Chargebacks Can Be Costly! Card-not-Present, e-Commerce merchants are financially responsible for charged back or fraudulent transactions, even if the transaction was approved by the issuer. The burden to defend the transaction is with the merchant due to the online absence of a card to swipe and a signature. A chargeback translates into a narrower profit margin for the sale, extra processing time and cost with the possibility of the complete loss of revenue. Merchants should know their re-presentation rights and always take steps to recover losses from consumers.

To minimize chargeback exposure, see suggestions below

**Chargeback Controls**

**Become Informed and Train Your Staff**

- Understand your direct responsibility for preventing chargebacks
- 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 Card Authenticity mechanisms 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

**How to Build Internal Chargeback Controls**

- Establish internal chargeback and fraud control functions and track performance
- Develop and maintain an internal negative file and use 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)

- **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. Ask for the last three numbers that appear in or beside the signature area on the back of Visa cards.

- **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. Ask for the last three numbers that appear in or beside the signature area on the back of MasterCard cards.

- **CID (American Express)** – CID (card identification digits) A 4-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. Ask for the four digit number on the front above the full 15 digit card number.

Avoid “cardholder unauthorized or cardholder not recognized” chargebacks by working with Merchant e-Solutions to implement Verified by Visa (VbV) and MasterCard SecureCode.

These are online real-time services that enable cardholders to authenticate themselves through a personal code. Add an in-line window prompting the cardholder to enter their unique personal code. It is then verified by the issuer of the card for validation. A successful authentication will help shift the chargeback liability from the merchant to the issuing bank for the following chargeback reason codes:

<table>
<thead>
<tr>
<th>Quick Tip</th>
</tr>
</thead>
<tbody>
<tr>
<td>✔ 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 this information.</td>
</tr>
</tbody>
</table>

What is? – Card Authenticity

Cardholder Verification

What is? – Verified by Visa/ MasterCard SecureCode
What is? – AVS (Address Verification)

Implement AVS to verify the cardholder’s billing address (street number and ZIP code) for electronic authorization. An AVS request with a transaction authorization will receive a result code indicating whether the address in the card issuer’s file is a full, partial or no match – research all AVS “partial matches” – ensure that AVS response is incorporated into the risk scores that may be used. Do not accept any transaction that has been declined regardless of AVS response.

Quick Tips

Merchants should:

✔ 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. Act quickly when a consumer with a valid dispute requests a refund or credit.

✔ Know your re-presentment rights for transactions with AVS, CVV2, CVC and CID and track all chargebacks and re-presentments by reason code.

✔ Contact Merchant e-Solutions with any report of suspicious activity.

Visa – 23: Invalid T & E, 83: Fraudulent MOTO/e-Commerce, 75: Cardholder does not recognize

MasterCard – 37: Non cardholder authorization, 63: Cardholder does not recognize, 49: Questionable merchant activity

These reason codes typically make up 70% of a merchants chargebacks.
Provide Essential Website Content for Products, Shipping and Delivery, Billing and Customer Service

Building consumer confidence is essential in today’s e-commerce environment for a successful online business. Give the consumer all the basics about your company operations – especially when it comes to product descriptions, policies regarding billing, shipping and refunds. This will help you avoid any consumer disputes, reduce expenses and increase 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 e-mail 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 e-mail response process to inform consumers of any delivery delays.

**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 acknowledgement. Customer service access should include a toll free number that is available with extended hours seven days a week. Merchants should also include an email address for customer questions.

**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 consumers bank or card statement 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 e-mail inquiry option for questions or concerns about the online purchase and include an e-mail inquiry response policy (such as how quickly your business will respond)
5. Establish e-mail inquiry response standards for your staff – make it clear what the standard time response goals are for your business and monitor them daily to confirm the response times are being met

**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 e-mail 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 allows 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 each recurring transaction to keep the consumer in the loop and prevent misunderstandings that can lead to chargebacks.

Remember to:

- Check customer logs daily for complaints, especially those relating to transaction amounts or failure to notify consumers in advance of a recurring transaction that exceeds the pre-authorized amount range
- Review customer logs daily for cancellation or non-renewal of services so that you do not process a recurring payment when the pre-established time frame has expired
- Process all recurring transaction cancellations credits promptly
- Provide the consumer with a cancellation number
- Consider sending monthly recurring transaction statements to keep consumers in the loop and remind them of the payment

Require Transaction Data Fields – Establish transaction data fields that can help you detect risky situation 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) and American Express (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.
**Screening High-Risk Transactions** – Implement screening tools to identify high-risk transactions and require a shipping address to match a billing address for higher risk transactions. 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, multiple cards used from a single IP address.
## Implement Solid Practices to Reduce Chargebacks

<table>
<thead>
<tr>
<th>QUICK TIPS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Merchants should:</td>
</tr>
<tr>
<td>✔ Highlight required data fields and establish transaction data fields that can help you detect risky or potential chargeback situations - Require the consumer to complete those fields.</td>
</tr>
<tr>
<td>✔ Develop controls to prevent duplicate transactions.</td>
</tr>
<tr>
<td>✔ Check the validity of the consumer’s phone number, physical address and e-mail address.</td>
</tr>
<tr>
<td>✔ Obtain an authorization number for the full amount of the sale – do not break the sale into several smaller amounts.</td>
</tr>
<tr>
<td>✔ When setting up recurring transactions by e-mail, keep a record on file for the duration of the arrangement – Send pre-notification e-mails for recurring billing cycles.</td>
</tr>
<tr>
<td>✔ Put proper controls in place to protect any stored cardholder information related to the transaction – <strong>never store CVV2 (Visa), CVC (MasterCard), CID (American Express) data.</strong></td>
</tr>
<tr>
<td>✔ Check customer logs daily for complaints, cancellations, 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.</td>
</tr>
</tbody>
</table>