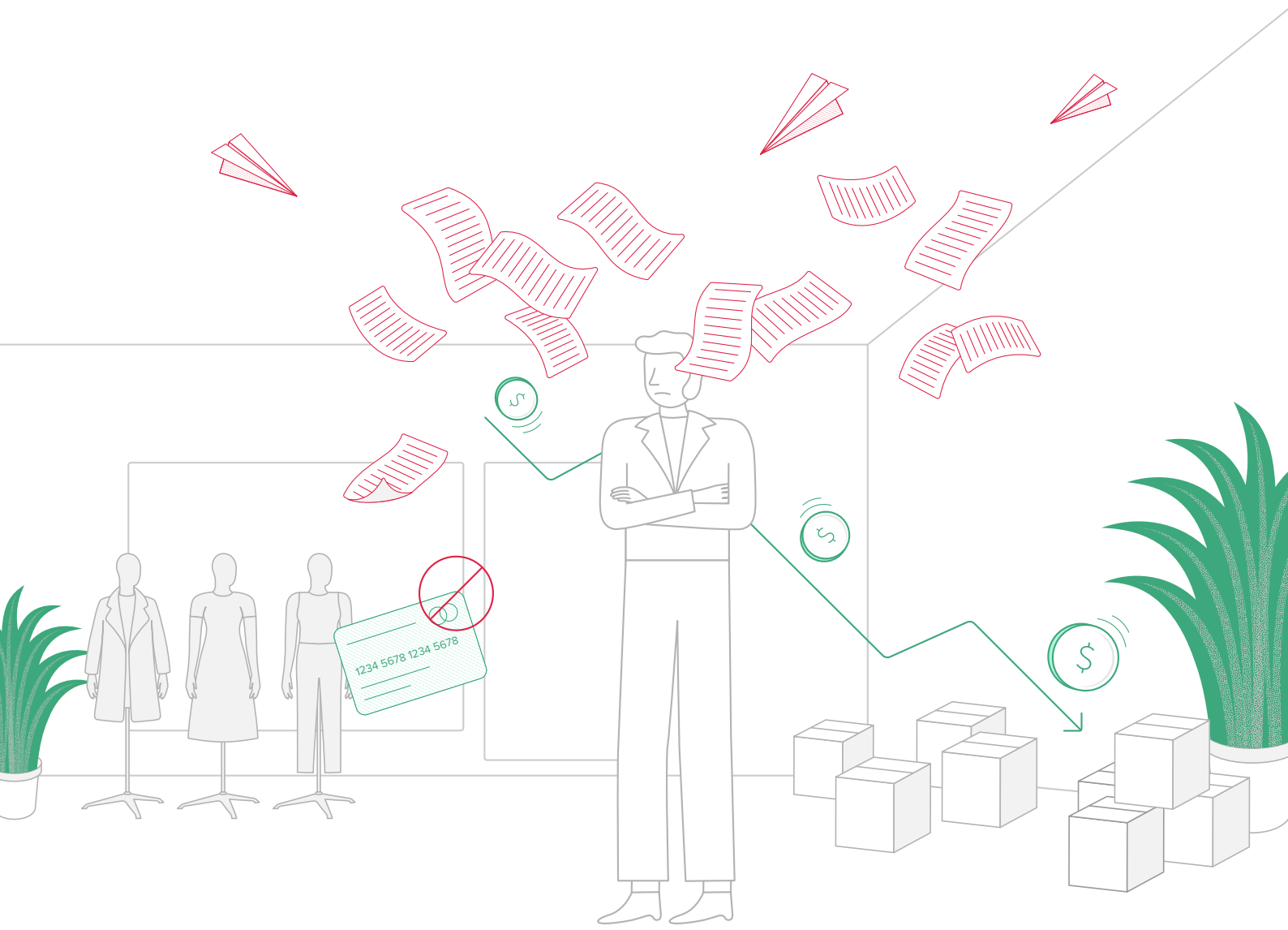
riskified

Disputing Chargebacks

A Guide for eCommerce Merchants



Introduction

In the competitive world of eCommerce, online retailers must provide an optimal customer experience or risk losing business. But many are seeing their hard-earned revenue fall victim to costly credit card chargebacks.

