

Subscription Fraud & Chargeback Defense Checklist



Why It Matters

According to Solidgate's data, the average fraud and chargeback rate in subscription businesses ranges **from 2 to 4%** — more than double what it should be according to Visa and Mastercard thresholds.

As a result, most subscription companies we worked with suffer from numerous consequences that cripple their annual revenue, go-to-market efforts, and scaling potential:



Placement into card monitoring programs

High fraud and chargeback rates always result in placement into card monitoring programs, which means fines, lower authorization rates, and even the inability to process card payments altogether.



Being blocked from PayPal

If your fraud and chargeback rates consistently exceed 1%, PayPal will limit your account, suspend it, or block you from opening it altogether, alienating you from numerous potential customers.



Enormous fees

To illustrate: Visa charges up to \$50 per dispute, a \$25,000 audit fee for being in the monitoring program for over 5 months, and \$75,000 if you stay there for up to 12 months.



MID termination

Certain countries, products, average sales, number of transactions, and marketing practices put a merchant account at higher chargeback risk, which, in turn, can lead to MID termination within a card network.



Being listed in Match

If your MID is terminated within Visa or Mastercard, you'll be placed into a shared database Match, which can prevent you from obtaining new merchant accounts with other payment processors or acquirers.

Put simply, high fraud and chargeback rates directly affect your ability to accept payments, grow your customer base, and generate revenue.

Why is that the case?

The recurring nature of payments, trial periods, and high transaction volume from various geographies open up doors to misunderstandings and disputes. Without 1. being upfront, clear, and thorough in communication about your terms and conditions and 2. implementing advanced fraud and chargeback management mechanisms, it's a matter of time before you find yourself buried in chargebacks.

What's Inside

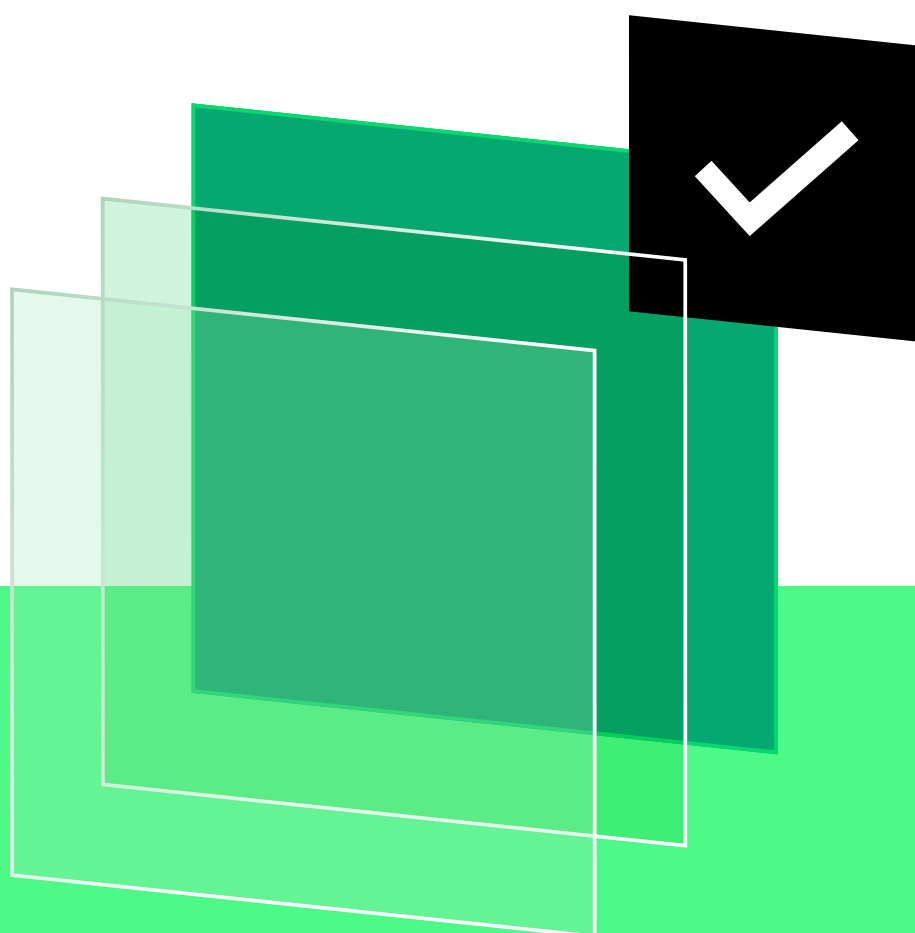
This Subscription Fraud and Chargeback Defense Checklist is your actionable, one-stop self-assessment tool for evaluating your derisk strategy and lowering your risk metrics.

