



# Merchant *On-line*

Spring 2007

Exclusively for Commerce Bank Merchants

## PCI Data Security Standard

Compliance regulations are becoming more strict, even for smaller merchants

A recent press announcement was made regarding a data security breach at a large retailer. This incident underscores the need for all businesses to ensure that they handle customer payment card data with the utmost vigilance.



The security of customer payment data is not just a card association issue, but is the responsibility of merchants

who accept cards. All merchants who store, process and transmit payment card data are required by the card associations to comply with the PCI Data Security Standard (PCI DSS) — their customers expect it and their reputations depend on it.

*continued on page 3*

### The “Digital Dozen”

The backbone of the PCI DSS consists of 12 requirements with which merchants must be in compliance:

- 1 Install and maintain a firewall configuration to protect cardholder data.
- 2 Do not use vendor-supplied defaults for system passwords and other security parameters.
- 3 Protect stored cardholder data.
- 4 Encrypt transmission of cardholder data across open, public networks.
- 5 Use and regularly update anti-virus software.
- 6 Develop and maintain secure systems and applications.
- 7 Restrict access to data by business need-to-know.
- 8 Assign a unique ID to each person with computer access.
- 9 Restrict physical access to cardholder data.
- 10 Track and monitor all access to network resources and cardholder data.
- 11 Regularly test security systems and processes.
- 12 Maintain a policy that addresses information security.

### Inside

|  |   |
|--|---|
| The Evolving World of Skimming Fraud ... | 2 |
| Don't Get Lured Into Phishing .....      | 3 |
| Commerce DirectCheck Card .....          | 4 |

# The Evolving World of Skimming Fraud

## *Is fraud coming from inside your business?*

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. The stolen card data is then used to make fraudulent cards.

---

***Skimming has grown beyond restaurants and gas stations, to other business types.***

---

Advanced technology and sophisticated hardware have caused a resurgence in this tried-and-true practice. Inexpensive skimming devices can be acquired easily on the Internet, and skimmed data has become a profitable commodity in the counterfeiting marketplace.

Criminals have expanded their point-of-sale attacks beyond the traditional targets (gas stations and restaurants) to a wider range of retailers, particularly smaller merchants who may be less equipped to prevent this crime.

### **Recommendations from the experts to help protect you and your customers**

- **Familiarize yourself and your POS staff with your payment terminals, so you will be more likely to recognize equipment that has been replaced or tampered with.**
- **Ensure that your hardware and software are updated so as not to store cardholder data after a transaction has been processed.**
- **During each transaction, compare the name printed on the receipt with the name embossed on the card. Additionally you can check the cardholder's ID to ensure that the name on the card matches the ID.**
- **Require POS staff to keep a customer's card in clear view at all times.**

### **Real skimming stories**

A recent account of a skimming ring that was broken up tells of two employees who stole data from hundreds of cards by simply swiping the cards twice — once through the



A skimming device is shown here from several different angles.

merchant's real terminal and then a second time through the skimming device. The stolen information was transmitted from a home PC over the Internet to a middleman, who sold the information to a group making counterfeit cards in another state.

Another new technique used by criminals is to replace legitimate payment terminals with equipment that records card data fraudulently.

### **You could earn a reward**

The major card associations are in agreement that the growing threat of skimming needs to be brought under control. Visa currently offers a reward of up to \$1,000 for information leading to the arrest and conviction of persons manufacturing or using counterfeit cards.

Skimming is a crime that affects merchants and cardholders alike. Cardholders, unaware that their critical information has been stolen, will discover the unauthorized charges only after the criminals are long gone. And skimming is one of the ways fraudulent cards are brought into circulation. If you are ever suspicious, contact our Merchant Support Center and your local law enforcement authorities.

## Payment Application Best Practices

The Payment Application Best Practices (PABP) guidelines (detailed on Visa's web site) help to define how information should be protected, or not stored in the first place. That way, even if a hacker makes it into your system, there's nothing for them to steal. PABP states that magnetic stripe data, including CVV2/ CVC2 and PIN Verification Value, should NOT be stored. Additionally, merchants must make every possible effort to

facilitate a secure network, including software updates and remote access to applications.

The PCI DSS and PABP were established to provide clear guidelines for merchants. By complying with these requirements, you will not only meet your obligations to the credit card associations, but also build a culture of security that benefits everyone. For more information about the PCI Data Security Standard and compliance requirements contact our Merchant Support Center.

## Data Security in the Global Marketplace

### KEEPING YOU UP TO DATE ON CRITICAL SECURITY ISSUES

#### Don't Get Lured Into Phishing

Normally we hear of phishing as it affects consumers. But this widespread email scam targets businesses too, and merchants need to be aware of how to protect themselves.

Phishing criminals send out emails requesting financial information. Sometimes the email looks like a letter asking the user to reply to the email and provide financial data. More recently however, criminals are sending emails with links to phony web sites that look amazingly like the legitimate sites of well-known financial institutions. The user is asked to submit data such as their credit card number, password or Social Security number.

Once a criminal has your critical financial data, that information is used to access your accounts or create fraudulent accounts in your name. This rapidly growing form of fraud is one of the most common ways in which identity theft happens.

#### What to look for and how to protect your business

- If you receive an email requesting your account or billing information, don't reply or click on any links within the email.
- Before you submit any information through any web site, look for the "lock" icon on the browser's status bar. This icon ensures that your information is secure during transmission.
- If you are suspicious of an email from any business or financial institution with which you already do business, call and speak with a representative personally.
- If you realize that you may have shared critical financial data with an unknown source, call your bank or credit card company right away.

Suspicious emails can be forwarded to **SPAM@uce.gov** or can be reported to the Federal Trade Commission at [www.ftc.gov](http://www.ftc.gov).

Visit [www.commercebank.com/datasecurity](http://www.commercebank.com/datasecurity) to learn more about PCI compliance.

# Business Solutions from Commerce Bank

Reduce payroll costs and increase efficiency with the Commerce DirectCheck<sup>SM</sup> Card

**N**ow you can expand your direct deposit program to all employees — including those who do not have a checking account.

The Commerce DirectCheck Card allows you to deposit funds directly to a reloadable prepaid Visa® card, avoiding the inconvenience of a paper payroll check.

Your employees can then use their Commerce DirectCheck Card to:

- Make purchases anywhere Visa debit cards are accepted



- Get cash at any ATM displaying the Visa or Plus® logo worldwide
- Get cash back on purchases at thousands of merchants accepting PIN-based transactions, including grocery, drug and discount stores

## 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.



call



click



come by

Commercebank.com

## Employers reduce costs associated with paper paychecks

- Reduce payroll costs by eliminating check printing and processing
- Eliminate costly out-of-cycle checks
- Simplify reconciliation
- Reduce the risk of check fraud
- Avoid charges and inconvenience of reissuing lost or stolen checks

## Added Benefits for Employees:

- Immediate access to funds on payday
- No need to pay check-cashing and money order fees
- Flexibility to shop or pay bills by phone, online or mail
- Access account information such as balance and transactions 24/7 at 1-866-518-4714
- Experience the world-wide recognition and acceptance of a Visa card.

If you would like to learn more about DirectCheck, contact Lindsey Carter at [Lindsey.Carter@Commercebank.com](mailto:Lindsey.Carter@Commercebank.com) or by phone at 816-234-8879.