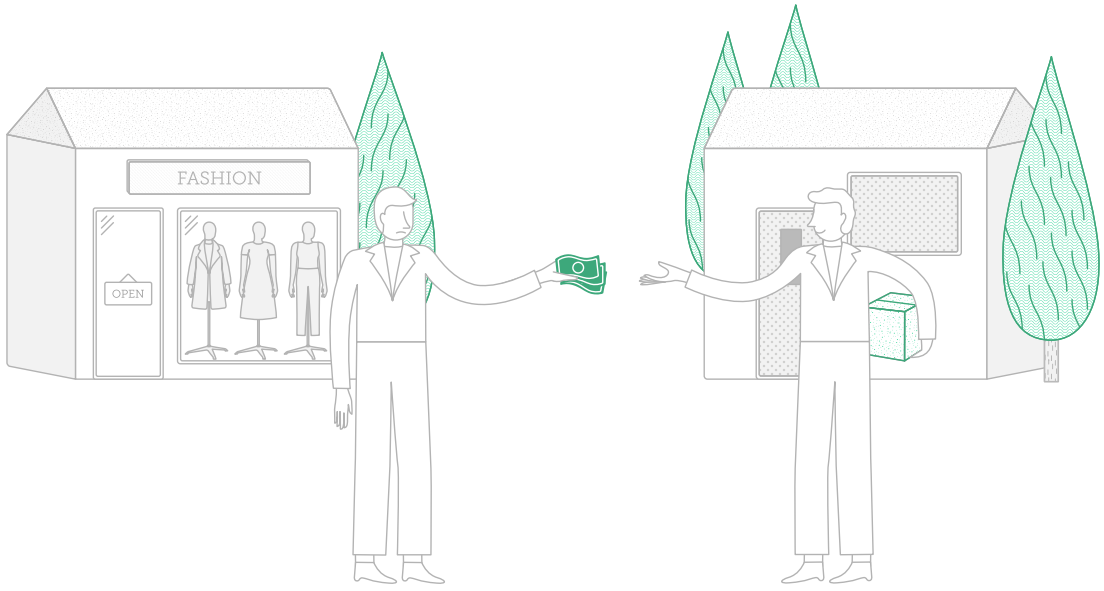
A chargeback occurs when a cardholder reports to their credit card issuer that a transaction was unauthorized or otherwise unsatisfactory, and requests a refund. When the refund is approved, the charge is forwarded to the merchant who is legally obligated to reimburse it. However, if a merchant can provide compelling evidence that the order was authorized and received by the genuine cardholder, a chargeback can be disputed.

Because any customer can file a chargeback, and issuing banks are more inclined to take the customer's side in a dispute, one of the main challenges merchants face is providing evidence to prove chargeback abuse. Issuing banks must be absolutely certain of abuse, so submitting partial evidence like screenshots of transactions from dashboards, or parcel tracking information indicating that the order reached its intended destination, generally won't suffice.

There's no doubt that the high burden of proof renders the chargeback dispute process both resource intensive and expensive. However, when streamlined and embedded in the business flow, the process can help businesses retrieve revenue they'd assumed was lost.

Riskified has extensive experience detecting CNP fraud and preventing the associated chargebacks. Our expertise extends beyond protecting eCommerce retailers from unauthorized credit card usage, to include identifying individuals taking advantage of the chargeback process. We also provide a representment service to assist our customers dispute chargebacks.

Throughout the fraud identification process, we collect a wide range of data that is also used as evidence to effectively dispute claims as part of this service. We've created this guide to assist eCommerce retailers become better acquainted with the types of information that can help them differentiate between unauthorized and authorized transactions to successfully beat chargeback abuse.



Why are chargebacks filed?

Below are some common chargeback scenarios.

An error on the merchant's end - neglecting to credit a return, ignoring a cancellation, failing to deliver the product, or a technical payment problem has occurred.

Clear cut fraud - an individual steals credit card information and makes a transaction without authorization of the cardholder. The cardholder then submits a chargeback to their issuer to recover the lost funds. Businesses must take full responsibility for approving such orders.

Unauthorized Credit Card Usage - a credit card is used to make a purchase by an unauthorized family member/friend and the cardholder subsequently submits a chargeback. We see many instances of children who use their parents' credit card to buy games online, or make an inadvertent purchase via an unlocked application on their parents' mobile device.

Chargeback abuse - an individual takes advantage of the chargeback process to claim a refund. They dispute the purchase despite having authorized and received it. The reasons generally provided for filing the chargeback are either that the transaction was unauthorized or the item not received.

In reality, their motives are different: they may be intentionally exploiting the chargeback system; they're suffering from buyer's remorse; or the purchase was made by an authorized family member and they don't want to pay for it.

