PCI Primer

A Practical Handbook

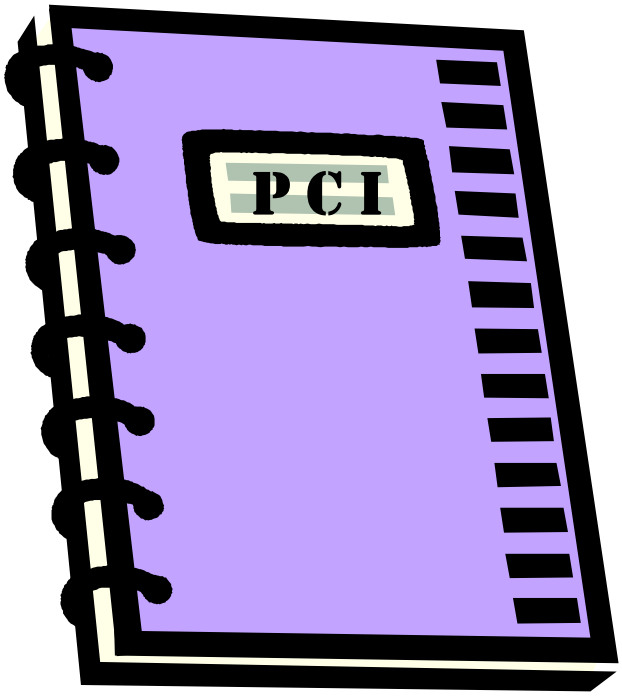


Table of Contents

INTRODUCTION

What is PCI?

PCI is a short way of saying everything we do to protect customer's private information while it's in our hands. It can stand for data security, network security, records storage/destruction, and employee training.

> The real name is the Payment Card Industry Data Security Standard, but you just hear **'PCI.'**

People's identity and private information are valuable commodities. Identities are stolen and sold like cars and TVs through criminal networks. Billions of dollars worth of merchandise and services are stolen with these fake identities.

The PCI Security Council has issued several sets of security standards to help organizations protect customer account data. They are:

- The PCI Data Security Standards –standards that you as a merchant must comply with.
- The Payment Application Data Security Standards (PA-DSS) standards that the payment application vendors (POS Software) must use to develop secure payment applications support compliance with the PCI DSS.

Why Should I Care?

PCI standards help form a strong data security plan for any business. By examining each aspect of your network and your processes, you will have a more secure operation. This will help you reduce fraud and loss and will mitigate your data breach potential.

There are also substantial fines and penalties if you don't comply with these standards. A breach currently costs between $90 and $300 per record. This does not include any local, state, or federal fines or the cost of defending yourself against local, state, and federal charges.

Why Do I Get Different PCI Answers?

You may check the internet or ask people in other businesses what PCI means. You will get all kinds of different answers, because PCI varies

with the size of the company, the industry, and how each company uses payment account data.

Oil companies are different from most retailers because of 'pay at the pump' dispensers, the acceptance of debit cards at the pump, and the sheer volume of our credit card transactions.

Each petroleum company is different because different brands have different network processors, credit card networks, agreements with the card brands, and vendor relationships.

Your PCI relationship is with Sunoco. Sunoco's documentation reflects Sunoco's PCI position and how your business must comply within the Sunoco model.

SUNOCO WORKS AGGRESSIVELY WITH THE PCI COUNCIL AND OUR LEGAL DEPARTMENT TO ENSURE WE PROTECT OUR CUSTOMER'S PRIVATE DATA.

"Customer Information"

For our purposes, customer information is any record containing non-public personal information about a customer that Sunoco maintains or handles. For the purpose of this booklet, the words "Customer Information" refer to the following:

- Account numbers
- Driver's licenses
- Credit card numbers
- Card Validation Codes/Values
- Magnetic stripe data
- Social security numbers
- Cardholder name, address, telephone number
- Any information identifying a person as an account holder of a financial institution

THE BASIS OF PCI

The core of the PCI DSS is a group of 12 principles and requirements commonly referred to as "The Digital Dozen" and are as follow:

The Digital Dozen

Build and Maintain a Secure Network

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.

Protect Cardholder Data

3: Protect stored cardholder data.

4: Encrypt transmission of cardholder data across open, public networks.

Maintain a Vulnerability Management Program

5: Use and regularly update anti-virus software.

