PCI Convenience Store Employee Data Security Training Manual

April 8, 2014

Version 1.4.1

CONEXXUS
solve forward

TABLE OF CONTENTS

INTRODUCTION

The protection of payment card data is of critical importance to <Merchant Name>. If payment card data were disclosed to unauthorized individuals, <Merchant Name> could face fines due to compliance violations as well as suffer a serious loss of reputation. In recognition of this risk, this policy defines requirements for the protection of payment card data. All employees and contractors are responsible for abiding by this policy. [PCI DSS Requirement 12.4] **Failure to comply with this policy is subject to Company disciplinary action.**

PAYMENT CARD PROCEDURE

Do Not Accept A Card If:

- The hologram is missing or of poor quality if present.
- The customer's signature does not match the one on the card.
- The account number or cardholders name are ironed out and the card is embossed with a different number. Evidence of this alteration is noticeable on the back of the card.
- The card is warped or has a dull finish.
- The account number is tilted or slanted, or the embossed data spacing is off.
- The printed information is on top of the laminated surface of the card.
- The printing on the back of the card is blurry or distorted.
- Information displayed on the printed receipt does not match the account number embossed on the front of the card.
- Do not accept payment card data over the phone.

Fraud Detection

Always be aware of the following:

- A hesitant customer. Shaky voices or delayed responses to questions may indicate that the cardholder is not comfortable with the information they are providing.
- P.O. boxes and mail receiving services, which may indicate lack of a permanent address.
- Toll-free numbers given as the day or evening phone number. Attempt to get a direct line instead.

Transactions Where The Payment Card Must Be Manually Keyed (Debit Cards Are Excluded)

Key-entered transactions carry additional fraud risk as the contents of the magnetic stripe are not obtained. *Manual Back-up Instructions:* These procedures must be followed if you cannot run a card through a card reader, i.e. cracked or damaged magnetic stripe, or if the POS equipment is not working properly or the credit card network is down.

- Imprint the card data on a sales ticket.
- Never accept payment card data from a customer without a card.
- Complete all of the fields on the Credit Card Sales Ticket, including the client's billing address.
- Call the appropriate authorization center and obtain an approval number and record on the sales ticket.
- Have the customer sign the receipt and compare the signature with the signature on the card. Do not accept an unsigned card.
- Properly secure and store sale ticket, i.e. locked cash drawer.
- Inform supervisor that transactions will need to be re-entered for processing.

System Outage/Failure

In the event of a POS system failure where the system is inoperable, contact your supervisor immediately. Never connect the POS to a phone line unless you have initiated the call to the POS help desk and notified your supervisor.

DAILY ACCESS LOGS

Use of a Daily Access Log is required to be filled out by the store associate for anyone having access to the back room, secure storage areas, point of sale equipment (POS), including PIN Pads and dispensers. Appropriate ID is required by any outside vendor who may have access to secure storage or equipment. Associates are required to also log any activity when accessing the dispensers and card readers.

A physical check of POS equipment must be done when an associate logs in for their shift and recorded and logged.

Date: _____

Vendor / Service Co. Employee Name / Number	Driver Name Technician Name	Time In	Time Out	Invoice # / Service # Device #	Reason for Visit
ABC Bread Company	*Jim Smith*	*6 am*	*6:30*	*88955*	
XYZ Pump Company	*Tom Jones*	*10 am*	*12 pm*	*12545*	
Employee #123	*Bob Smith*	*1 pm*	*1:30*	*Pump 2*	*Chg Paper*

STORE LEVEL REQUIREMENTS

Overview

At < merchant name>, we have a responsibility to our customers, and our stakeholders, to protect all sensitive data. We need to monitor that we are taking proper steps in our handling of data, and that any instances of suspected tampering or fraud is reported.

Handling Payment Cards

Every associate needs to take certain precautions when handling payment cards. All credit transactions at the dispenser should be processed by the customer. All inside transactions should also be processed by the customer; with the exception of faulty/missing self serve equipment, or payment card mag stripe problems.

Copying encoded data from the magnetic strip of any payment or debit card, by skimming devices or any other means, is expressly forbidden and will lead to immediate termination and full prosecution as permitted by state and federal laws. Photo copies of payment or debit cards are expressly forbidden.

