SEON

seon.io

Chargeback Fraud: Detection & Prevention

Contents

Introduction

A notable surge in friendly fraud marks the current state of chargeback fraud. The 2023 Chargeback Field Report noted that nearly 75 percent of respondents reported an uptick in chargeback fraud – with friendly fraud accounting for an average of 44 percent, attributed to expanding payment methods and increasing economic pressures. This worrying trend underscores the need for proactive chargeback management and fraud prevention strategies to mitigate lost revenue in today's challenging commercial environment.

What is Chargeback Fraud?

Chargeback fraud encompasses the deceptive activities linked to chargeback requests or processes. It can range from customers filing false chargeback claims, known as friendly or first-party fraud, to the use of stolen credit cards, in which charges are later disputed and charged back by the rightful owner. Another more complex form of chargeback fraud occurs when a customer obtains goods without payment, illegally requesting a chargeback or exploiting a stolen card.

How Does Chargeback Fraud Work?

Chargeback fraud mimics legitimate chargebacks. In a fraudulent transaction, the cardholder contacts their bank and provides a misleading or exaggerated reason for requesting a chargeback – such as that an item was never received or the transaction was not authorized. The bank contacts the merchant's bank to initiate the process. The merchant is then faced with a decision to either contest or accept the chargeback. If uncontested, the cardholder receives back the amount of the transaction.