6: Develop and maintain secure systems and applications.

Implement Strong Access Control Measures

7: Restrict access to cardholder data by business need-to-know.

8: Assign a unique ID to each person with computer access.

9: Restrict physical access to cardholder data.

Regularly Monitor and Test Networks

10: Track and monitor all access to network resources and cardholder data.

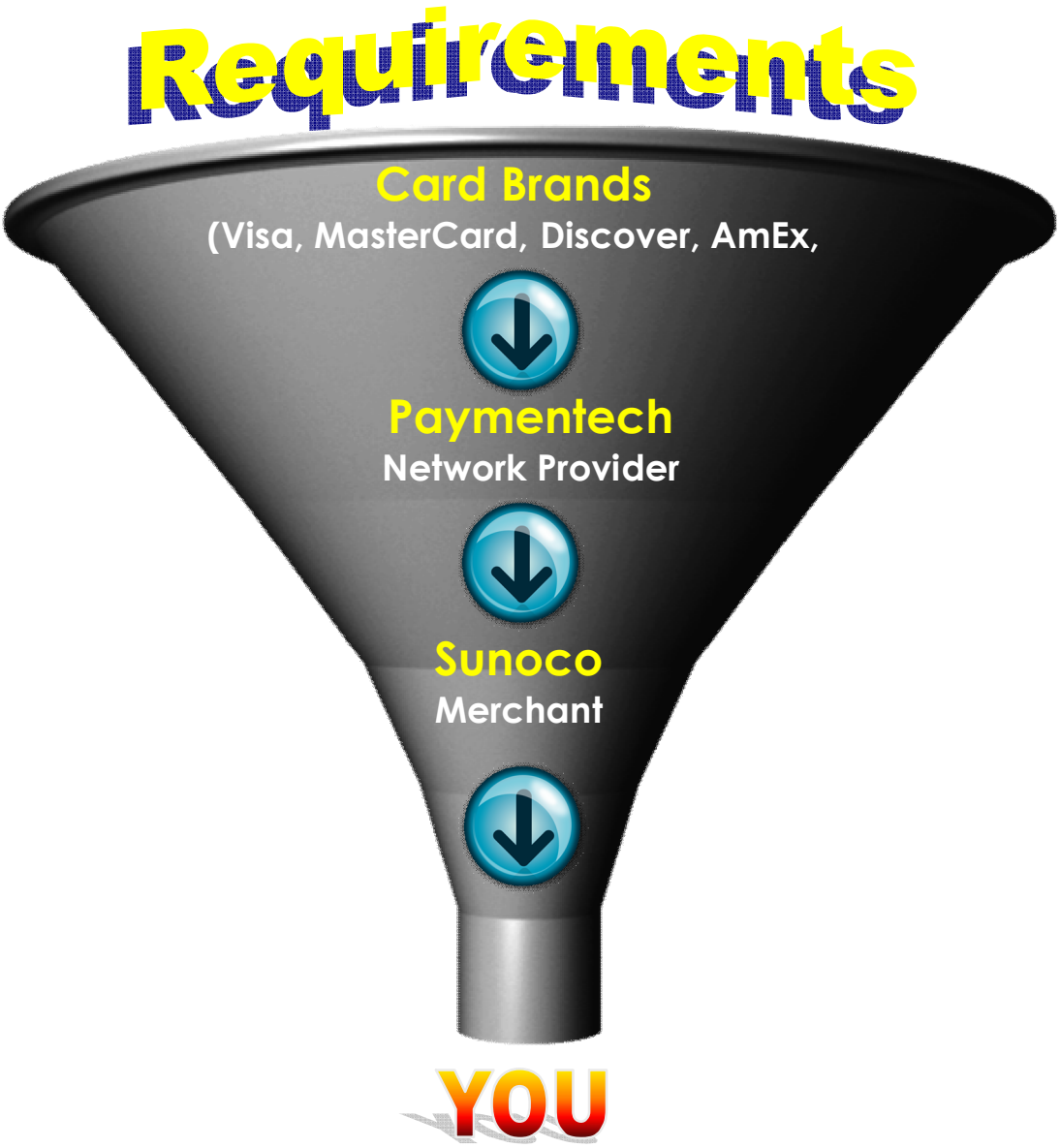
11: Regularly test security systems and processes.

