SEON

EBOOK

The Ultimate Guide to **Reducing Chargebacks**

SEON Technologies Ltd.
seon.io

info@seon.io
0044-20-351-44790

Table of content

Introduction

Browsing the user forum of Shopify, the largest online store builder, you'll find hundreds of comments from new merchants who are baffled by chargebacks. The company has no less than three support pages dedicated to explaining what they are.

The main takeaway? Chargebacks are unfortunately an inescapable fact of selling goods or services online.

Accepting payments worldwide and at all times has tons of advantages, but chargebacks are without a doubt the most negative consequences of working in the card-not-present space.

However, there are steps anyone can take to decrease those rates. This ebook will dive deep into the technical processes of chargebacks and explain how to implement the right solutions to eliminate them.

Chargebacks: a definition

Chargebacks are a protection designed to help customers. When someone maliciously used their card without their knowledge (or they are dissatisfied with a product they bought online or over the phone), they can claim a forced reversal of funds to their bank account - or chargeback.

The funds have to be taken from the merchant's account, and sent back to the customer. This can take weeks or months and cost a great deal in administrative fees, which are always passed on to the merchant.

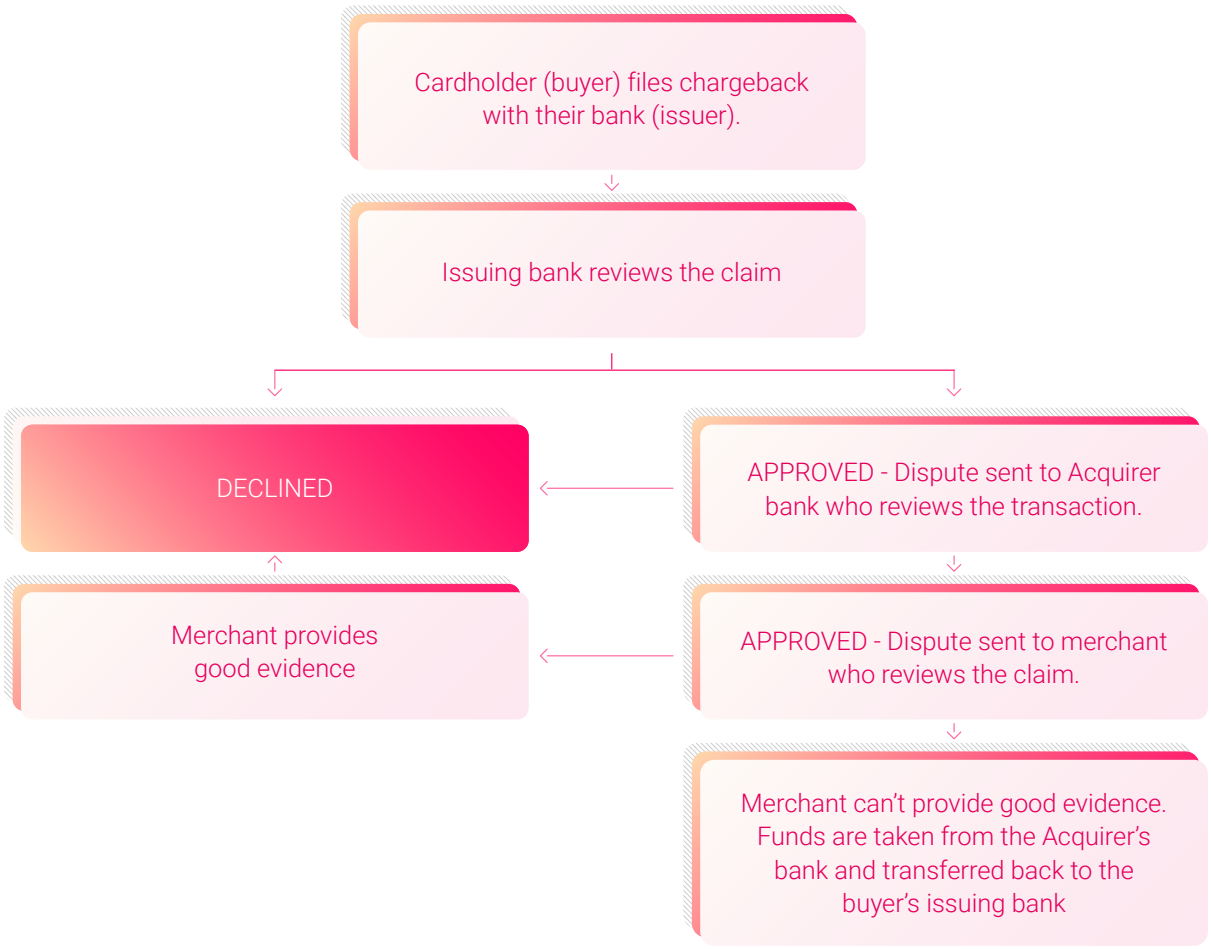
1.1 KEY PLAYERS IN THE CHARGEBACK PROCESS

