ask   listen   solve

Merchant *On-line*

Exclusively for Commerce Bank Merchants

On-the-Spot Credit Card Processing

Commerce Bank announces new wireless product offering

A new product, coming this fall, will allow mobile merchants to process card transactions using their cell phone as a point-of-sale system. The CellTrek Mobile Merchant enables merchants to capture card account data, obtain an authorization and provide their customers with a receipt on the spot. This product is perfect for merchants with seasonal wireless or mobile needs, such as trade show merchants or sidewalk sales. It is also a great program for any service personnel, contractors, electricians and plumbers.

The CellTrek Mobile Merchant integrates payment processing with cell phone functions, reducing the number of devices the merchant carries and making payment processing equipment more affordable, especially for smaller merchants. This product supports all industry standard card-present and key-entered transactions including sale, void, and refund. It also permits both card-swiped and key-entered transactions.

Advanced security capability

CellTrek maintains high security standards for encryption, certification and privacy, and meets or exceeds all current Payment Card Industry (PCI) security requirements. Transaction encryption is used throughout the transaction process, from the initial card swipe, through the wireless network, to the host and back again.

A cost-effective solution

CellTrek makes wireless card acceptance affordable to merchants for whom this type of service has previously been cost-prohibitive. In addition to the cost savings of the hardware and software, merchants can reduce their transaction costs by qualifying for lower "card-present" processing rates.

If your business relies on mobile services, contact our Merchant Support Center to learn more about CellTrek Mobile Merchant.

Inside

Commerce Bank Member FDIC

PIN Debit Acceptance Requires PCI Compliance

Controlling fraud as consumers embrace PIN debit, and merchants benefit from lower fees

Merchants enjoy reduced interchange fees when customers use their PIN instead of a signature at the point of sale. But it's critical that merchants keep all their systems, hardware and software up to date, and ensure that PIN data is not being stored on the merchant's system after a transaction is completed.

For a complete listing of the Payment Card Industry (PCI) data security standards, visit www.usa.visa.com/business.

Recent reports of PIN debit fraud point to a greater need for merchant compliance with the PCI data security standards. Only about 25% of U.S. merchants surveyed in 2004 and 2005 were fully in compliance, but experts are cautiously optimistic, looking for 73% compliance by the end of this year.[1]

Careful controls needed on all back-up media

PCI regulations require merchants to encrypt transmission of cardholder data across public networks. One area in which recent security breaches have occurred is within the merchant's application. Hackers have found numerous "back doors" that allow access to cardholder data stored within the application. An Application Gateway placed in front of card data processing applications is one step in making your system PCI compliant. (See illustration below.)

Users   Firewall   Application Gateway   Merchant Applications

Be sure your staff members can distinguish between visitors, customers and fellow employees.

Restrict physical access to cardholder data

Information theft can occur just as easily within your merchant location as it can in cyberspace. An estimated $2 million was siphoned from hundreds of bank accounts in recent months by criminals using point-of-sale terminals that had been altered to steal cardholder data.[1] This underscores the need for constant vigilance by business owners, managers and staff. Any piece of equipment that differs from your normal processing equipment should be reported immediately.

Here are some tips that may help you protect the data that you need to store:

✔ Use security cameras to monitor sensitive areas.

✔ Develop procedures to help your staff easily distinguish employees from visitors, especially in areas where cardholder information is accessible.

✔ Destroy media containing cardholder information when it is no longer needed for business or legal reasons.

Contact our Merchant Support Center for more information on data security.

1. *Digital Transactions* July 7, 2006

RCPS Helps Merchants Avoid Chargebacks

Consumers now have the ability to cancel recurring payment agreements through their card issuer using the MasterCard® Recurring Payment Cancellation Service (RPCS). This service benefits merchants by preventing chargebacks that occur if recurring payments are declined. In fact, the fee for using RPCS is lower than the cost of an unwanted transaction and the resulting chargeback.

Tell your customers about RPCS while explaining the benefits of automatic billing, to help reduce the uncertainty that many cardholders have about automatic billing. RPCS will help boost cardholder confidence in recurring payment agreements by protecting them from billing errors.

RPCS helps merchants maintain their good reputation by blocking unauthorized recurring payment transactions.

Contact our Merchant Support Center if you process recurring transactions and want to take advantage of this new service. You can learn more at **www.mastercard.com**.

Data Security in the Global Marketplace
KEEPING YOU UP TO DATE ON CRITICAL SECURITY ISSUES

Recently, someone called one of our merchants claiming to be from MasterCard, and said they needed transaction information so they could fix a mistake. The caller told the merchant they had just accidentally erased the last three transactions from that merchant's terminal, and that they needed the card numbers and CVC2 data from those transactions. Luckily, the merchant became suspicious, and asked for a contact name and number, at which point the caller hung up.

We encourage you to follow this simple rule: If you ever receive a call or an e-mail from someone claiming to be from the government, a bank, the police department or credit card company – always refuse to give out any confidential information such as credit card numbers, expiration dates or cardholder names. Instead, offer to call the person back. If they are not from a legitimate entity, they probably won't pursue the communication any further. No one from Commerce Bank or any of the card associations would ever ask a merchant to divulge critical cardholder data in such a manner. If you are ever suspicious about a call or an email, notify our Merchant Support Center at 1-800-828-1629.

American Express® and Discover® Card regulations require terminal download

Updated Processing Requirements

American Express and Discover Card are in the process of updating their merchant acceptance requirements, which will require changes to the way those cards are processed through your POS terminal. If you have not already had your terminals upgraded you will be contacted soon to complete this process.

What does this mean to merchants?

In order to be in compliance with these new requirements and keep your acceptance costs down, you will need to receive a software download for your POS terminal by October 31, 2006.

There will be a nominal fee for each terminal download and for each training session. The download will take approximately 30 minutes per terminal. Training will be provided once the downloads are complete.

Commerce Bank has engaged TASQ Technologies, Commerce Bank's preferred supplier of terminals and merchant supplies, to assist you with the terminal download.

If you have not already been contacted, you should expect a call from a TASQ representative on behalf of Commerce Bank, to schedule these services. Prior to the download and training, you will receive a compliance packet in the mail with Quick Guides and/or Overlays that you will need during the download and training.

Industry-wide requirement

All merchants accepting American Express and/or Discover are required to comply with these changes. Commerce Bank has tried to streamline this process to make it as efficient and cost effective as possible. Your business is important us. If you have any questions, please feel free to contact our Merchant Support Center at 1-800-828-1629.

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**
- **Supplies**
- **Service Questions**
- **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.

Commercebank.com

call   *click*   *come by*