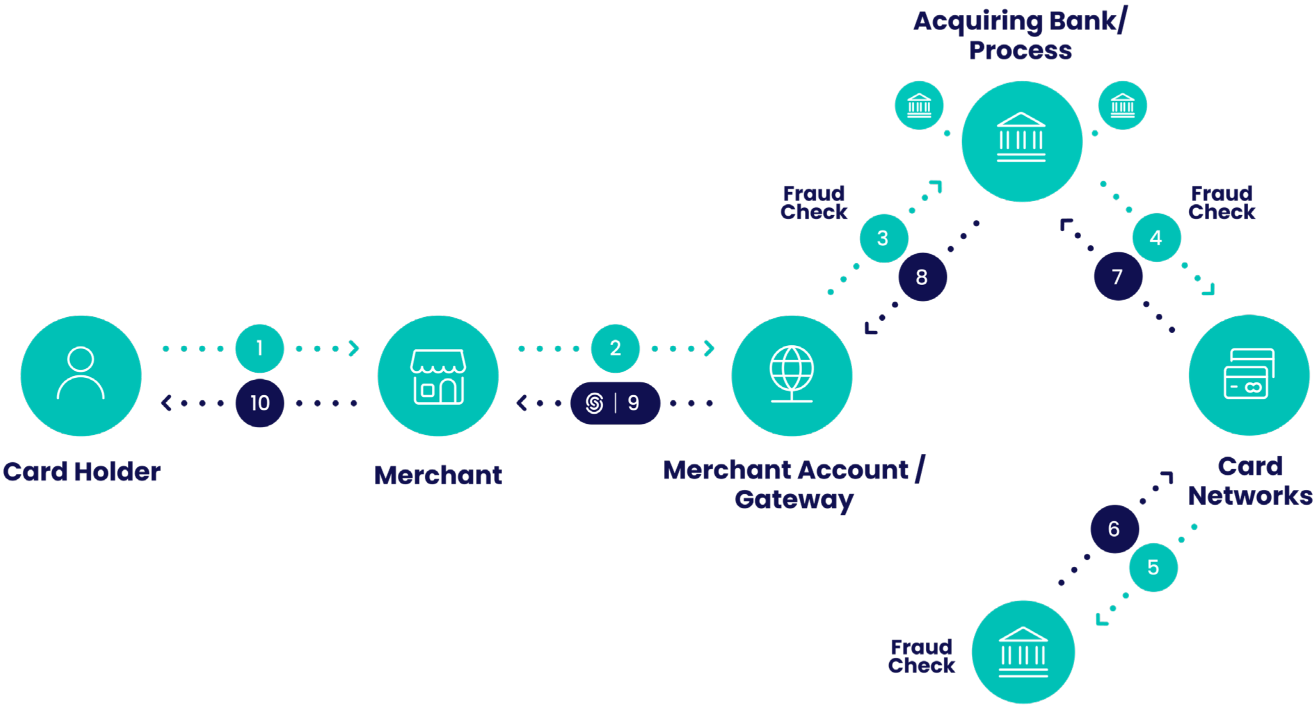
Steps in a Chargeback

1 The cardholder approaches their issuing bank and requests a chargeback, providing an explanation of the issue.

2 The cardholder's bank contacts the acquiring bank, which is who the merchant deals with.

3 The merchant chooses whether to accept or contest the chargeback.

4 The cardholder receives the contested sum of money.



Three Common Types of Chargeback Fraud

While some chargebacks stem from merchant error or poor customer service, it is worth noting that honest disputes do occur as a result of communication breakdowns. The three most common types of chargeback fraud include:

Friendly Fraud

Friendly fraud is a broad category of fraud in which legitimate buyers are responsible for unwarranted chargebacks. In these scenarios, the card's rightful owner makes an online purchase and later disputes the charge with their bank, falsely claiming it was unauthorized or the product was never received. Subcategories include innocent or accidental fraud and opportunistic or malicious friendly fraud.

Criminal Fraud

This form of deliberate fraud is where a criminal uses a stolen credit card to make a purchase and then requests a chargeback from the bank after receiving the goods or services. In this type of fraud, the fraudster's objective is to receive purchased items or services without paying for them. At the same time, the genuine cardholder remains unaware of the transaction until after the fraud has occurred.

Triangulation Fraud

Triangulation fraud is a particularly malicious and complex exploit involving the customer, the fraudster and an online store. The fraudster sets up a web store or lists items on a big marketplace at unrealistic prices. When they receive an order for an item, they'll use the unsuspecting customer's information, shipping address and stolen credit card data to purchase that item from a different store. The customer receives their order, unaware of the fraud. Meanwhile, the customer's payment information is retained for further unauthorized transactions.

How Do Chargebacks Work?

Three Possible Outcomes

After a chargeback is initiated, there are three potential outcomes – all with negative consequences for the merchant.

1. The merchant accepts the chargeback

- The merchant loses item(s), funds and admin fees
- The merchant's chargeback ratio increases
- The cardholder receives the money
- The cardholder or fraudster keeps the item(s)

2. The merchant contests the chargeback but loses

- The merchant loses item(s), funds and admin fees
- The merchant's chargeback ratio increases
- The merchant loses time spent gathering and filing evidence
- The cardholder receives the money
- The cardholder or fraudster keeps the item(s)

3. The merchant contests the chargeback but wins

- The merchant loses item(s) and admin fees
- The cardholder does not receive money
- The cardholder or fraudster keeps the item(s)

This dispute process that takes place if the merchant chooses to contest a request is called chargeback recovery. It can be an extremely time-consuming process that requires extensive knowledge of chargeback codes for specific reasons. Risk teams may jeopardize hours fighting a single dispute.

Many merchants opt to simply deal with the loss rather than wasting energy challenging the chargeback. Rather than dealing with chargebacks in the aftermath, the best scenario is to prevent them from happening in the first place.

Why Do Buyers Request Chargebacks?

Four common reasons why merchants receive chargeback requests include:

- **Merchant error:** Shipped the wrong item, forgot a discount or technical mistake.
- **Unauthorized payments:** Someone used a card without permission – usually family members, such as children who purchase mobile games without their parents' consent.
- **Card fraud:** The card details have been stolen by fraudsters who purchased goods without the original cardholder's authorization.
- **Friendly fraud:** Also known as chargeback abuse, first-party fraud or "liar buyer", this is a growing problem stemming from opportunistic buyers taking advantage of card issuers' and merchants' goodwill.

What Are the Costs of Chargeback Fraud for Businesses?