To understand why chargebacks are so expensive, it helps to see who is involved in the process:

- **Buyer, or customer:** the person who files a chargeback request. We'll go into the numerous reasons later.
- **Merchant:** the online store or business that sold the goods or services. They can either accept the chargeback, or fight it through a dispute.
- **Issuer:** The bank connected to the buyer's credit card.
- **Acquirer:** The bank or financial institution that processes card payments for the merchant.
- **Payment Gateway:** the software used to transfer transaction data from the merchant to the acquirer.
- **Credit card company:** The organization that oversees the whole chargeback process. As we'll see, major credit card companies have different procedures for dealing with chargebacks.

1.2 ANATOMY OF A CHARGEBACK

The positive consequence of having so many parties involved is that any of them can prevent or dispute a transaction if it looks suspicious. Unfortunately, this sometimes leads to false positives, which are frustrating for customers.



The True Cost Of Chargebacks

Chargebacks add insult to injury for retailers. They lose a sale, a physical or digital item, and have to pay a fee of $20 - $100. It can even incur penalties if it happens too often.

Failing to meet card company's requirements for chargebacks means merchants will be considered high-risk, fined, and in extreme cases, prevented from accepting the company's payments altogether.

In fact, it has been estimated that every dollar lost to a chargeback costs merchants $2.40. This means a **$100 chargeback can result in losses of more than $240** due to the extra fees.

And that's before we even consider the additional time and effort lost to chargebacks for the sales team, IT or customer support agents.

You can read the full Visa Chargeback guide here. Here are also the guides for Amercian Express, and for Mastercard.

2.1 THE SCALE OF THE PROBLEM

There is limited published data regarding chargebacks because parties involved tend to keep their information to themselves. Issuing banks and card networks, for example, refuse to publish essential data or specific numbers on chargebacks in areas such as dispute win rates.

Similarly, merchants hesitate to release any information regarding chargebacks, as it could harm their reputation.

Despite the lack of transparency, it's clear the chargeback problem is getting worse. It is estimated that chargebacks cost retailers worldwide up to $40B in 2018.

Harsher rules: the visa example

Credit card companies do everything they can to pass the task of decreasing chargebacks onto merchants. Visa, for instance, recently updated their policies:

- *Retailers cannot go through more than 100 disputes per month*
- *The dispute rate must be under 0.9% of all transactions*

