



PAYMENTS INSIDER

Delivering the inside story in payments news

Issue 11, October 2009

A Publication of Heartland Payment Systems®

Dear Valued Merchant:

As a business owner, it's important to protect your profits and customers — especially because there are many fraud schemes out there that target both. The scams are often creative — with the goal to “steal” your money or cheat your business and customers. Some tactics include simply illegally accessing and using private business and cardholder data.

This issue of *Payments Insider* details common types of internal and external fraud — perpetrated by employees — or “cardholders.” Read on for details on how to identify warning signs and ways to proactively prevent bank card fraud.

As always, if you have any questions about payments — including best practice payments tips for business owners — please call your relationship manager, account manager or your Heartland servicing team at 888.963.3600. Feel free to also email us at Heartland@e-hps.com.

Best regards,

Eleanor Beckmann, director of loss prevention
Mike Hall, senior fraud strategy analyst
Heartland Payment Systems

IN THIS ISSUE

- Introduction
- Protect Your Business — and Your Customers — by Taking a Proactive Approach to Fraud
- Fraud Warning Signs

Get *Payments Insider* Electronically!
SIGN UP TODAY.
HeartlandSignUp.com

Protect Your Business — and Your Customers — by Taking a Proactive Approach to Fraud Prevention

Fraud can happen to — and at — any business, regardless of your size and location or the products and services you offer. And, fraud schemes — whether perpetrated by employees or customers — can be simple or complex. By learning about them and their warning signs — and taking an active role in fraud prevention — you can decrease the chances of it happening at your business. Here are some simple ways to proactively avoid bank card fraud.

Keep a Watchful Eye on Internal Fraud

While you may have great people working at your business, be sure they are trustworthy — especially because employees can easily use point-of-sale (POS) equipment and other tactics to cheat customers — and your business. Because fraud by employees is common, taking the time to hire quality people can benefit you in many ways.

- **Skimming:** Employees who have customers' credit and debit cards for a few seconds — like servers and sales clerks — can quickly steal card information. It's easy to do when cards are out of customers' sight. All employees need to do is copy card numbers by hand or with a small device that records information with a single card swipe. Once a

card's information is copied, it can easily be downloaded to a computer and re-encoded onto a blank card.

Prevent skimming: Be aware of your employees' activities and keep an eye out for suspicious devices or notepads. Also, consider offering your customers the ability to settle their bills at the point of service using portable, hand-held POS devices. Your customers simply swipe and go — keeping their cards in-hand.

- **Unusual Credits:** Unscrupulous employees may issue credits to a friend's, family member's — or their own — personal credit or debit card for a return that isn't legitimate or for an amount exceeding the actual cost. Employees typically throw away the sales slip associated with these transactions so there is no record of the credit.

Prevent unusual credits: Consider making your POS equipment's credit function “password-protected” so only you — and your manager on duty — can issue a credit. Also, make it a best practice to always match credits with the original sales receipt.

- **Over-tipping:** In industries where adding a tip to debit and credit cards is common, be on the lookout for employees who over-tip themselves. This happens when customers leave the tip line item on a receipt blank — or when employees report a tip for an amount greater than the cardholder has authorized. Employees then retrieve the overage in cash as they “tip out” at the end of their shifts.

Prevent over-tipping: Be aware of tips that seem larger than normal, and look for patterns in employee tips. For example, take note if a particular employee consistently earns generous tips.

- **Data Breach:** If your business is compromised, private information — stored on items such as a laptop, office server and POS system — may have been illegally accessed and could lead to credit card data theft, fraud and financial loss. This type of fraud can happen internally or externally — and can happen for several reasons. For example, your business may be running on outdated POS software that stores data, hasn't been upgraded or is known to be vulnerable. If you use your POS system as a

general computer for tasks like surfing the internet and back-office duties, the risk of downloading malicious viruses that can compromise the system or make it easier for hackers to access your programs increases.

