

Best Practices to Minimize Copy Requests continued from front page



occurs, the transaction may be returned to you as a chargeback for an illegible copy, and unless you can improve the readability of the receipt, you may take a loss on the transaction.

Merchant Support Center

We're here to assist you with all your merchant needs. Commerce Bank Customer Service Representatives are available to help you with:

- Processing
- Service Questions
- Supplies
- Statement Questions

We offer personalized service through our in-house Support Center at: 1-800-828-1629 Monday-Friday: 8 a.m. to 6 p.m. and Saturday 9 a.m. to 1 p.m. (CST). Fax us at: 1-816-234-2181.

For faster service, have your merchant number ready when you call the Merchant Support Center.

Telephone authorizations: 1-800-228-1122.
Call 24 hours a day, seven days a week.

Write us at:

Commerce Bank
Merchant Department
825 Main Street, KCBC-1
Kansas City, MO 64105

We're always at your service.

This publication does not constitute legal, accounting or other professional advice. Although it is intended to be accurate, neither the publisher nor any other party assumes liability for loss or damage due to reliance on this material.

Entire publication © Commerce Bancshares, Inc. 2005. All rights reserved. ask listen solve and call click come by are trademarks of Commerce Bancshares, Inc.

Commercebank.com



call



click



come by

Printer cartridge should be changed routinely. Faded, barely-visible ink on receipts is the top cause of illegible receipt copies. Check the clarity on all printers daily, and make sure the printing is clear and dark on every sales draft.

Change point-of-sale printer paper when the colored streak first appears. The colored streak down the center or the edges of printer paper diminishes the legibility of printed information.

Keep the white copy of the transaction receipt. If your receipts include a white original and a colored copy, give customers the colored copy of the receipt. Colored paper does not photocopy as clearly as white paper, and often results in illegible copies.

Handle carbon-backed, silver-backed, or carbonless paper carefully. Silver-backed paper appears black when copied. Any pressure on carbon-backed or carbonless paper causes black blotches, making copies illegible.

Provide Adequate Training for Your Sales Staff

Your sales associates can be your greatest allies. Help them to understand the importance of following proper procedures at the point of sale. Key points of instruction should be:

- ✓ Review each transaction receipt for accuracy and completeness.
- ✓ Ensure the transaction receipt is readable.
- ✓ Give the cardholder the customer copy of the transaction receipt, and keep the original, signed copy.

Copy requests can be kept to a minimum by establishing and following these simple guidelines. Contact our Merchant Support Center if you have any questions.

ask listen solve



Best Practices to Minimize Copy Requests

Merchants who keep copy requests to a minimum are less likely to incur chargebacks. Here are a few ways to minimize copy requests and boost your profitability.

Confirm that Your Business Name is Recognizable on Your Customers' Bills

Cardholders must be able to look at their bank statements or credit card bills and recognize transactions that occurred at your establishment. Check with our Merchant Support Center to be sure it has your correct "Doing Business As" (DBA) name, city, and state. You can check this information yourself by purchasing an item on your credit or debit card at each of your locations and then checking how the merchant name and location appear on your monthly card statement. Is your name recognizable? Can your customers identify the transactions made at your establishment?



Ensure that Your Business Name Is Legible on Receipts

Make sure your company's name is accurately and legibly printed on transaction receipts. The location, size, or color of this information should not interfere with transaction detail. Similarly, you should make sure that any company logos or marketing messages on receipts are positioned away from transaction information.

Legibility of transaction receipts is key to minimizing copy requests and chargebacks. If you do receive a copy request, you will usually photocopy or scan the receipt before mailing or electronically sending it to our Merchant Support Center. If the receipt is not legible to begin with, the copy that we receive and then send to the card issuer may not be useful in resolving the cardholder's question. If this

Inside

Combating Online Fraud	2
The Authorization Cycle	3
Critical Security Issues	3

Identifying and Combatting Online Fraud

Look for signs of high-risk transactions, and help prevent costly chargebacks

Online merchants must learn to recognize the warning signs of fraud in order to effectively protect themselves. Even with the sophisticated technology available, vigilance and common sense can be your greatest ally.

