MERCHANT e-SOLUTIONS

Powering e-Commerce Globally

# What Can I Do to **Minimize E-Commerce Chargebacks**?

Chargebacks are not going away. And now there are new rules. Selling products and services online and using credit cards for payment is a convenient and great way to maximize your sales numbers and open doors to new consumers as well as opportunities. However, as with many things, there is a downside to taking credit cards. They're called chargebacks, and as of April 16, 2011 the rules and consumer rights regarding chargebacks changed.

## What are Chargebacks?

Unlike paying with cash, issuers of credit cards support a process for the consumer to challenge a transaction charged against their credit/debit card. The issuer becomes the intermediary between the consumer and the merchant, with chargebacks being the vehicle for the challenge. Reasons for chargebacks can range from fraud, to the goods or services either not being delivered or meeting expectations. The consumer is encouraged to contact the merchant prior to initiating the chargeback process, however this process is not policed, so you may get a chargeback without ever hearing from the cardholder. The issuer has a responsibility to ensure that there is enough evidence in support of the consumer, they will start the process. Once the chargeback process starts, you, as the merchant, become responsible for proving that the consumer should pay for the goods or services.

## What has changed since April 2011?

Before April 16, 2011, a signature was typically required of a cardholder to initiate a chargeback identified as "fraud" and not having been authorized by the cardholder. Today, the cardholder is no longer required to make this attestation. Unfortunately for you, the merchant, your ability to submit a rebuttal (dispute) is now severely limited under the new chargeback rules.

## What is the Chargeback process?

Once the chargeback process is initiated by the consumer, the issuer submits the chargeback through the card brands, which is then sent to your merchant account provider. When your merchant account provider receives a chargeback, depending on your agreement with them, your depository account will be debited the chargeback amount and be charged a fee. You will be notified of the chargeback by an online report, email, letter or fax.

Depending on the chargeback type, you will have a defined number of days to respond to the merchant account provider. The time-frame is included in the chargeback notification you receive. If you choose to rebut the chargeback, you will need to provide evidence about the transaction. The merchant account provider will then process the rebuttal documentation and verify that you have enough information to support the challenge to the chargeback. If you do, then a “representment” is created by the merchant account provider, and is sent to the card issuer. At the same time, depending on your agreement with your merchant account provider, you may receive a provisional credit for the transaction amount. The chargeback fee, however, usually remains.

You may win the chargeback process at this point, however the issuing bank can rebut the chargeback representment. If they do so, once the second presentment chargeback is received, your depository account will be debited the chargeback amount. Once again, depending on your agreement with the merchant account provider, you may be charged another fee. To rebut a second presentment chargeback is expensive for all parties. An arbitration process is initiated, and you will need to work with your merchant account provider to make sure that the costs are worth it, and there is a reasonable chance of winning. The arbitration process is the last stage in the chargeback process.

## How much do Chargebacks cost?

As a Card-Not-Present, e-Commerce merchant, you are financially responsible for fraudulent or other transactions charged back to your business, even if the transaction was previously authorized by the issuer. The burden to defend the transaction is with you, the merchant, due to the online nature of the transaction and the absence of a card to swipe and a customer signature.

By the time a chargeback occurs, you are faced with a narrower profit margin for the sale, plus any extra processing time and cost, as well as the possibility of the complete loss of the transaction revenue.

## What role does the Merchant Account Provider play?

Your merchant account provider is responsible for managing and notifying you about chargebacks in a reasonable amount of time. Chargebacks are time-sensitive and understanding how long you have to respond is the key to effectively managing chargebacks.

The merchant account provider is also responsible for representing your chargeback rebuttal documentation to the card issuer. Each merchant account provider has a team of employees that work on your behalf to ensure that you have provided enough documentation to allow a reasonable outcome in the chargeback process. Part of your selection process of a merchant account provider should be to understand how receptive they are to assisting you in this process.

## How do I protect myself against Chargebacks?

- **Educate** yourself on ways to use all possible tools available in the taking of transactions as well as prevent chargebacks, and also on your rebuttal rights.
- **Decide** which prevention methods will help you prevent and manage chargebacks most effectively.
- **Implement** the chargeback prevention and management tools.
- **Always** take steps to recover losses from a customer that has issued a chargeback against you. However once a chargeback has been initiated it does not benefit you to issue a credit as it is possible for both the credit and the chargeback refund to post to the cardholders account.

## How can I help to prevent Chargebacks?

1. **Become informed and train your staff**
   - **Understand your direct responsibility** for preventing chargebacks.
   - **Respond to Retrieval Requests** – these are requests for copies of Sales Drafts. Failure to respond will result in a chargeback that does not provide you the ability to submit rebuttal.
   - **Develop a thorough understanding** of various reasons for chargebacks.
   - **Know your rights** to resubmit transactions that have been charged back to your business for fraud-related reasons.
   - **Use Verified by Visa, MasterCard SecureCode and American Express Card Identification** digits to reduce the chance of chargeback risk exposure.
   - **Train your employees** in e-business risk and chargeback management.
   - **Know your liability** for data security problems.
2. **Build internal Chargeback controls**
   - **Establish** internal chargeback and fraud control functions and track performance.
   - **Develop and maintain** an internal negative file and use it to screen transactions. Once a chargeback has been issued, have your system block that card from further uses.
   - **Create** velocity limits based upon transaction risk.
   - **Verify a card's authenticity** by implementing and using CVV2 (Visa), CVC (MasterCard) and CID (American Express) to establish card authenticity.
3. **Implement Card Level Fraud and Chargeback Prevention**

   To help reduce Fraud and chargebacks, the card brands: MasterCard, Visa, Discover and American Express have implemented fraud prevention techniques for their cards.

