



Merchant *On-line*

Winter 2009

Exclusively for Commerce Bank Merchants

Be Sure Customers Know Your Return Policy

Good communication at the time of sale facilitates returns and exchanges

This is the time of year when you will be faced with lots of returns and exchanges. There will be customers who don't have receipts, people who want to exchange for a different item, and those who just want their money back.

MasterCard and Visa Regulations

The major card associations have strict policies regarding returns and exchanges on credit card transactions. Here are the basics:

- ▲ Never refund cash on a credit transaction. If it's simply a return, you must issue a credit to the account to which the original sale was charged.
- ▲ If the customer wants to exchange for something more expensive than the original item, you should complete a transaction for the difference in price. When the new item costs less than the original item, credit the price difference to the card that was used for the original sale.



Post a Return and Exchange Policy

If you're a brick-and-mortar merchant, display your Return and Exchange policy at the point of sale. Have your terminal set up so that your policy is printed on your receipts. Mail order merchants are required to disclose their policy on the mail order form, invoice or contract.

E-commerce merchants must communicate their refund policy during the ordering process, and require customers to accept it.

Use Gift Cards as In-Store Credit

After the holidays, it is understandable that customers may not have a receipt for a gift. By issuing a gift card in the amount of the return, you can save the sale and maybe even end up with a new customer. If you handle returns and exchanges smoothly, customers will remember your good service and may return.

Inside

Identifying and Combatting Fraud	2
Meet Jeffrey Koelling	2
PCI Releases version 1.2 of PCI DSS	3
Commerce Bank Visa® Gift Cards	3
Prevent Skimming and Keystroke Logging ...	4

Identifying and Combatting Fraud

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

What To Look For

Here are some of the most common characteristics of fraudulent transactions:

- ✓ Larger-than-normal orders — Stolen cards have a limited lifespan, and many criminals will maximize their fraudulent transactions.
- ✓ 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 the 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.

What You Can Do

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

- ✓ Obtain an authorization — Although an authorization does not guarantee payment, it 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. If a criminal only has a card number and not the actual card, then merchants may deter fraud simply by asking for this number.

Contact our Merchant Client Support Center at 1-800-828-1629 if you have questions about preventing fraud in your transactions.

Getting to Know Commerce Bank

Meet Jeffrey Koelling, Senior Business Systems Analyst



“Our team welcomes any challenge”

Jeffrey Koelling sees the most important part of his job as the support he provides to the sales, client support and relationship teams.

In his 3¹/₂ years with Commerce Bank, Jeffrey’s work has ranged from assisting clients in achieving optimal interchange qualification to helping

merchants become compliant with Payment Card Industry Data Security Standard (PCI DSS), as well as finding solutions that will provide the best credit card acceptance experience.

Jeffrey’s prior work experience prepared him for his current position within Commerce Bank. He was responsible for the installation of credit card terminals and software for merchants, as well as training merchants on how to use them. Additionally, Jeffrey managed PCI DSS compliance for merchants and service providers.

The people he assists on a daily basis, whether internal or external, make Jeffrey’s job enjoyable. He is backed up by strong leadership that helps give him the knowledge to get the job done.

Data Security in the Global Marketplace

PCI Releases Version 1.2 of PCI Data Security Standard

The PCI Security Standards Council has announced general availability of version 1.2 of the PCI DSS. Version 1.2 is effective immediately and Version 1.1 of the standard will expire on December 31, 2008. This latest version is the culmination of two years of feedback and suggestions from industry stakeholders, including retailers, security product vendors, electronic funds transfer networks, point-of-sale application developers and banks.

Version 1.2 includes clarifications and explanations of the requirements that improve flexibility to meet today's security challenges and ensure organizations can adequately comply with the standard.

While Version 1.2 does not introduce any new major requirements to the existing

12 requirements in place since the Council's inception, the updates do change some practices, such as the sun-setting of implementations of Wired Equivalent Privacy (WEP) wireless security by June, 2010.

Risk Profiler

TrustWave's Risk Profiler is an easy-to-use risk assessment tool that will help you comply with PCI DSS, as well as discover your level of security against theft and fraud. TrustWave is a leading third-party assessor and an authorized Qualified Data Security Company (QDSC) for both VISA and MasterCard. Please visit www.trustwave.com for additional information.

Press Release. "PCI Security Standards Council to Release Version 1.2 of the PCI Data Security Standard in October 2008," PCI Security Standards Council, May 14, 2008.

Visit www.commercebank.com/datasecurity to learn more about PCI compliance.

Incentive and Employee Recognition Options

Use Commerce Visa® Gift Cards for your 2009 incentives and employee recognition

When planning for employee incentives, recognitions or gifts, don't limit yourself to the traditional items; enhance your giving with a Commerce Visa Gift Card! Order as many as you need, loaded with any whole-dollar amount from \$25 to \$1,000. Each card will cost you only \$4.99.



Ease of ordering

Commerce Visa Gift Cards can be ordered online and delivered to your office. Visit commercebank.com and visit our Gift Card section. Select from many available payment options.

Occasions for Gift Card Giving

- ▲ Bonuses
- ▲ Employee Recognition
- ▲ Incentives and Rewards
- ▲ Awards and Appreciation
- ▲ Service Anniversaries and Retirement Gifts

To learn more about the Commerce Visa Gift Card, contact Tina Tubwell at Tina.Tubwell@commercebank.com or giftcard@commercebank.com or by phone at 816-234-2150.

Knowing Your Point-of-Sale Hardware Can Help Prevent Fraud

Advanced technology and inexpensive hardware continue to give criminals new ways of stealing cardholder data. Merchants need to be increasingly vigilant in helping to protect their customers' card information. Two card fraud methods currently impacting merchants are skimming and keystroke logging.

Skimming

Skimming is a form of card fraud and identity theft in which a card's magnetic stripe data is captured by swiping a legitimate card through a small hand-held device about the size of a pager. Inexpensive skimming devices can be acquired easily on the Internet.



A skimming device is shown here from several different angles.

Keystroke Logging

Keystroke logging is a method of capturing and recording computer user keystrokes. Criminals use key logging devices to potentially capture usernames, passwords, driver's license numbers, credit card numbers and other confidential

information. These PS2 or USB devices plug in between the keyboard and the computer, logging all keystroke activity to a small device that can easily blend in with the rest of the computer.



Keystroke logging devices are shown above.

Recommendations from the experts to help protect you and your customers

- ▲ Familiarize yourself and your staff with your payment terminals so you will be more likely to recognize equipment that has been compromised.
- ▲ Ensure that your hardware and software are updated so as not to store cardholder data after a transaction has been processed.
- ▲ Compare the name printed on the receipt with the name on the card.
- ▲ Require point-of-sale staff to keep a customer's card in clear view at all times.

If you are ever suspicious of any activity within your business, contact our Merchant Client Support Center at 1-800-828-1629.

Merchant Support Center

We offer personalized service through our Merchant Client 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). For faster service, have your merchant number ready when you call.

Telephone authorizations 24/7 at: 1-800-228-1122

Write to us at: Commerce Bank, Merchant Department

811 Main Street

KCBC-2, Kansas City, MO 64105

Fax us at: 1-816-234-2181

Visit us online at: Commercebank.com



call click come by

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 ©2008 Commerce Bank N.A. All rights reserved. ask listen solve and call click come by are trademarks of Commerce Bancshares, Inc.