METRO MERCHANT SERVICES ePAYMENT PROCESSING SOLUTIONS

# Understanding Fraud and Chargebacks

Fraud is a significant and growing problem for businesses. Online fraud jumped up 33% in 2016, with total fraud losses that year calculated at $6.7 billion. Some analysts expect that figure to rise to $7.2 billion by 2020.

**WHAT IS A CHARGEBACK?** A chargeback occurs when a consumer contacts their bank or credit card issuer, disputes a charge on their account, and requests a refund. It typically occurs when they spot a charge on their bank or card statement that they either

1) don't recognize or
2) are unhappy in some form or fashion.

Consumers may file chargeback disputes for various reasons, including dissatisfaction with the product or service they purchased, a higher-than expected cost, late or delayed shipment, or unknown charges due to true fraudulent activity or identity theft.

**Chargebacks are one of the biggest challenges facing merchants today.** Not only do they equate to millions in lost sales every year, but because of associated fees—the costs to manufacture, market and ship the product, and the potential damage to valuable merchant accounts—they typically mean a financial loss of 2.5 times the sale price.

Sadly, the problem is getting worse, too. From 2016 to 2017, the rate of chargebacks jumped 179 percent from four years prior, and merchants lost a whopping 1.9 percent of their revenue.

## 5 Types of CNP Fraud –

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

### True Fraud

This is the relatively straightforward form of fraud most of us associate with the term. It refers to using stolen credentials— either identity theft or a credit card number—to make a purchase online. The implementation of EMV technology has caused a surge in e-commerce fraud—as credit card fraud has become harder in card present environments, thieves have shifted their focus to online targets.

### Friendly Fraud

"Friendly" fraud is anything but friendly. It takes its name from the fact that it starts out as a perfectly legitimate transaction. The fraud comes in when the purchaser disputes the purchase with their bank, getting their money back via chargeback and keeping the goods or services they purchased. Some customers commit friendly fraud unknowingly, out of impatience, frustration with the merchant, or ignorance about how the chargeback process is supposed to work.

### Phishing (Account Takeover Fraud)

"Phishing" refers to a variety of techniques criminals use to gain access to other people's personal accounts. There are many ways to do this, which can be as simple as guessing poorly-chosen password reset security questions (it's not that hard to find out somebody's mother's maiden name). A phisher who gains access to a customer account at an online store could use stored payment credentials to make purchases.

### Refund Fraud

This is when a criminal purchases something with a stolen credit card, then returns it to the store for a refund to a different account, or for cash or store credit. Historically, this form of fraud has been easier to pull off in brick-and mortar stores, but the idea has been adapted for use in e-commerce settings.

### Card Testing/Carding

Sometimes, a cyber thief gets his hands-on a stolen credit card number but doesn't know if it's valid, or how high the credit limit is. They might make small test purchases to garner information about the card. Card testing can scale up in a big way, with organized criminals using bot networks to test thousands of stolen cards at once. This type of fraud is particularly dangerous for merchants, who might get hit with separate chargebacks for many small purchases, incurring fees for each one. This type of fraud is on the rise, growing by over 200% in 2017.

## Effective Prevention Tools & Strategies

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

# True Fraud

## In-House Strategies

**1. Activate AVS and CVV matching features in your payment gateway.** Few thieves will possess 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 it.

**2. Review orders that request rush or overnight shipping** manually before fulfilling them, especially if they have different billing and shipping addresses. Fraudsters often ask for expedited shipping so they can get their purchases before merchants catch on to their deception. A brief phone call or email can confirm whether the request is valid. Also, if you ship internationally and the transaction is fraudulent, you will automatically lose any chargebacks.

**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. Flag orders that are unusually large,** multiple orders from the same customer, and unusual international orders for review. It can be hard to turn a skeptical eye on an unexpected order that seems too good to be true, but assuming the best isn't an effective way to stop fraud. Orders that don't fit your usual sales patterns should be scrutinized.