This type of chargeback abuse (often referred to as 'friendly fraud' or 'liar buyer'), which is much more difficult to prevent, has increased in recent years. This is precisely why eCommerce businesses should ensure they're collecting the relevant customer data - in case evidence of the genuine cardholder authorizing the purchase is required.

What are the ramifications of too many chargebacks?

Regardless of the reason, chargebacks are a costly business. Where a merchant can't justifiably dispute a chargeback, or ultimately loses the dispute, they will lose the revenue from that sale, plus be forced to reimburse shipping costs. Even when the dispute is resolved in the merchant's favor, it is a resource intensive process that involves various fees from both the merchant's bank (the acquirer) and the issuer.

In addition, if a merchant receives too many chargebacks they risk being enrolled in an excessive chargeback program. The terms of these programs vary between issuers, and depend on the degree and persistence of high chargeback rates. But most penalties include some combination of fines, higher processing fees, and mandatory risk education programs. In some cases, merchants may even risk losing their ability to accept certain credit cards.

Merchants who procure fraud management solutions that offer chargeback guarantees need to keep a close tab on performance as well. While they're not exposed directly to chargebacks due to the built-in liability shift, their business can still suffer at the hands of an underperforming solution.

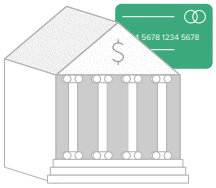
What's involved in disputing a chargeback?

The dispute process is the merchant's opportunity to refute a chargeback claim. In order to successfully argue their case, compelling evidence is required, and normally needs to be submitted a week to 10 days after the chargeback was filed. As previously stated, when the chargeback is neither the result of merchant error or criminal fraud, it's generally in the merchant's best interest to dispute the claim.

The process and reason codes vary depending on the card issuer, so it's important to familiarise yourself with their policies (links to the main credit card issuers' chargeback guides can be found on page 8).

The process can take anywhere from 6 weeks to 6 months and generally involves the following steps:

The cardholder files a chargeback

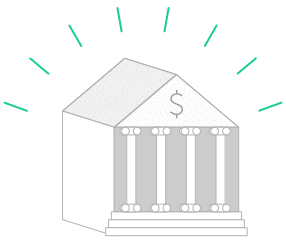


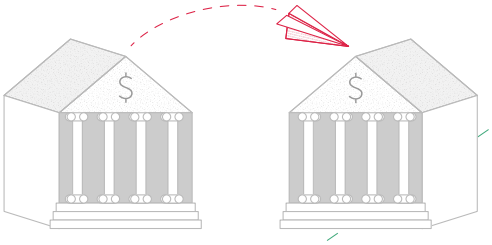
The issuing bank reviews the claim

If it's determined that the dispute may be valid, the transaction is sent to the acquirer

If the acquirer finds the chargeback to be invalid, they will decline it and inform the card issuing bank

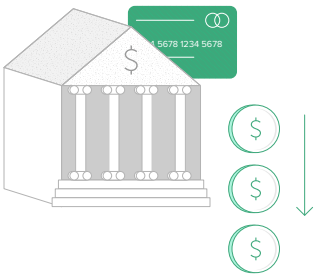
If the acquirer suspects the claim may be valid, they forward it to the merchant. The merchant investigates the claim and either accepts the chargeback or provides evidence disputing the claim





If the evidence is not compelling, the credit will eventually be taken from the acquiring bank

If the evidence is compelling (proving there's been no fraudelent activity) the issuing bank/payment provider rejects the claim and the customer will be charged for the sale



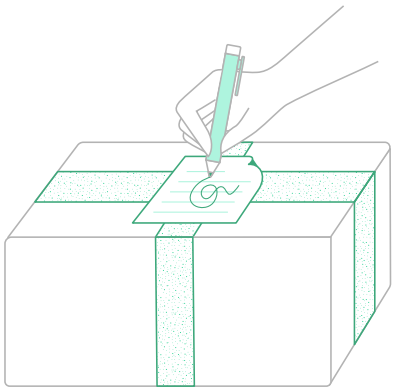
The issuer may also require industry-specific information. For example, in October 2015, Visa introduced new representment rights for chargebacks relating to airline transactions. In order to shift the liability from the acquirer to the issuer, airlines and OTAs should be able to prove that the cardholder name on the flight manifest for the departed flight, matches the cardholder name on the purchased itinerary.

What information should online merchants collect?