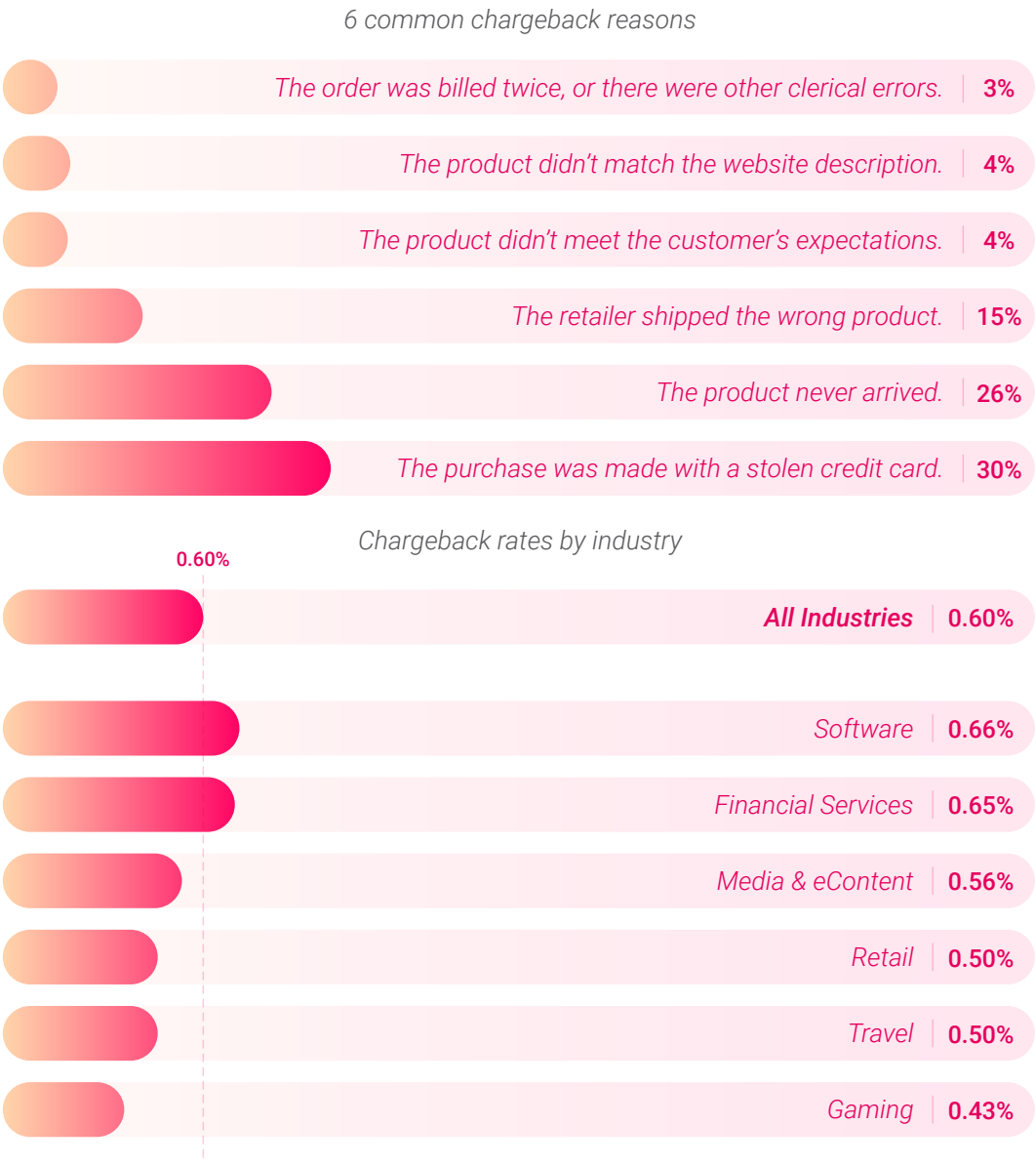
Historically, the accepted dispute ratio was set around 1%. We can expect more card providers to be increasingly strict and lower those rates in the future.

2.1 WHY BUYERS REQUEST CHARGEBACKS

There are typically four broad reasons why a buyer would want to process a chargeback:

- **Merchant error:** shipped wrong item, forgetting a discount, or technical mistake…
- **Unauthorized payments:** usually from family members, such as children who purchase mobile games without their parent's consent.
- **Clear fraud:** card details have been stolen by fraudsters who purchased goods without the original cardholder's authorization.

- **Friendly fraud:** also known as chargeback abuse or liar buyer. This is a growing problem which we will break down in detail below.



Source: Chargebacks911

What Makes a High Fraud Target

While certain industries are more often hit than others, there are a few telling signs you could be a high-risk merchant.

1. Do you sell high resale value items?

High-end electronics such as Apple products, computer hardware, GoPro cameras or cutting-edge TVs are all in high demand by scammers. Digital goods and gaming goods, but also airline tickets and accommodation bookings are increasingly in demand by fraudsters.

Finally, it is interesting to note that fraudsters also target business services such as hosting services, logo and web design, and even legitimacy-boosting tools like search engine optimization services and coupons for Facebook ads.

2. Do you operate as a digital wallet?

As an elegant and simple alternative to cards, a digital wallet also means accessing real funds that are only protected by a password. However, fraudsters are increasingly cunning when it comes to securing these passwords, whether it is to access P2P transfer accounts, cryptocurrencies, or any marketplace with a deposit and withdrawal option.

According to a report by Gallup, a leading corporate analytics firm, more than 55% of users are still on the fence about digital wallets due to safety concerns. Specifically, users do not enjoy the fact that they might become target of phishing attacks in order to secure their passwords.

3. Do you give generous promos or bonuses?

Promotional offers are a fantastic way of attracting new customers. From free trials to opening discounts, they provide a strong incentive for users who are still undecided about signing up to your offer. Sadly, fraudsters are adept at finding loopholes and strategies to abuse these offers.

Similarly, referral fees and affiliate payouts are also a strong target. Fraudsters certainly have the means, time and incentive to create hundreds or thousands of accounts in order to abuse your generous offers.

How Credit Card Details Are Stolen

Before customers file chargebacks because of fraud, their credit card details must end up in the wrong hands. Unfortunately, fraudsters have access to a growing number of methods with which to access these details.

Most people will already be familiar with phishing, where fraudsters pose as legitimate companies via email or phone to get people to submit their details voluntarily. One trend we've seen develop in the last few years is also to create fake job posts and gather information through applicant video and forms.