   - **Address Verification (AVS) of the Cardholder's Address**
     Implement the use of AVS to verify the cardholder's billing address. An

AVS request with a transaction authorization will; a) receive a result code indicating whether the address in the card issuer's file is a full, partial or no match, b) research all AVS "partial and non-matches," and c) ensure the AVS response is incorporated into the risk scores that may be used or into the decision of whether to accept an order or not. When you choose to ship to an AVS-matched address and request a signature upon delivery, your chargeback rights improve significantly.

- **Card Authenticity – The Consumer has the card to hand**
  Card Authenticity helps validate the consumer entering the credit card data has the actual card at hand.

  **CVV2 (Visa)** – A three-digit security code printed on the back of Visa cards to help validate that a legitimate card is in the possession of the person placing the order.

  **CVC (MasterCard)** – A three-digit unique security code on the back of a MasterCard card that validates that a legitimate card is in the possession of the person placing the order.

  **CID (American Express)** – A four-digit number that appears on the front of the card above the American Express card number and helps verify that it is a legitimate card.

  **CID (Discover)** – A three-digit number that appears on the back of the card in the signature panel to the right of the card number and helps verify that it is a legitimate card.

**TIP: Merchants should require the entry of a CVV, CVC or CID number by the consumer during all online transactions. Note that it is a violation of card association security standards to store these numbers.**

- **Implement Cardholder Verification, Verified by Visa (VbV) and MasterCard SecureCode,** to avoid "cardholder unauthorized" or "cardholder not recognized" chargebacks by working with your merchant account provider. There are online real-time services that enable cardholders to authenticate themselves through a personal code known only by them and the card issuer. Implementation requires the addition of an in-line window prompting the cardholder to enter their unique personal code. The code is then verified by the issuer of the card.

**TIPS:**

- **Ask consumers** for both the payment type and card account number for matching purposes.
- **Require consumers** to enter an expiration date from a pull-down window and establish transaction data fields and require the consumer to complete them.
- **Never complete** a transaction if the authorization request was declined nor attempt to re-run the transaction on the same card account number.
- **Act quickly** when consumer with a valid dispute requests a refund or credit.
- **Know your representment rights** for transactions with AVS, CVV2, CVC and CID and track all chargebacks and representments by reason code.
- **Contact your merchant account provider** with any report of suspicious activity.

4. **Build external Chargeback controls and provide essential website content for products, shipping and delivery, billing and customer service.**

- **Build Consumer confidence** – In today's e-commerce environment, earning your customers' trust is essential in maintaining a successful online business. So be upfront and clear with consumers about your company's policies and practices – especially regarding billing, shipping and refunds. This will help you avoid any consumer disputes, reduce expenses and strengthen your profitability.
- **Product Description** – Describe your goods and services thoroughly on your website. Develop clear and concise descriptions (images and photos) to avoid disputes when the product is received by the consumer.
- **Order Fulfillment Information** – Clearly state time-frames for order processing and always send email confirmation and an order summary within one business day. Inform the consumer at once of current stock information when a product is not available. The consumer should receive an automatic email to confirm the purchase immediately following transaction with all order content listed, ship date, shipping tracking information and customer service contact included. This will test the validity of the consumer's email address by sending the order details and confirming the order content. Have a mechanism to hold an order if you receive a bad email address response. This does not mean the order is bad, but you may want to do some further checking before fulfilling the order.
- **Delivery Policy** – Develop and clearly state any product or service delivery policies and any restrictions on your website. Create comprehensive shipping policy information and make it clearly available. Develop an email response process to inform consumers of any delivery delays. (You must state your refund policy right next to where the cardholder selects an "Accept or I Agree" button.)

- **Billing Practices** – Provide full disclosure of your billing practices, terms and conditions and post them for the consumer at the time of the online purchase. Merchants selling hard goods can obtain payment authorization at the time of order but cannot charge the consumer's payment card for purchases until goods are shipped. Payments for soft goods can be authorized and settled on the same day. Provide a merchant descriptor that consumers will recognize that matches the goods or services they purchased to avoid confusion when receiving their monthly credit card statement. Describe thoroughly when the consumer's payment card will be charged or alternative payment services will be billed on the various types of bankcard or billing statements. Be sure there is consistency between the name of your online business and the name of the business that will appear on the consumer's statements. Ask consumers to retain a copy of the transaction to reduce any uncertainty when their monthly statement arrives.

