


bankonit

ROBERT K.O. LUM

Assistant Vice President and Merchant Services Sales Manager

— April 2009

Safeguard Your Card Processing; You'll Sleep Better!

It's 2:00 a.m. Cash from yesterday's card transactions should be crediting to your business checking account in a few hours. Or will it?

Cash flow and liquidity are critical to your business whether it is making payroll, taking discounts from vendors for paying bills early and just as importantly, being able to sleep at night.

Nearly every week, fraudulent activity strips cash from small businesses. Fraudulent credit and debit card activity has increased from petty thieves skimming credit card numbers; email and text message phishing scams; to computer hackers infiltrating computer systems and stealing personal information from millions of card owners. In January 2009, Heartland Payment Systems reported over 100 million credit and debit card account numbers had been breached. VISA and MasterCard have already detected fraudulent credit cards being used throughout the United States.

Businesses must exercise due diligence when processing card transactions to accomplish two important objectives: 1) prevent losses at the point of sale and 2) protect the cardholder information that their customers have entrusted to them. How often have you heard of a merchant getting paid or receiving merchandise back from a fraudulent transaction? Also, would you trust your purchases to a merchant that was careless with your card data and allowed it to be stolen? In most, if not all cases, the answer is "never!"

If you employ these simple ideas, you can avoid losses by preventing fraud at your point of sale and by protecting your client's card information.

First, let's talk about your point of sale. How does your business handle card transactions?

Does your cashier compare signatures and 4 digit codes?

This is an easy step, and only needs to take a few seconds. The signature on the card should match with the signature on the sales receipt. Also, the name and last 4 digits on the card should match the name last 4 digits printed on the sales receipt. You are at risk if the card belongs to Mary, but the person signing is Joe.

Always swipe the card. The magnetic stripe on the back of every credit or debit card contains the cardholder name, card account number and expiration date, as well as special security information designed to help detect counterfeit cards. When the stripe is swiped through the terminal and electronically read, this information is relayed to the issuer and used as crucial input to the authorization of the transaction.

Are you using all the fraud detection tools we provided you with? If you can't swipe the card, then you need to take additional action to protect yourself. Make sure you are using the Address Verification Service (AVS) and Card Verification Value 2 (CVV2) to complete your transaction.

Secondly, are you protecting your valued customers? A data breach could result in fines, penalties and civil suits against your business and ruin your reputation.

How old is your credit card terminal, pin pad, or Point-of-Sale software? If your terminal or POS software is outdated, it may not meet data encryption standards, industry security requirements and may be storing credit card numbers or cardholder data, making this sensitive data susceptible to theft.

What do you do with your credit card sales receipts? Your credit card sales receipt contains your customer's card information and is your insurance policy against chargebacks and transaction disputes. Stolen receipts could lead to credit card fraud, and damage your business' reputation. Your receipts should be stored in a safe and secure place.

In summary, contact your card processor to see what they are doing to prevent fraud and protect you with the following:

Does your card processor offer fraud detection tools like AVS and CVV2? Do they charge you for this service? If so, then they are penalizing you to protect your business.

When was the last time your card processor updated your merchant profile? If your business has changed, you should communicate with your card processor. The better processors monitor your account for suspicious or out-of-the-ordinary transactions.

How well does your processor understand the mandatory Payment Card Industry Data Security Standards (PCI DSS)? Are they helping you becoming compliant? PCI DSS was released in 2007 and provides required guidelines for merchants such as storing and securing credit card receipts and ensuring that data is protected from computer hackers. These requirements were put in place to help protect businesses. All merchants are required to understand and comply with these requirements.

Fighting fraud and theft can be a daunting task for the business owner. But, you are not alone. Make sure your card processor is reliable, conscious of your best interests, and you will sleep restfully through the night.