Credit card skimmers are also on the rise, and FICO estimated a 70% increase in compromised credit cards between 2016 and 2017. Malicious card readers that "skim"

the card information and send it back to criminal servers are particularly found at gas stations and ATMs.

Abusing zero-day vulnerabilities in e-commerce platforms continues to be the major source of credit card theft. In these cases, the delinquent exploits a bug right before the developer has the opportunity to create a patch fix.

Point of Service (PoS) malware is also something to watch out for, and so are other viruses, trojans and malicious software found on tablets, phones and personal computers.

Data breaches, which show no sign of slowing down, can also contain credit card information along with personal details, and this data usually ends up on the darknet where fraudsters can purchase it.

Customer Friction vs Trust

All these avenues for fraudsters to acquire credit card numbers means merchants have to be more suspicious than ever. In fact, even the most customer-focused retailers have to be vigilant with new registrations and account takeovers (where fraudsters find a legitimate user's login information).

Unfortunately, manually reviewing each account and transaction isn't just extremely time consuming. It also slows down business by increasing customer friction, which could turn legitimate buyers away.

According to Radware, even a 2 second delay at checkout can increase abandoned cart rates up to 87%.

The challenge of balancing security and user experience is particularly great when it comes to countering the biggest reason for chargebacks: friendly fraud.

5.1 NOT SO FRIENDLY FRAUD

Friendly fraud is the fastest growing reason for chargebacks, growing at a rate of 41% per year. It is estimated that 60-80% of all chargebacks are from customers who:

- **Experience buyer's remorse:** this is often observed after holiday sales or special events such as Black Friday, where customers change their mind

about a product, and hope to game the system by keeping it and getting their money back.

- **Don't want to pay for a family member's purchase:** this is different from unauthorized payments, as the cardholder was aware of the purchase, but then asks for a refund nonetheless.

- **Are plainly malicious:** this is for buyers who are aware of chargeback policies and simply want to exploit them with their own credit cards.

This type of fraud can be harder to prevent, simply because, on paper, the cardholder looks like a legitimate buyer. However, we'll see how collecting the right data through a fraud prevention tool can help with dispute resolution, and even help stop friendly fraud before it's committed.

5.2 MERCHANT RESPONSIBILITIES

Educating buyers goes a long way in preventing refund requests. Luckily, there are a number of steps that any online business can take to reduce the amount of chargebacks:

- **Be as descriptive as possible:** your products or services should be described as precisely as you can to ensure customers aren't disappointed or underwhelmed by the difference between what they expect and what they receive.

- **Be easy to reach:** Particularly useful with buyer's remorse (friendly fraud). It is important to have a phone number, live agent or support email for customers, clearly highlighted on your website. Your contact details should also be present on receipts, emails and packing slips.

- **Respond as quickly as possible:** this adds a lot of value and is part of the overall customer service experience any business should offer.

- **Ensure you have full authorization for an order:** To prevent improper authorization chargebacks, an online merchant should get authorization for each package they ship out from their store/warehouse.

- **Wait until shipping before charging:** There is a difference between an authorization hold and the customer being charged. The customer should not be charged until the goods leave the warehouse, or the services have been provided.

5.3 DEALING WITH CHARGEBACK DISPUTES

Unfortunately, even with the best intentions, chargebacks happen. They will reach retailers and merchants via a message from the issuing credit card company.

Example B – Chargeback Debit Advice

Date

TRW REDI PRPRT
Attn: Ms. Judy Smith
1234 Main Street
Any City, XX 12345

Respond Required By: MM/DD/YY

This is a notification of a chargeback initiated by: (Name of Issuing Bank)
Reason: (Example) 53 – Not as described

Code: 53
Type: Retail Sales
Trans. Amount: $225.00
Chargeback Amt: $225.00
Invoice/Ticket #:
Cardholder #: 0000000000000000
Member Message:

Case #: 1234567890 1 0
Ref #: 123456789123456789 1234
Posting Date: MM/DD/YY
Resolved Date: MM/DD/YY
Original Ref #: 12345678
Received Date: MM/DD/YY

ACTION TAKEN BY MERCHANT SERVICES

- Verified this chargeback is valid and has been received within timeframes established by MasterCard/VISA rules and regulations.
- The above Chargeback Adjustment Advice information is accurate.
- Your account has been adjusted because:
- Cardholder canceled/Cardholder due this amount (action varies based on chargeback reason code)

Please Be Aware

- Review the "Merchant Action Necessary to Remedy Chargeback" section of the accompanying chargeback adjustment reversal request form. This will aid you in identifying the proper information of documents needed for us to make every effort to resolve this chargeback and collect your funds.
- You must supply chargeback rebuttal documentation no later than MM/DD/YY. Failure to do so will result in the forfeiture of your reversal rights established by current Master Card/VISA rules and regulations.
- Your business checking account has been adjusted for the chargeback amount.
- Should you have further questions, you may contact NPC Customer Service.