Fraudulent or not, every chargeback is detrimental to your bottom line in direct and indirect costs. Significant impacts include:

- **Fees** - It's estimated that every dollar lost to a chargeback costs merchants between 1.5 and 2.5 the disputed dollar amount, with fees ranging from $20 to $100 per chargeback. With most card networks shifting responsibility for paying the chargeback fees onto businesses, merchant costs total around 260 percent of the item's sale price.
- **Lost Inventory** - Fraudsters are not obligated to return products once a chargeback has been initiated in their favor – compounding financial loss with further inventory loss.
- **Card Monitoring Program Costs** - Banks track how frequent chargebacks occur for each merchant, and if your chargeback ratio exceeds 1%, you are

at risk of being tasked with extra card fees, put on a monitoring program, or worse, cut off from selling.

- **Operational Costs** - While delivering positive ROI, anti-fraud solutions are an extra expense you wouldn't have to contend with if chargeback fraud didn't exist.
- **Lost Opportunity Costs** - Every second spent dealing with a chargeback is time you could have dedicated to better customers. Being stuck in a dispute resolution process affects your resources and labor management. The opportunity cost is exceptionally high for customer service agents, the finance department, and even sales teams.

Who Is Involved in the Chargeback Process?

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

- **Buyer, or customer:** the person who files a chargeback request. Also known as the original/legitimate cardholder.
- **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. Major credit card companies have different procedures for dealing with chargebacks.

The Difference Between Chargeback & Other Fraud

There is a lot of overlap between chargeback fraud, first-party fraud and friendly fraud.

One thing to keep in mind is that all friendly fraud is conducted by a legitimate shopper (who is nevertheless acting maliciously), all first-party fraud is conducted by the cardholder (who is also acting maliciously), but **not all chargeback fraud comes from the cardholder.**

Another way to look at it is that it all comes down to intentions. While this isn't something that can be understood when the first transaction is made, you can spot patterns over time – ie, if a person appears to initiate chargebacks more often than not, they should be looked into.

Such a difference does come into play when balancing customer communication/ relationships and the option to simply blacklist them entirely.

Friendly Fraud vs Chargeback Fraud

Friendly Fraud

All fraud committed by legitimate customers, either deliberately or not – including return fraud, chargebacks and more.

Chargeback Fraud

All fraud linked to the chargeback process specifically – from chargeback requests under false pretenses to triangulation schemes and more.

Five Tips to Reduce Chargeback Fraud Today

Educating buyers goes a long way toward preventing both chargeback and refund requests. There are a number of steps that any online business can take to reduce the number of attempted chargebacks:

- **Be as descriptive as possible:** Your products or services should be described as precisely as possible to ensure customers aren't disappointed or underwhelmed by the difference between what they expect and what they receive.
- **Be easy to reach:** This is particularly useful with buyer's remorse. 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:** Place an authorization hold before you charge the customer. The customer should not be charged until the goods leave the warehouse, or the services have been provided, because a hold is incredibly easy to reverse.

How to Detect and Prevent Chargeback Fraud

Preparing your business to handle chargebacks effectively is a good strategy, but preempting chargebacks altogether is even more advantageous. A robust fraud detection and prevention solution can accurately identify your customers, focusing primarily on three critical interactions: user signups, login and the purchase/checkout process.

Striking a balance between deploying security measures, which can add friction at the checkout point, and allowing customers to have a seamless experience is crucial for maintaining customer satisfaction while ensuring transaction security.

Enable Secure Payment Processing Protocols

The following mechanisms are integral to deterring fraudsters and reducing chargeback events:

- **Data Encryption** - Acquire Secure Sockets Layer (SSL) certificates to demonstrate that your business is trustworthy and serious about data protection.
- **Address Verification Service (AVS)** - AVS is not a bulletproof step, but ensuring that the checkout address matches the cardholder's address may catch less sophisticated fraud attempts.
- **Card Verification Value (CVV)** - Certain online stores have removed CVV checks for faster payments. This simple tool could help lower chargeback fraud in the long run by adding CVV forms.
- **3D Secure 2.0 (SDS2)** - The primary card authentication method that introduces frictionless authentication for online transactions, SDS2 collects data, including IP addresses, transaction histories and purchase amounts, which is shared with the issuing bank, acquiring bank and payment processor. Analyzing collected data allows transactions to be deciphered as low or high-risk.
- **Tokenization** - A process whereby transaction data is replaced with randomly generated character strings, tokenization helps ensure that cardholder data remains confidential, making it harder to steal and use the card for transaction fraud.
- **Strong Customer Authentication (SCA)** - Part of the European Union's revised Payment Services Directive (PSD2, SCA forces businesses to increase authentication efforts such as multi-factor authentication (MFA), one-time passwords (OTP), or biometrics, for example.

Deploy Digital Footprinting

Referring to the trail of data individuals leave behind when they engage in online activities, and this information can be examined to evaluate risk. It can also be stored to dispute a chargeback or as part of a manual review.

- **Digital Footprint Analysis** - Access your customers' most comprehensive online identity and behavioral data by surveilling social signals and profiles to confirm identity and root out suspicious users.
- **Domain Analysis** - Derive insights from patterns, behaviors and methods related to domain information. For example, how old is the domain? How frequently is it updated? Is a user's email address attached to a temporary or disposable domain name?
- **Email Address Profiling** - Gather identity-related information, online behaviors and associations through email address analysis. Looking at the age of the email account, ensuring the address matches the customer's name and verifying information on the WHOIS database can compile a more precise picture to weed out fraudulent accounts.
- **Data Breach Checks** - An email address's age and maturity can be inferred if the address appears in data breaches. Fresher addresses imply an increased risk.
- **Messenger Use** - By identifying if a user's phone number is linked to messenger apps like WhatsApp, Viber, etc., you can capture information regarding when the user was last online, see a profile picture and often find a biography to verify user veracity.
- **Carrier Analysis** - Carrier analysis can detect the country of origin of a user's phone number, decipher whether it is a landline or mobile number and highlight SIMS or eSIM numbers to deduce risk profiles.
- **Phone Number Verification** - This is a simple way to filter out invalid phone numbers.
- **Risky Connections** - Determining if a user connects online via proxy, Virtual Private Network (VPN) or Tor can contribute to elevating risk. Likewise, pinging open HTTP ports can detect the use of proxies.
- **Internet Service Provider Identification (ISP)** - Risk factors can be impacted by

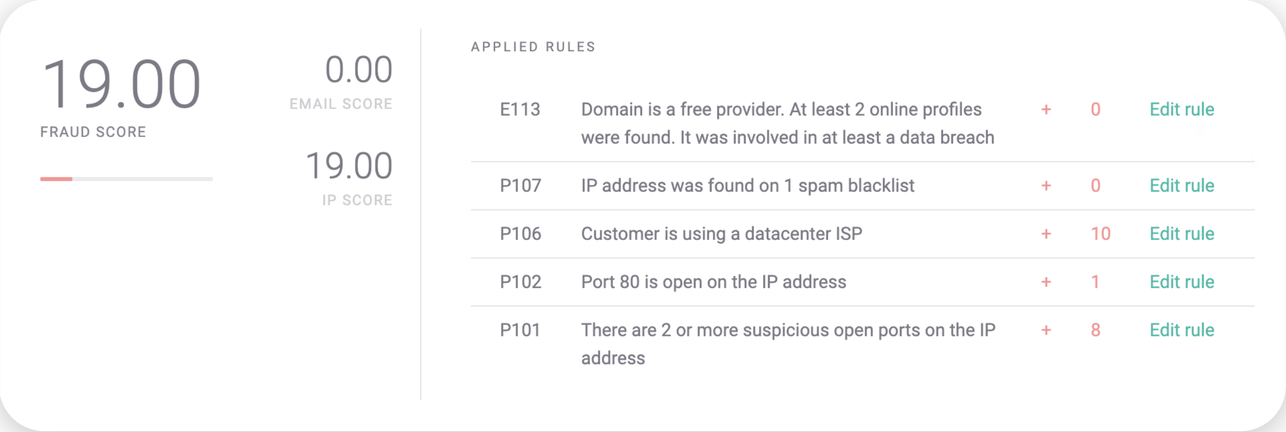
Leverage Data and Create Adaptable Velocity Rules

Examining the extensive device, IP, software and digital footprint data and taking points in isolation or combination while factoring in time and overall behavior can enable clearer insights to determine suspicious payments.