We have compiled a list of data merchants should collect to be prepared for chargeback disputes. The more evidence a merchant has to support the legitimacy of the transaction, the better the chances of successfully disputing a claim.

Proof of delivery

- Signed proof of delivery to the cardholder's shipping address



Customer communication

- Text message and/or email confirmation from the mobile number/email address provided in the order details
- Any other communication with the customer may also be helpful

Positive payment result

- The billing address on record with the credit card issuer matches the billing address provided at the time of purchase (positive AVS and CVV)
- Payment method previously used by customer. Purchases made with the same card and online identity that didn't result in a chargeback

Address matches

- Billing address & customer's name - the billing details provided match a public listing
- Shipping address & customer's name - the shipping details provided match a public listing
- Billing address & shipping address - a match will increase the likelihood that the purchase was made by the legitimate cardholder

Social media

- In most fraud attempts, the perpetrator and legitimate cardholder are not connected, so check to see if the customer and the recipient are friends on Facebook, connected on Google+, or seem to have any other substantial online link.

Social media can help prove cases of chargeback abuse. In a case disputed by Riskified, an individual filed a chargeback for tickets to a major sporting event, claiming the transaction was unauthorized. We subsequently found photos on facebook of the customer in the stadium, attending the event. In another similar case, a customer filed a chargeback for a pair of luxury shoes she then posted on Instagram. In both cases we successfully disputed their claims, using social media as supplementary evidence.

Email matches

- The email address is listed under the same name provided in the billing or shipping details
- The address linked to the email address matches the billing or shipping address
- The email address is linked to social profiles that match the customer's name
- The name linked to the email address matches the name of a Facebook connection of the customer

Phone matches

- The phone number's area code matches the billing address
- The billing phone number provided matches a public listing under the customer's name
- Phone is connected to social profiles listed under the customer's name

IP connection

- Connection type (standard vs. proxy)
- Proximity between the IP location (the customer's geographical location) and the billing address.
- A match between the domain of the email address and the Internet Service Provider.
- The email domain is registered under the customer's name.

Browsing data

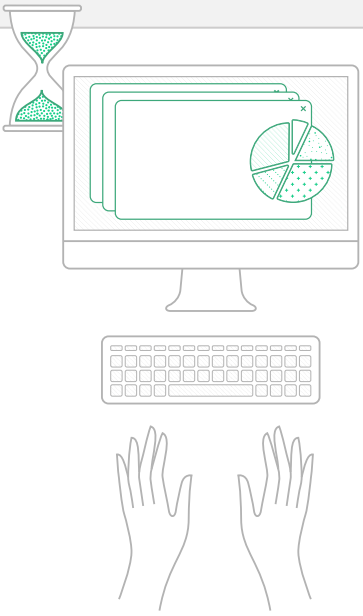
- A digital purchase was downloaded through the same device used to make the online purchase.
- The purchase was completed following a long browsing session on the website (which involves navigating via legitimate patterns).

Some fraud prevention solutions offer a storefront beacon (a snippet of code embedded on all customer-facing pages and mobile shopping apps), which records browsing patterns and helps detect such cases.

Purchase history

- Details of previous legitimate purchases with the same billing details and online identity (which were not charged back)

Riskified has the added benefit of access to customer history across merchants and verticals - data of every new order is automatically cross-referenced with data points of all previous orders across our network. So tagging cases of chargeback abuse allows us to prevent otherwise unidentifiable attempts. Merchants who aren't using a third-party fraud prevention solution should document returning customers across various channels, geographical locations, and via multiple data points across their own system.



Further information

Credit card issuer chargeback guides

- Chargeback Management Guidelines for Visa Merchants
- American Express Merchant Chargeback Guide
- Download the Mastercard Chargeback Guide

How can Riskified help?

Riskified analyzes orders submitted by online retailers for fraud. By leveraging proprietary, cutting edge technology (including machine learning, behavioural analysis, elastic linking, and device fingerprinting), we provide merchants with a fast, accurate 'approve' or 'decline' decision.

The purpose of our solution is to identify CNP fraud attempts before they turn into chargebacks. If we do approve an order that incurs a fraud-related chargeback, it is backed by a chargeback guarantee, which means the merchant is reimbursed for the order amount and any shipping costs included in the order. After reimbursement, we offer our representment service to help merchants dispute chargebacks for which we are liable.

For further information on how Riskified can help protect your online revenue from CNP fraud, including details of our 100% chargeback guarantee, visit our website. If you have specific questions about chargeback prevention and representment, feel free to contact us.