- **Refunds or Credits** – Develop and display a clear statement of your refund and credit policy. Be certain that the statement is available with visible links and click through confirmation for important elements and details. Include a button to Accept or Agree for consumer acknowledgment. Customer service access should include a toll free number that is available with extended hours seven days a week. Merchants should include an email address for customer questions.
- **Digital Content Policies** – Create and specify terms that state a consumer's payment selection will not be billed until the website services are actually accessed via an applicable password. Ensure that all terms and conditions are clear and concise. Before the sale is conducted, clearly communicate any special restrictions to the consumer. Avoid the use of false expectations such as stating that products or services are "free" if they are not.

- **Recurring Transaction Processing** – Clearly display your recurring transaction disclosure policies, how much you are billing, duration of time and what the consumer does to cancel. Require click and accept to confirm. Make sure that the email receipt for an initial recurring transaction contains essential details including the frequency of debits, the period of time that the consumer has agreed to the debits and all the cancellation details. Keep this record on file for the duration of the recurring payment arrangement. Visa and MasterCard allow internet merchants to accept an electronic record with an email message as the consumer's permission to set up a recurring transaction. Consider sending an email at the time of or prior to each recurring transaction to keep the consumer in the loop and prevent misunderstandings that can lead to chargebacks.
- **Require Transaction Data Fields** – Establish transaction data fields that can help you detect risky situations and require the customer to complete those fields.
    - **Demographic information** – Telephone number, name and billing address, shipping name and address.
    - **Cardholder Verification Value** 2 (CVV2) Visa, MasterCard (CVC), American Express (CID) and Discover (CID).
- **Avoid Duplicated Numbers** – Develop controls to help consumers avoid submitting a transaction more than once. Require the consumer to make positive clicks on order selections and then send an email message to confirm the order.
- **Implement Risk Management Rules and Screen High-Risk Transactions** – Take advantage of industry available fraud prevention products that will help manage risk and implement screening tools to identify high-risk transactions, for example a higher than normal dollar amount and require a shipping address to match a billing address.

**Check for:**

- Matched data stored in your internal negative files.
- Exceeded velocity limits and controls.
- Generate an Address Verification Service mismatch.
- Transaction source and treat non-US transactions as higher risk. Use greater scrutiny and verification for international transactions.

**Analyze Questionable Transactions** – Be alert for certain characteristics that include: larger than normal orders, big ticket items, request for shipment to be rushed or overnight delivery, orders shipped internationally, orders shipped to the same address using different cards, multiple transactions with one card over a very short period of time, and multiple cards used from a single IP address.

- **Customer Service Access** – Offer excellent customer service support.
  1. Display local and toll-free telephone numbers on your website and include the hours of availability with extended hours – preferably, 7 days per week.
  2. Have your toll-free number printed on your consumers' bank and card statements along with the name of your online business.
  3. Upon shipping immediately send the consumer a shipping notification along with the shipment tracking number.
  4. Provide an email inquiry option for questions or concerns about the online purchase and include an email inquiry response policy (such as how quickly your business will respond).
  5. Establish email inquiry response standards for your staff, making it clear what the standard time response goals are for your business and monitoring those goals daily to confirm the response times are being met.

### Reminders – To implement solid practices to reduce Chargebacks, you should:

- Highlight required data fields and establish transaction data fields that can help you detect risky or potential chargeback situations, then require the consumer to complete those fields.
- Develop controls to prevent duplicate transactions.
- Display only the last four digits when showing a card number to a repeat consumer.
- Check the validity of the consumer's phone number, physical address and email address.
- Obtain an authorization number for the full amount of the sale – do not break the sale into several smaller amounts.

- When setting up recurring transactions by email, start by send pre-notification emails for recurring billing cycles, then keep a record on file for the duration of the arrangement.
- Put proper controls in place to protect any stored cardholder information related to the transaction. That means **never store CVV2 (Visa), CVC (MasterCard), CID (American Express) data.**
- Request the consumers account number only as payment for goods and services.
- Check customer logs daily for complaints, cancellations and non-renewal, especially when related to any transaction amounts or failure to notify consumers in advance of recurring transactions that exceeds authorized amounts.
- Always provide the consumer with a cancellation number.

Be aware that Visa and MasterCard have programs to identify and reduce merchants with a high percentage of chargebacks to sales. Businesses with marketing practices that may be deemed as deceptive may face high fines each month they are listed as well as the possibility of termination plus listing on the Card Associations Negative File.

**Choose your merchant account provider wisely. Choose the one that will support ALL of your transaction processing needs.**

## About Merchant e-Solutions:

Merchant e-Solutions, founded in 1999, provides Internet-based payment processing solutions for merchants and banks. Merchant e-Solutions currently processes more than $14 billion dollars in payments for more than 70,000 merchants, supporting 150 global currencies and all major credit, debit and alternative payment solutions.

The company specializes in services for e-commerce and card-not-present merchants and provides a comprehensive suite of payment solutions that are PCI compliant and designed to reduce merchant risk exposure. Merchant e-Solutions is headquartered in Redwood City, CA with operations in Spokane, WA and satellite offices in Minneapolis, MN and Columbus, GA.

For more information, go to http://www.merchante-solutions.com or contact **(866) 663-6132**