**5. If you have a suspicious order, call the customer to verify their phone number, email, and physical addresses.** You don't need to catch many fraudsters this way for it to be well worth the extra time and work it takes, and legitimate customers should appreciate your due diligence.

**6. 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.

# 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 your charge on their bank statement. The name of your business or store should be included in the descriptor so that customers can easily identify the origin of the charge.

**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 friendly, 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 24/7 customer service line instead. If your customer service staff is easy to reach and trained to provide comprehensive assistance with a great attitude, 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 expecting to receive 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.

# Phishing

## 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 accordingly. Don't give them that option.

**2. Make your customers create complex passwords** that include numbers, special characters, capitalized letters, and 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 unsecure Wi-Fi network.

**4. When utilizing third-party developers,** establish secure processes and protocols for writing code, saving code, and storing login credentials. Your own security measures won't matter much if you give copies of your data to people or companies that aren't as cautious.

**5. Decrypt 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.

**6. Use reliable third-party hosting services** like AWS or Google Cloud when using custom CRM systems. Smaller or newer hosting services aren't likely to have similarly robust security features.

**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. Subscribe to your own email updates and newsletters** so that if a fraudster ever gains access to your subscription list and tries to pose as you, you'll know about it.

**10. 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.

# Refund Fraud

## 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. Avoid overnight shipping during the holiday season.** This is a prime time for shipping delays, and criminals often take advantage of that as a cover for fraud.

**6. 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 Blacklisting these customers can help your customer service team avoid issuing refunds to known chargeback abusers.

# Card Testing AKA Card Cracking

## 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. Look for a spike in small orders.** Fraudsters often try to place multiple small orders within a short span of time in order to test different card numbers they've stolen. Set a minimum order amount and keep a skeptical eye on small order spikes that look too good to be true.

**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. Sometimes all it takes to verify an order is a quick phone call or email.

**5. Blacklist customers 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.

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

**Even with the best, most up-to-date, tested fraud prevention tactics deployed, chargebacks are still going to happen.**

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

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

# Chargeback Representment & Prevention

Merchants have the right to dispute a chargeback should they feel it is unmerited. If the merchant knows they've fulfilled their obligation to the client, delivered their goods and services, and has proof, they may be able to fight the chargeback and recover their lost funds. This is called chargeback representment:

1) Cardholder initiates a dispute for a transaction
2) Issuer sends the transaction back to Acquirer electronically
3) Acquirer receives the chargeback, resolves or forwards to the merchant
4) Merchant accepts the chargeback OR addresses and resubmits to Acquirer
5) Acquirer reviews the information from the merchant – if agrees, then represents chargeback electronically to Issuer
6) Issuer receives the item and redeposits it to the cardholders account OR submits it to VISA or MC to determine financial liability if the item is not addressed
7) Cardholder receives the dispute resolution information and may be credited or rebilled for the item in question.

**It's very important that merchants fight chargebacks whenever possible.**
As chargebacks cost merchants in lost sales, cost of goods, marketing expenses, transaction fees and more, they often result in significant financial losses. They can also threaten the very merchant accounts necessary to do business if you step over the chargeback thresholds set by the Card Networks.

## How the Dispute Process Works

Cardholders can contact their issuing bank within a specified timeframe (usually 120 days) from the date of a transaction and reverse the transaction. The bank will ask them why they are disputing the charge, then assign the appropriate reason code to the chargeback. The reason codes, which are defined by the Card Networks, help you to understand the root cause of chargebacks and what supporting documents you're going to need if you choose to dispute a given chargeback.

When a cardholder calls their issuing bank to request a chargeback, the bank takes the customer's explanation at face value; if the customer claims fraud, the bank attaches the "Fraudulent Transaction" reason code, and if they say it was a merchant error, the bank believes

them. What this means is that if you believe the customer is incorrect – or is lying – the burden of proof lies entirely on you. It's your responsibility to prove that you fulfilled your end of the bargain.