Prevent a data breach: Ask your POS installer — and Heartland — about the system you use and if it is up-to-date. Also, speak to your IT specialist about network and data access security — such as firewalls, remote access and external file transfer. Consider blocking all internet usage (email, web search, etc.) from employees and change passwords often. Monitor your computer and systems daily for strange or unknown files and attachments.

Be Aware of Cardholder/External Fraud

Fraud by outsiders can happen when you least expect it — especially since fraudsters are creative with their schemes. It's important to be cautious of odd behavior and unusual requests — and train your employees to speak up if something about a transaction or customer seems suspicious.

Some examples of external fraud and ways to prevent it include:

- **Wire Fraud:** A typical scheme includes a call or order placed through the hearing impaired system TeleTypewriter or TTY (where fraudsters type in questions and communicate with you via an interpreter) or by email — typically written in broken English — from a Yahoo, Gmail or Hotmail address. The fraudster places an order and provides a credit card number for payment. The card number may authorize, but it may be declined. If it's declined, the fraudster supplies another credit card — usually the same sequence of numbers except for the last few digits.

The fraudster benefits from the last part of the scam where he or she asks you to charge an extra fee on the card — often several hundreds of dollars — and wire the funds through Western Union or another wire service.

Prevent wire fraud: Look for warning signs and never wire funds.

- **International Shipping and Domestic Shipping Fraud:** In an international shipping fraud scheme, you're typically asked to ship an order to a third-world country. You are contacted through TTY, and the "customer" switches your conversation to email using a generic email address. You receive a large order and are given several card numbers to complete the transaction. Domestic shipping fraud is similar — but you're given a US shipping address. The "cardholder" asks for the shipping number and then redirects the shipment overseas.

Prevent international shipping and domestic shipping fraud: Take note of shipping requests and shipping locations. Be cautious with overseas shipping.

- **In-Person Sales Fraud:** Be wary when cardholders give you invalid credit or debit cards — and offer you an authorization number. Completing an invalid transaction can lead to a chargeback to your business — where you lose the product and the profit from the sale. Also, customers whose debit or credit cards are invalid may pretend to call the bank using their cell phones or your business phone. They often hand you the phone so you can receive the authorization code. However, you may be speaking to an accomplice.

Prevent in-person sales fraud: Question customers who are overly knowledgeable about debit and credit cards and try to force the sale.

- **Phishing:** Phishing is a relatively easy — and increasingly common — fraud tactic. Someone pretending to be a representative from law enforcement, the card brands such as Visa® or MasterCard®, an issuing bank or other authority calls you and tries to get your debit and credit card information — and your customers' information — over the phone.

Prevent phishing: Never give your debit and credit card information — or your customers' information — over the phone.

Be sure to make fraud prevention a best practice at your business. Hire honest and trustworthy workers, and be sure to train all employees on how to spot fraud warning signs (see the sidebar "Fraud Warning Signs" for more information) — and what to do if they are involved in a potentially fraudulent scenario. Taking these steps can help protect your business and your legitimate customers — and save you from the headaches associated with fraud.

Fraud Warning Signs

Take note of these warning signs typically associated with fraudulent schemes:

- Requests to wire (through Western Union or another wire service) an order's shipping fees after charging the cardholder
- Requests to force swiped card transactions with an authorization number that the customer provides
- Requests from a customer to use your card equipment to input a sale after it's been declined
- Multiple attempts with various cards or card numbers to complete a transaction
- Receiving suspicious calls from a bank, card company or law enforcement agency requesting a customer refund or credit card numbers

If you suspect fraud or other suspicious behavior, call the Heartland Loss Prevention department at 888.798.3133.

You have rights!

Go to MerchantBillOfRights.com today.

To receive useful business tips, sign up to receive *Payments Insider* via e-mail at HeartlandSignUp.com

Break out of the box and build your business with ...
HEARTLAND GIFT MARKETING

Visit HeartlandPaymentSystems.com to learn more.



Heartland
PAYMENT SYSTEMS™

The Highest Standards | The Most Trusted Transactions

888.963.3600
HeartlandPaymentSystems.com