Maintain an Information Security Policy

12: Maintain a policy that addresses information security.

PCI AT YOUR SUNOCO STATION

PCI compliance is a contractual obligation between a merchant and an acquiring bank. For you, Sunoco is the merchant and Paymentech is the acquiring bank. Sunoco dealers and distributors use the Sunoco merchant ID to process credit cards but do not have a direct relationship with Paymentech. Your contract is with Sunoco, so your PCI requirements come through Sunoco.



Be sure that your business processes are compliant with PCI and data security standards. Each site is responsible for ensuring employees are handling credit card and private information correctly.

Each site must ensure that equipment is checked for signs of tampering and management is responsible for confirming this is done.

"Is my site PCI-compliant?"

This is a question that only you can answer; you must determine if your site is PCI-compliant. To assist you with your PCI compliance efforts, Sunoco provides PCI- compliant hardware and applications. The configuration is compliant, as long as the installation is properly conducted and the base configuration is not altered after installation. And Sunoco can only offer 'Best Practices' as to your business processes.

You validate your site's compliance through the use of the PCI-DSS Self-Assessment Questionnaires (SAQ) or through the use of an authorized PCI Auditor. Remember that PCI validation is a snapshot in time but PCI compliance is an ongoing effort. And PCI isn't just about hardware and systems; it is also about how you train your employees and how you handle payment cards and private information.

SUNOCO'S RECOMMENDED PLATFORMS/BEST PRACTICES

A Best Practice is the most efficient and effective way of accomplishing a task, based on repeatable procedures that have proven themselves over time.

Sunoco has worked with the PCI Council, independent auditors, and outside legal counsel to ensure compliance with not only PCI standards, but also state and federal laws related to private data security. Sunoco also reviews equipment and software, capabilities, and effectiveness for use in the Sunoco retail environment.

Sunoco publishes information about best practices and recommended platforms. Remember efforts to upgrade PIN pads or to remove the Ingenico 510 terminals? Both happened because of changes in retail technology and PCI. This section provides you with the best information Sunoco can provide in regard to the equipment you use.

HARDWARE, SOFTWARE, AND SERVICES HERE MEET OTHER SUNOCO REQUIREMENTS (NETWORK PROCESSING, SUPPORT, AND CONTRACTUAL).

PCI IS JUST ONE PART OF THE SUNOCO RETAIL PAYMENT TECHNOLOGY STRATEGY.

"PCI-Compliant"

Vendors say "PCI-Compliant" when offering hardware and software. **Be aware!** Buying 'PCI-Compliant' or 'PCI-certified' equipment does not make you compliant! Installation and use are just as important!

POINT OF SALE (POS)

Along with using the most current software versions, compliance with PCI requirements and assorted mandates, the following "Do's and Don'ts" simplify your compliance efforts. If you have any questions, please contact your area representative or pci@sunocoinc.com.

- **DO -** Always make sure that your non-Sunoco-supplied system is protected by anti-virus software.
- **DO** - Update the anti-virus software to ensure you are protected against the latest/greatest virus threats.
- **DO –** Monitor your event logs for unusual activity.
- **DO –** Reduce the amount of sensitive data that you store.

DO – Use an authorized ASC technician to configure your POS and perform maintenance.

DO – Always install your POS according to the manufacturer's guidelines and following standard Sunoco implementation processes.

DON'T – Use the POS machine to surf the internet, read personal email, or any other unauthorized activity.

Verifone DOs

- **DO** consult the Verifone-provided implementation guide to configure your POS network.
- For Sapphire – **DO** make sure the login switch is left UP.
- For Sapphire – **DO** configure the Verifone router using the PABP Implementation Guide provided by Verifone.
- **DO** put a firewall between the Verifone router and any external connection.
- **DO** update anti-virus protection on Sapphire and Topaz.

Verifone DON'Ts

- **DON'T** configure the firewall to "Allow all Traffic In."
- **DON'T** plug a back office PC on the LAN side of the router.

Nucleus DOs

- **DO** consult the Dresser/Wayne provided PA-DSS Implementation guide to configure your POS network.
- **DO** put a firewall between the Nucleus POS and any external connection.
- **DO** update anti-virus protection on the servers and IPTs.