Once it has been initiated by a buyer, it's the retailer's job to respond to the notice. You will have numerous opportunities to dispute the chargeback and should collect as much data as possible about the buyer, combining your own systems and, if possible, an effective fraud prevention tool:

- **Proof of delivery:** Ideally signed by the buyer when the item reached their house.

- **Customer communication:** Any email, text message, or other forms of communication that proves the customer was aware of the purchase.
- **Customer communication:** Any email, text message, or other forms of communication that proves the customer was aware of the purchase.
- **Positive payment result:** Showing that the billing address linked to the credit card issuer matches the billing address where the items were sent / delivered.
- **Address match:** Billing address and shipping address linked to a customer's name can be matched to a public listing.
- **Purchase history:** You should also collect the payment methods previously used by the customer, and keep a history of all purchases made with the same card that didn't result in a chargeback.
- **Social media:** An increasingly useful tool in proving fraudulent chargeback requests. With clear fraud, the buyer and cardholder are rarely connected in real life. However, showing that they are friends on Facebook, Twitter or other platforms can increase the likelihood of proving friendly fraud.

Spotting fraudsters through social media lookup

Showing that a new customer has no social media presence is a strong indicator that they could be fraudsters. According to our own research, 98% of fraudsters who used a new email address whose name matched the card name had no social media presence.

Social media history can also reveal overt friendly fraud attempts. For instance, a customer might claim they never received a pair of shoes and post a picture of them on Instagram.

- **Email and phone matches:** The email address and phone number should match the ones linked to the billing or shipping details, and also that of social media profiles.
- **Connection type:** You should keep track of whether the customer used special connection tools such as proxies or VPNs. A large distance between the IP address and the shipping address should also raise red flags.

Preventing Chargebacks Before They Happen

Preparing yourself for fighting chargebacks is great. Preventing them from happening in the first place is even better.

On top of all the data highlighted above, a good fraud prevention tool should also give you a good idea of who the buyers really are, by focusing on three touchpoints:

- **Signup:** The ideal phase to flag fraudsters, as they won't even be able to access your website.
- **Login:** In the case of account takeover (ATO), it's important to see if customers really are who they say they are.
- **Purchase:** your last chance to prevent a fraudulent transaction from taking place.

Luckily, there is a tremendous amount of information you can leverage to ensure fraudulent purchases don't go through. At SEON, we combine a number of modules to gather and enrich data, and machine learning to generate a risk score.

- **Powerful device fingerprinting:** generates browser and device fingerprint IDs, which help you track users across incognito browsing, emulators and VPNs. Thousands of data points are collected and compared to identify bad users - even after they reinstall or update their browser.
- **Email profiling:** a single email address can reveal useful information through data enrichment. You can use the social media lookup feature, and evaluate how risky the address is by looking at domain age, type, string analysis, and more...
- **Predictive Scoring:** Combines machine intelligence with human insights to generate risk scores. The rules can be tweaked manually, and improve overtime.
- **Whitebox Machine Learning:** SEON's algorithm learns from previous chargebacks patterns and retrains itself numerous times a day. You get results via human readable rule suggestions with specific accuracy percentages, where rules are branches and parameters are the node of a decision tree.

- **Behaviour Analytics:** Collect and screen complete customer activity on your website via API. You can enable specific algorithms for login, checkout and even signup to prevent fraudulent transactions at the earliest point possible.

Using one or all of these modules helped companies like the Avis Rental Group slash chargeback rates by 23%, and global trading platform Libertex Group reduce theirs by 45%.

The costs and resources lost to chargebacks aren't likely to decrease for online retailers and merchants. With added pressure from credit card companies, it's becoming more important than ever to prevent chargebacks before they happen, instead of wasting time and money fighting them.

Luckily, there is a lot you can do today in educating your customers about chargeback risks and protecting yourself from friendly fraud attempts. Moreover, fraud prevention tools like SEON increase the amount of data you can use to block fraudsters before they register to your platform, login, or make a purchase.

To see how SEON can help you reduce chargeback rates today, please visit www.seon.io

To see how SEON can help your company prepare for the future, please visit seon.io

Visit our website

Or schedule a personalised product showcase call now.

Schedule a call

SEON Technologies Ltd.
seon.io

info@seon.io
+44 20 8089 2900