The checklist is based on the Solidgate team's expertise in fraud and chargeback management, proven industry frameworks for subscription businesses, and, well, plain common sense.

Here, you'll find:

- Metrics and thresholds for Visa, Mastercard, and PayPal;
- Key customer communication requirements;
- General website requirements;
- Requirements for a subscription business model;
- Requirements for a business model with negative billing;
- Strategies for lowering fraud metrics;
- Strategies for reducing chargebacks.

Subscription Fraud & Chargeback Defense Checklist



Risk Metrics & Thresholds

Merchants with higher rates of fraud and disputes are automatically placed into monitoring programs, which leads to hefty fees and potential account termination. To avoid this scenario, let's look at the key metrics and thresholds set by Visa, Mastercard, and PayPal that you shouldn't cross.

Visa

| Metric | Threshold | Repercussions |
|--------------|------------------------------------|---|
| Fraud volume | > 0.9%, or > \$75,000 | Placement in Visa Fraud Monitoring Program (VFMP) |
| Dispute rate | > 0.9%, or > 100 disputes/month | Placement in Visa Dispute Monitoring Program (VCMP) |

Mastercard

| Metric | Threshold | Repercussions |
|-----------------------|---------------------------------------|----------------------------------|
| Fraud volume | > 0.5%, or > \$50,000 | Placement in ECM |
| Chargeback rate/count | > 1.5%, or > 100 chargebacks/month | Placement in EFM |

PayPal

| Metric | Threshold |
|-----------------|--|
| Dispute Ratio | Below 1.5% |
| Chargeback Rate | Below 0.4% |
| Dispute Fees | \$15 for resolved disputes |
| Repercussions | \$30 fees per dispute, account limitations, and potential account suspension |

Additional resources

[Visa and Mastercard monitoring programs](#)

[PayPal risk metrics](#)

Terms and Conditions communication

- ☐ Your T&C policies are available on the same website as the product/service purchase flow and are published on separate, easy-to-find website pages (linked in the footer or on the navigation panel)
- ☐ Your pricing, billing, T&C, Cancellation, and Refund Policies are written in concise, simple, and explicit language as well as in a positive tone of voice (e.g., “we’re not responsible...” - is a no-go)
- ☐ Your legal name is displayed on your Terms of Service and website pages preceding the checkout
- ☐ Your billing terms are clearly shown at checkout, including the total price, service, frequency of charges, the last four digits of the card to be used to make payments, and a link to the Cancellation Policy
- ☐ For negative option billing, you explain initial charges, trial periods, and subsequent subscription costs
- ☐ You inform users of the cancellation and refund policy and collect their consent in a disclaimer before the checkout page
- ☐ There’s no incorrect, insufficient, or misleading information about your T&C on your website or other marketing channels

Post-sale communication

- ☐ You send a transaction receipt to the customer immediately after the first and each subsequent (or recurring) charge
- ☐ Your transaction receipt includes your name, location, transaction amount and date, the purchased services, credit card details, terms, and links to Cancellation and Refund Policy
- ☐ You keep consumers in the loop by communicating their order status, promptly reporting any issues with the purchase, and proactively making sure they get what they paid for
- ☐ You make it easy for customers to cancel subscriptions online via a separate button on the website, in the user's account, or via a support email
- ☐ You timely communicate rate changes and remind clients of the next billing date in advance (ideally—seven days before the date)
- ☐ Your emails include your company name, support email, purchase details, payment information, and clear instructions on how to cancel the subscription
- ☐ Your billing descriptors allow customers to easily recognize your business by containing your domain, business name, or customer service info
- ☐ Your descriptors are between 5 and 22 characters, and avoid special characters
- ☐ You use carriers that offer online tracking and delivery confirmation
- ☐ Your billing descriptors allow customers to easily recognize your business by containing your domain, business name, or customer service info