What To Look For

While the following situations can exist in a normal transaction, here are some of the most common characteristics of fraudulent transactions:

- Larger-than-normal orders — Stolen cards have a limited life span, and many criminals will maximize their fraudulent transactions. Review all orders that exceed a pre-determined dollar amount.
- Orders for multiple quantities of the same item — This is the time to ask yourself: would a person normally buy a large quantity of this item?
- International orders — In recent years a tremendous amount of fraudulent activity has originated from Nigeria, Indonesia and Eastern Europe.
- “Rush” or “overnight” orders — Most consumers won’t pay for overnight delivery except at gift-giving times.
- Multiple purchases from same Internet address on the same day; orders shipped to a single address but made on several different cards; or transactions on one card with multiple shipping addresses.
- High-priced, easily resalable products — electronics, jewelry and event tickets are hot items for Internet fraudsters.

What You Can Do

It’s a delicate balance, taking the time and resources to practice fraud-prevention methods, while at the same time processing Internet transactions rapidly and cost-effectively.

Here are some best practices that should be standard procedure for all online merchants.



Your staff should be made aware of the latest fraud schemes, and be well trained in fraud prevention.

- ✓ Obtain an authorization — An electronic authorization, while not foolproof, will show if a card has been reported lost or stolen.
- ✓ Use Address Verification System — This system compares the billing and shipping addresses provided by your customer with the database of the card-issuing bank (U.S. addresses only!) The response code returned by the system will tell you if the information matches the info on file with the bank.
- ✓ CVC2/CVV2 verification — This three-digit code, (four digits on American Express Cards) is unique to each card, and is not a part of the account number. If a criminal only has a card number and not the actual card, they will probably not have the code. It has been suggested that merchants who request the CVC2/CVV2 may deter fraud simply by asking for it.

Contact our Merchant Support Center if you have any questions about identifying and preventing fraud in your online transactions.

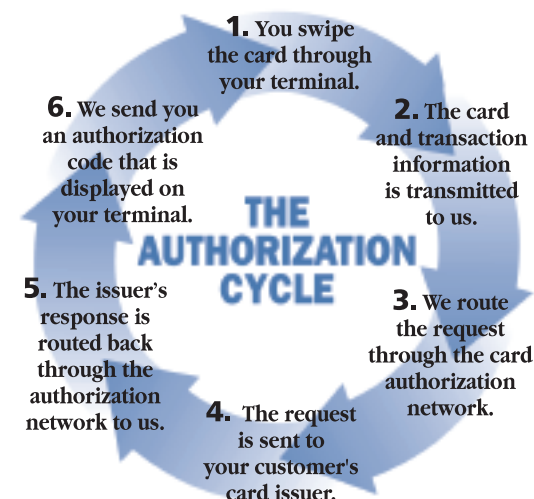
A Behind-the-Scenes Look at Authorizations

It may seem like magic. You swipe the card, and a few seconds later you receive an authorization. What you may not realize is, in that brief time, three different organizations usually have to review the transaction before it can be authorized.

This chart shows a closer look at what happens behind the scenes when you swipe a card for an electronic authorization.

Authorizations protect your profits

The information stored on the card’s magnetic stripe is compared to a database containing millions of records. Most transactions are approved, but if a transaction is questionable you will get a response telling you to call your authorization center because more information is needed before an autho-



zation can be issued. If a card has been reported lost or stolen, the transaction will be declined and you may be asked to keep the card. Call our Merchant Support Center if you have any questions.

Data Security in the Global Marketplace

KEEPING YOU UP TO DATE ON CRITICAL SECURITY ISSUES

At Commerce Bank we want you to be armed with the tools you need to fight fraud and increase your profits. Look for this feature in every issue to learn the latest trends in data security and fraud prevention.

Developing your own Data Security & Privacy Plans

Perform a **Security and Privacy Reality Check** by answering these questions about your business.

- ✓ Do you transact business over the Internet?
- ✓ Do you collect customer information — names, addresses, phone numbers, SSNs?
- ✓ Do you accept credit cards?
- ✓ Do you share customer information?

- ✓ Do you engage in direct mail marketing?
- ✓ Do you store customer information for ANY period of time?

If you answered “YES” to any of these questions, your business is in serious need of a data security and privacy plan.

Find your weak spots

1. List all of the ways information is handled.
2. Train personnel that have contact with sensitive information.
3. Review your policies on a regular basis.

Contact our Merchant Support Center for more information about the Payment Card Industry Data Standard and compliance requirements. We’re here to help.