There are five parties involved in a chargeback:

- The Cardholder
- The Issuing Bank
- The Card Network
- The Acquiring Bank
- The Merchant

## Just because a customer claims they never authorized a transaction doesn't make it true.

The bank can be defrauded just as easily as you can, so it's always best to do your own analysis of the transaction rather than taking the issuer's word for it. If you believe that a chargeback is illegitimate, then you have the right to fight back. To dispute a chargeback, you will need to submit a rebuttal letter arguing your case and a variety of supporting documents to your acquirer, who then forwards them to the issuing bank to make a ruling. The requisite documents vary depending on the exact nature of the chargeback, so there is no one-size-fits-all process for winning a dispute. Adding an additional challenge to this process is the fact that it can often take a long time for the issuer to inform the acquiring bank and for your acquirer to inform you. Disputing a chargeback must be done within a narrow timeframe, so by the time you find out about a chargeback you may not have much time left to fight it.

## This is why you need to fight chargebacks the smart way.

The process can be confusing, the rules and regulations governing it are frequently changing, and the amount of time you have to fight back is limited, so be prepared. If you're handling your chargeback management in-house, you need to have a smart strategy in place in order to win.

## The Card Networks break chargebacks down by reason codes.

Each network has their own set of codes, which can teach you a lot about the root causes of your chargebacks. But because issuing banks always take the cardholder's explanation at face value, these reason codes often don't line up with the truth.

Some merchants assume that a reason code which indicates a fraudulent transaction always means true fraud, so they don't dispute the chargeback because the merchant is liable in that case. But making this assumption can cause you to lose up to 25% more of your revenue to chargebacks. It's best to do your own analysis in order to discover the true cause of chargebacks so that you can maximize your success and recover the most revenue.

## The centerpiece of any dispute is the rebuttal letter.

This is a cover letter which explains clearly and concisely why you believe the bank should rule in your favor.

At the issuing bank, the person who is ruling on your dispute may only have five minutes to evaluate all your supporting information, so they're going to rely on your rebuttal letter to make a compelling case. Highlight the key points and provide a list of all the supporting documents provided because they may not manually look through them all.

***The key is to make it easy for them to rule in your favor, so keep it under one page and keep your paragraphs short.***

# Compelling Evidence

The Card Networks have clearly defined what kinds of documentation qualify as compelling evidence depending on what kind of business you operate: a retail store, an eCommerce store selling tangible goods, an eCommerce store selling digital goods and/or subscriptions, or a travel and ticketing agency.

### Retail

In point-of-sale retail, chargebacks are typically filed on high value purchases, often caused by buyer's remorse. To dispute these chargebacks, you will be required to prove that you verified the cardholder's identity at the time of purchase. For high ticket items, the best practice is to ask the customer for ID before processing the transaction and to scan and store a copy in case of a future chargeback.

### Physical Goods

When selling physical goods online, a signed proof of delivery is your best weapon. Any online transactions should also be supported by Address Verification (AVS) and a CVV match (the 3-digit code on the back of a credit card). If all else fails, photos posted on social media showing the customer using your products also qualifies as compelling evidence.

### Digital Goods and Subscriptions

Selling digital goods and/or subscriptions makes it more challenging to prove the delivery of the product. At the time of sale, it's a good idea to match their IP address to the address associated with their credit card, and if possible, to use their IP to collect proof that they have used your product, for instance by downloading a program or logging into a platform.

There are many different reasons why a consumer might file a chargeback, so there are just as many ways to dispute them. Take time to understand the chargeback process, implement preventive measures internally and keep all supporting documentation handy. Also, keep up to date on the changes made to the chargeback guidelines by the Associations. The best way to do this is to sign up for Google Alerts to notify you every time one of the Card Networks releases a new set of regulations.