Fraud protection & security

- ☐ You choose your target markets carefully and pay close attention to your traffic sources to avoid the influx of fraudulent transactions from high-risk locations
- ☐ If you target locations with a high level of fraud, you configure the system to require additional verification for payments from these regions while minimizing false positives
- ☐ You use an [Address Verification System \(AVS\)](#) to check the billing address listed in the transaction against the address registered with the issuing bank
- ☐ You require the CVV code to ensure the customer has physical possession of the card
- ☐ You use [3D Secure 2.0](#) or later to authenticate customer identities
- ☐ You recognize fraud-indicating red flags like in-bulk orders of the same item, especially pricey purchases, data discrepancies (like, single card and multiple addresses and vice versa)
- ☐ You closely monitor both first-time customers and repeat ones, checking the purchasing history of the latter for fraudulent behavior
- ☐ You collaborate with your payment processor to block fraudsters and accept transactions from pre-approved customers blocklists and allowlists
- ☐ You use velocity checks to flag potential fraud, based on the rate at which a buyer submits multiple transactions
- ☐ You've incorporated enhanced security checks and tools like 2-factor authentication, email links, SMS codes, captchas, fingerprinting, geolocation, IP tracking, etc.
- ☐ You keep your customers' payment data safe by never writing it down or storing it unless necessary, accessing it through secure servers, or using network tokenization and [E2EE](#)
- ☐ Your business is [PCI-DSS-compliant](#), which helps protect sensitive information while it is being stored, processed, and transmitted
- ☐ You limit the sale of digital items purchased in bulk, cap daily sales volume per cardholder, and require memberships or limit access to loyalty perks
- ☐ You collect and store all documentation required to challenge an unjust chargeback, such as sales receipts, delivery confirmations, email communications, etc.

Chargeback management solutions

- ☐ You enrolled in card network automated response programs like Consumer Clarity by Mastercard or Visa's Order Insight, which eliminate client billing confusion with enhanced transaction data in near real-time
- ☐ You leverage pre-chargeback alerts such as CDRN and Mastercard's Ethoca Issuers notices of intended chargebacks, allowing you to deflect the dispute or refund the customer before the chargeback is filed
- ☐ You use automatic dispute resolution like Visa's RDR, using transaction amount and other thresholds to quickly resolve disputes without the merchant's involvement
- ☐ You use advanced antifraud measures like Order Insight and Visa CE 3.0 to streamline dispute resolution
- ☐ You leverage analytics, tracking performance statistics and chargeback deflection per issuer, acquirer, and alert type
- ☐ You grant credits and cancellations as soon as the customer asks
- ☐ You contest illegitimate chargebacks to protect your reputation

Customer service

- ☐ You share your phone numbers, email addresses, and social media on every page of your website (in the footer), on receipts, invoices, and other communications you send to customers
- ☐ Your customer service contact information is accessible and easy to find
- ☐ You provide customer support through phone, email, or live chat, and respond promptly (up to 24 hours)
- ☐ You quickly address customer inquiries and concerns to prevent issues from escalating into chargebacks
- ☐ Your site or app functionalities work as expected, and you test new features before launch

Additional resources

[Scheme Requirements for Subscription Merchants](#)

[Website Checklist for Online Businesses](#)

Have any questions left?

Our team is always happy to answer all your questions and give advice every step of the way.

If you are a Solidgate merchant, please reach out to your account manager or our support team.

Contact support

support@solidgate.com

If you want to get started with Solidgate, contact our sales team to discuss the details.

Contact sales

sales@solidgate.com

solidgate

solidgate.com