulnerable online store, they will commit fraud against it at least 3 to 4 times.

External Tools

1. Payment gateways with PCI compliance, fraud screening features, and AVS/CVV matching.
2. Automated fraud prevention tools that are capable of reviewing suspicious orders on the fly and blocking fraudulent orders and customers instantly.
3. CAPTCHA verification helps distinguish between human users and bots.

Measuring Effectiveness

Fraud prevention tools that catch card testing serve a dual purpose—they'll help you prevent other types of payment card fraud as well. But they can also raise concerns for merchants due to their high false positive rate and the costs of licensing and managing them. You can't just set-and-forget good fraud prevention tools, they need constant tweaking to adjust to the ever-changing landscape of internet fraud scenarios. High-volume merchants might even want a dedicated employee or part-time staff to actively monitor and adjust these tools.

The overall effectiveness of the tools and strategies you're using can be measured by the number of instances of card testing fraud per year. For small and medium-sized merchants, card testing fraud can be a major issue due to the fact that it can lead to a huge spike in chargebacks.

AN INTRODUCTORY GUIDE TO ECOMMERCE FRAUD AND PREVENTION

Empower Yourself to Fight Fraud — But Get Help If You Need It

Even with the best and most effective fraud prevention tools and strategies in place, chargebacks are still going to happen.

01

Responding to chargebacks in time to dispute them, putting together the evidence necessary to succeed at having them reversed, and identifying the root causes of your chargebacks can take a lot of time, labor, and resources.

02

While some businesses may have a small enough chargeback problem that they're able to handle it in-house, sometimes it makes sense to call in the experts and hire a chargeback management company.

03

The main advantages of outsourcing chargeback management are increased ROI, access to expertise, 24/7 availability, and comprehensive reporting that can help you understand the vulnerabilities in your business.

04

On the other hand, expert chargeback management doesn't come cheap, and it's important to choose a company that offers transparent billing along with security and performance guarantees. A good company should be able to show you, by the numbers, how they're providing a solid return on your investment.

05

Fighting fraud and chargebacks will always be an ongoing, evolving process. The best you can do is stay educated, understand the threats you're facing, and make every reasonable effort to protect your business from fraud.

AN INTRODUCTORY GUIDE TO ECOMMERCE FRAUD AND PREVENTION

Chargeback Gurus’ Vendor Profile

Chargeback Gurus

CHARGEBACK GURUS

Chargeback Gurus helps businesses protect and recover revenue by providing effective chargeback management solutions, AI analytics and insights powered by our proprietary **FPR**ONE™ platform.

By understanding our clients' needs and fully aligning with their goals, we help them reduce chargebacks and increase recovery rates to maximize revenue retention. Our technology solutions use powerful data science and AI analytics—combined with deep industry expertise—to deliver hundreds of millions of dollars in recovered revenue to our clients.

Contact us

✉ win@chargebackgurus.com ☎ 866.999.3758

Follow us on

CHARGEBACK GURUS