Setting up velocity rules is a mechanism that checks how often an action is performed in a specified timeframe. For example:

- Numerous failed login attempts
- Shipping address changes
- Many credit card numbers were attempted at checkout

This data can be fed through a risk rules engine to decide if the payment is suspicious.



19.00
FRAUD SCORE

0.00
EMAIL SCORE

19.00
IP SCORE

APPLIED RULES

E113	Domain is a free provider. At least 2 online profiles were found. It was involved in at least a data breach	+	0	Edit rule
P107	IP address was found on 1 spam blacklist	+	0	Edit rule
P106	Customer is using a datacenter ISP	+	10	Edit rule
P102	Port 80 is open on the IP address	+	1	Edit rule
P101	There are 2 or more suspicious open ports on the IP address	+	8	Edit rule

Looking at the red numbers above, you can see which rules were triggered and how they affected the overall fraud score. By adding and averaging the total number of points, it is possible to get a score that indicates risk. Rules can be weighted in order of importance to your business use case, as well as customizable thresholds set to automatically accept or reject a payment if it reaches a certain fraud score.

How SEON Fights Back Against Chargeback Fraud

Businesses can fight back against chargeback fraud by using an effective fraud prevention solution. With the ultimate goal of understanding their online visitors better through digital footprint analysis, device intelligence, and more secure payment processing protocols, you can create a customer-friendly, trustworthy environment to safeguard your business's bottom line.

FAQs

How serious is chargeback fraud?

Chargebacks directly impact both present and future revenue. Not only can a loss of stock and profits ensue but also merchants can lose the account with their card network or face higher fees when accepting orders – all because of a high chargeback rate.

Is a chargeback considered fraud?

This depends on the context but a chargeback is considered fraud if it's with malicious intent. Due to the fact the chargeback is actioned from the customer's side, telling the difference between deliberate chargeback fraud and genuine chargebacks can be difficult for merchants.

How do you fight chargeback scams?

Collecting as much evidence and establishing a customer profile is the best way to dispute chargeback claims yet it is still difficult for merchants to claim that the person is a fraudster as the system is set up to support the customers. Understanding who they are and their typical behavior will ultimately help, and provide that valuable evidence.

How did chargeback law start?

In 1974, the Fair Credit Billing Act in the US decreed that consumers who noticed a suspicious credit card transaction could contest it with their bank. The goal was to boost trust in the credit card and banking system and to de-incentivize merchants from committing fraud. Similar legislation was also put in place in other countries and regions – for example, the Consumer Credit Act in the United Kingdom. Chargeback regulations are the modern-day evolution of such legislation.

What happens when you request a chargeback?

First, the card-issuing bank receives the chargeback request. It is then handed to the acquiring bank that does the actual payment processing. The merchant is then served the request, and then can either accept the chargeback, paying back the spent money as well as incurred fees, or contest it, providing evidence that the product and its delivery were all up to par. The merchant will either win, concluding the issue, or lose – in which case the chargeback goes ahead.

How long does a chargeback take?

The process of a chargeback can take anywhere from 30 to 90 days. If the merchant does not dispute the chargeback, it will take much less time than if they do. Disputing the chargeback will trigger an arbitration process that involves looking at any evidence the merchant has that suggests the chargeback is invalid – a process that can drag on for weeks.

Sources

Chargebacks911: 2023 Chargeback Field Report

SEON

Reduce Chargeback Rates Now

Get real-time fraud prevention that leverages digital footprinting, device intelligence, machine learning, and custom lists and rules to know exactly who you are dealing with online.

Speak with an expert

seon.io info@seon.io +44 20 8089 2900 SEON Technologies Ltd.