In the rare occasion that an associate manually enters a payment card number into the POS (point of sale register), the number can never be written down, manual imprints are allowed.

The following are items that we cannot store on paper, in the POS, or on a receipt:

1) Pin Number

2) Security Code

The following are items that we can store on paper, in the POS, or on a receipt:

1) Cardholder Name

2) Authorization Code

3) Last 4 Digits of Credit Card

Incident Reporting

It is the responsibility of each <merchant name> associate to report any breaches of security of the card holder data. Every instance will be investigated without repercussions to the associate reporting the incident.

When a suspected problem has been revealed, the associate needs to fill out a General Incident Report and contact their immediate Supervisor. In most cases this is your store manager.

Associate has read and understands <merchant name> best practices, policies and procedures.

Associate _____ **Date** _____

Supervisor _____

ADDITIONAL RESOURCES

www.pcisecuritystandards.org/education/pa-dss_training.shtml

www.pcisecuritystandards.org/faq.html

http://usa.visa.com/merchants/risk_ management/cisp.html

http://www.mastercard.com/us/merchant/support/demos.html

http://www.bbb.org/data-security

www.ftc.gov/bcp/edu/multimedia/interactive/infosecurity/index.html

www.verifone.com/industry-solutions/petroleum--convenience/industry-trends/pump-security-best-practices.aspx

http://www.vendorsafe.com/video/Credit_Card_Safety_Employees/video.html

http://www.bankinfosecurity.com/articles.php?art_id=2878&opg=1

CONEXXUS DATA SECURITY GROUP AND DISPENSER PROVIDER GUIDANCE

Protecting Payment Card Data At Your Dispensers

Your fuel dispensers can be an attractive target to thieves who are becoming more sophisticated and aggressive when it comes to stealing credit and debit card information. We encourage retailers to develop their own security plan to help prevent this type of theft. No single solution will completely prevent attacks, but careful procedures can significantly reduce the opportunity.

Low Cost Steps

- Monitor your dispensers for any high levels of bad card reads or problems accepting cards.
- Create a reference sheet of what your cashiers should look for and post by your POS, including:
  - Be suspicious of vehicles parked on the forecourt for a long time — especially on outside islands.
  - Be suspicious of any "technicians" performing unscheduled work on dispensers.
  - Be alert to any unit off-line message at the POS. Investigate the reason for any offline message.
- Train your store personnel to perform daily site-level dispenser security checks: compare visual inspection to "known good" photos.
  - Use access security strips to aid store personnel in visual inspection and to assist in the detection of tampering at the dispenser, if applicable.
  - Daily inspection of dispensers to examine locks and panels for tampering (scratching, cuts).
  - Periodic inspection of interior of dispenser payment terminal by qualified service provider for evidence of tampering or skimming.
- Stay current on security standards, as well as fraud and theft vulnerabilities in the convenience and petroleum retailing industry.
- Work with your equipment service provider to create acceptable standards for technician visits and identification. Train your store personnel to ask for identification and confirm scheduled work before any work is done on your POS or dispensers. Restrict service technician's access to dispensers without management approval or approved work order.
- Position your store personnel and POS in a location where there is an unobstructed line of sight to dispensers to aid in observing any suspicious activity on the forecourt.

Invest In Pump Security

- Replace common dispenser payment terminal door locks with ones that are unique to your location.
- Upgrade your dispenser's flat membrane keypads to PCI-Compliant Encrypting PIN Pads (EPPs) with full-travel numeric keys that make it difficult to add a fake keypad overlay.
- Consider adding card readers that provide increased physical protection and encrypt payment card magnetic stripe data.
- Consider installing dispenser access security kit upgrades for high risk locations (interstates, high volume).
- Use video surveillance equipment to discourage unauthorized access to your dispensers. Make equipment monitoring obvious and post signs stating monitoring is in use.
- Install proper lighting on the forecourt.
- Perform a review of your dispensers with your equipment provider to create an acceptable baseline for your location and determine an upgrade strategy that considers both the risks for your location, mandates and your business needs.

Note: *If the location has an ATM, a periodic inspection of the ATM should also be conducted for tampering as well.*

Samples of Skimming Devices