Summer 2008

Merchant On-line

Exclusively for Commerce Bank Merchants

Taking Control of Your Interchange Fees

Rates of interchange can vary according to the type of transaction and its associated risk. For example, fees are lower for electronically authorized transactions than for key-entered or manually imprinted ones. Fees may be higher for mail, phone or Internet transactions because of the increased risk of fraud associated with card-not-present transactions.

The type of card used also affects the interchange fee, for example, rewards cards impose a higher fee. Unfortunately, as a merchant, you do not have control over what type of card is used. There are many opportunities to reduce fees. Here are some tips for keeping interchange fees to a minimum.

Face-to-Face Merchants

- **Swipe the stripe.** Key-entered transactions result in higher interchange costs. If you find you are key-entering often, your terminal's magnetic stripe reader may need to be cleaned.
- **Submit batches daily.** Transactions in batches that remain open beyond the following day will result in a higher interchange expense.
- **Obtain an authorization for all ticket-only transactions.** This should provide adequate documentation in the event of a cardholder dispute. The authorization code should be entered through your POS terminal at the time the transaction is entered. The ticket amount must equal the authorization amount. Due to tips, restaurants, bars and salons are exempt. An imprint of the card is also required.

Commercial Card Acceptance

- **Submit Level II/III data.** Submitting specific data, when prompted, for Commercial Card transactions can help reduce interchange fees. For instance, a sales tax amount must always be entered (entering $0 does not qualify as a valid amount). The tax indicator must also be passed to qualify for level II (e.g. tax included or tax exempt). Your POS terminal or software should include an entry point for the cardholder's Customer Code.

continued on inside page

Inside

Business Solutions from Commerce Bank 2
Meet Chris Tanos, Client Support Manager .. 2
What to Do After a Data Compromise 3
Data Security is a Shared Responsibility 4

Business Solutions from Commerce Bank

Reduce payroll costs and increase efficiency with the Commerce DirectCheck℠ Card

Now 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

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
- Split your pay between direct deposit and the Commerce DirectCheck card
- Access account information such as balance and transactions 24/7 via the web or phone
- Experience the worldwide recognition and acceptance of a Visa card

To learn more about DirectCheck, contact Jenni Kahle at **Jenni.Kahle@commercebank.com** or by phone at 816-234-8879.

Getting to Know Commerce Bank

Meet Chris Tanos, Merchant Client Support Manager

"The most important part of my job is building partnerships with our merchants and creating a fun working environment for the team."

In her eight years at Commerce Bank, Chris Tanos has held several positions within bank operations including, programming and deploying equipment, project management, Branch Hotline, and records management. She also has over 12 years of experience in retail sales and management. Currently, Chris manages the Merchant Client Support Team consisting of 17 employees. Her team is responsible for account boarding and maintenance, merchant implementation and training, the merchant support desk, and fraud analysis.

When you contact a member of Chris' team, you will interact with a team that has an average tenure of six years in the acquiring industry. The Merchant Support Team is here to assist you with questions and troubleshooting. Chris and her team truly care about the success of their merchants and are committed to helping them meet their payment processing needs. A recent survey rated this team a 5.59 out of 6, a 93% positive satisfaction rating.

Taking Control of Your Interchange Fees

continued from front page

Card-Not-Present Merchants

- **Utilize Address Verification Service (AVS).** This is the fraud detection tool most often used by online merchants to assist in authenticating the data supplied by the customer. POS software should prompt for entry of the customer's ZIP code and the numeric portion of their address.
- **Enter an order number.** Your POS terminal or software should include an entry point for an order number.

Understanding the factors that affect interchange fees can help merchants achieve the best rates. As experts in payment processing, Commerce Bank can help you reach your business goals. Call the Commerce Bank Merchant Support Center at 1-800-828-1629 if you have questions about controlling interchange fees.

Data Security in the Global Marketplace

KEEPING YOU UP TO DATE ON CRITICAL SECURITY ISSUES

What to Do in the Event of a Data Compromise

Whether data theft is initiated by a disgruntled employee, a malicious competitor, or a hacker, these attacks can cause damage and disruption to your payment system. How you respond to and handle such an incident determines how well you will be able to control the resulting costs and consequences. Preparation for security incidents is vitally important to the protection of key cardholder information. If your business ever experiences a data security breach, you must take immediate action to help prevent additional damage and adhere to PCI DSS requirements.

First Steps After a Compromise

1. Immediately contain and limit the exposure. Prevent further loss of data by conducting a thorough investigation of the data compromise.

2. Alert all necessary parties immediately. First contact the Commerce Bank Merchant Support Center to provide details; followed by your local law enforcement office.

3. Commerce Bank will request that you provide information on all compromised cardholder accounts and they will brief you on notifying major card associations. The major card associations will distribute the compromised account numbers to card issuers and ensure the confidentiality of non-public information.

4. Within three business days of the data compromise, you will need to provide an Incident Report document to Commerce Bank.

Rest assured that Commerce Bank will be with you every step of the way if such an incident should occur at your business. It is often difficult to detect when a system has been attacked or an intrusion has taken place. Be sure to contact our Merchant Support Center immediately at 1-800-828-1629 if you notice any suspicious activity within your payment processing system.

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

Data Security is a Shared Responsibility

Merchants are encouraged to stay current with PCI DSS Requirements

The Payment Card Industry (PCI) Data Security Standard (DSS) was developed by the major card associations to protect customer information by requiring merchants of all sizes and business types to follow consistent data security measures. Today it is mandated that all merchants, whether online or brick-and-mortar, meet these security standards when storing, processing and transmitting cardholder information.

By adhering to the PCI Data Security Standard you'll help ensure the safety of your customers' transactions.

The "Digital Dozen"

The backbone of the PCI DSS consists of these 12 requirements, which merchants must follow.

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.

Stay Up to Date on PCI Requirements

It is the responsibility of every merchant to have the proper systems in place. Call our Merchant Support Center or visit the Visa® and MasterCard® web sites for the latest information on how to make card transactions safe for your customers and profitable for you!

Merchant Support Center

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). 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*