Nucleus DON'Ts

- **DON'T** configure the firewall to "Allow all Traffic In."
- **DON'T** plug a back office PC on the LAN side of the router.

Passport DOs

- **DO** consult the Gilbarco provided PA-DSS Implementation guide to configure your POS network.
- **DO** configure the Passport router using the PA-DSS Implementation guide provided by Gilbarco.
- **DO** put a firewall between the Passport Router and any external connection.

- **DO** update Anti-Virus protection on Server and IPTs.

Passport DON'Ts

- **DON'T** configure the firewall to "Allow all Traffic In."
- **DON'T** plug a back office PC on the LAN side of the router.

DISPENSERS

The following Dos and Don'ts have been identified relating to dispensers, automatic fuel dispensers, etc. If you have questions, please contact your maintenance help desk or area representative.

DO – Change the locks on any Advantage/Encore systems. Add special locks/keys to replace standard locks/keys.

DO – A weekly inspection of each unit looking for anything that should not be there. Look for extra hardware or changes in the card reader. If you find anything suspicious, contact your servicer and put the dispenser "OUT OF SERVICE."

DO – Look around the dispenser area to see if anyone has installed a camera to watch customer's enter their PIN numbers. Look closely for a hole where there shouldn't be one. These cameras are very small and can be hidden anywhere!

DO – Change the programming access codes for the dispensers regularly.

DO – Remove the manager's keypad from the dispenser and store it in a safe location.

DO – Monitor and compare the "Pump Total" and the "Station Total" reports on the POS and the tank monitor.

DO – Make sure employees can see all dispensers – thieves don't like to be seen.

DO – Be alert to any pump off-line messages on the POS.

DO – Be alert to service calls for dispensers that have been "off-line" (might indicate fraud has happened).

DO – Inspect your site often, looking for loose pump faces, doors, stray wires, or other unusual parts.

DO – Be alert for abnormal traffic patterns on the forecourt.

DO – Check video camera tapes daily for suspicious activity at the pumps.

DON'T – Allow any POS settings that allow a "hot-authorization."

SCAM ALERT: PERSONS POSING AS SUNOCO TECHNICIANS ARE TRYING TO ACCESS YOUR NETWORK. SOME OFFER A FAKE LETTER AUTHORIZING THE WORK. IF THIS HAPPENS TO YOU, CALL THE HELP DESK AND/OR THE POLICE!

WHEN IN DOUBT, CHECK IT OUT!

BACK OFFICE HARDWARE/SOFTWARE

Along with using current software versions, compliance with PCI requirements and assorted mandates, the following "Do's and Don'ts" simplify your compliance efforts. If you need more information, please contact pci@sunocoinc.com or your area representative.

DO - Make sure that your back office system does not store track data or debit card PIN numbers.

DO - Physically secure your system and do not allow anyone access to the office.

DO - Always make sure that your system is protected by anti-virus software.

DO - Update the software to ensure you are protected against the latest/greatest virus threats.

DON'T – Access the Internet through any POS equipment.

DO – Make sure that you really need to keep all of the files/information that you're keeping.

DO – Connect your PC to your POS according to your POS's PABP/PA-DSS Implementation Guide.

DON'T - allow unauthorized people to touch your machines. When in doubt, contact the maintenance help desk to verify that you have an authorized repair person.

DON'T – Store unnecessary electronic transaction data or personal information.

DON'T – Use the POS machine to surf the internet, read personal email, or any other unauthorized activity.

PIN PADS

PIN Pads are the devices that customers use to enter their debit card Personal Identification Number (PIN). Along with using current software versions, compliance with PCI requirements and assorted mandates, the following "Do's and Don'ts" simplify your compliance efforts. If you need more information, please contact your area representative or pci@sunocoinc.com.

DO – Train managers and cashiers on PIN Pad security

DO – Perform weekly terminal inspections. Look at the unit for unauthorized hardware or any changes. Check the serial number and perform electronic serial number validation.

DON'T – Allow unauthorized service calls or unknown people to service the unit.

DO – Change the default PIN Pad password to a strong password.

DO – Change the password often.

DO – Mount PIN pads to the counter.

DO - Use the PIN pad shields provided when counter mounting the PED.

STORE NETWORK

Your store network includes your point-of-sale machine, the back office, routers, and firewalls. Basically your network connects all of these pieces so that each can talk to the other.

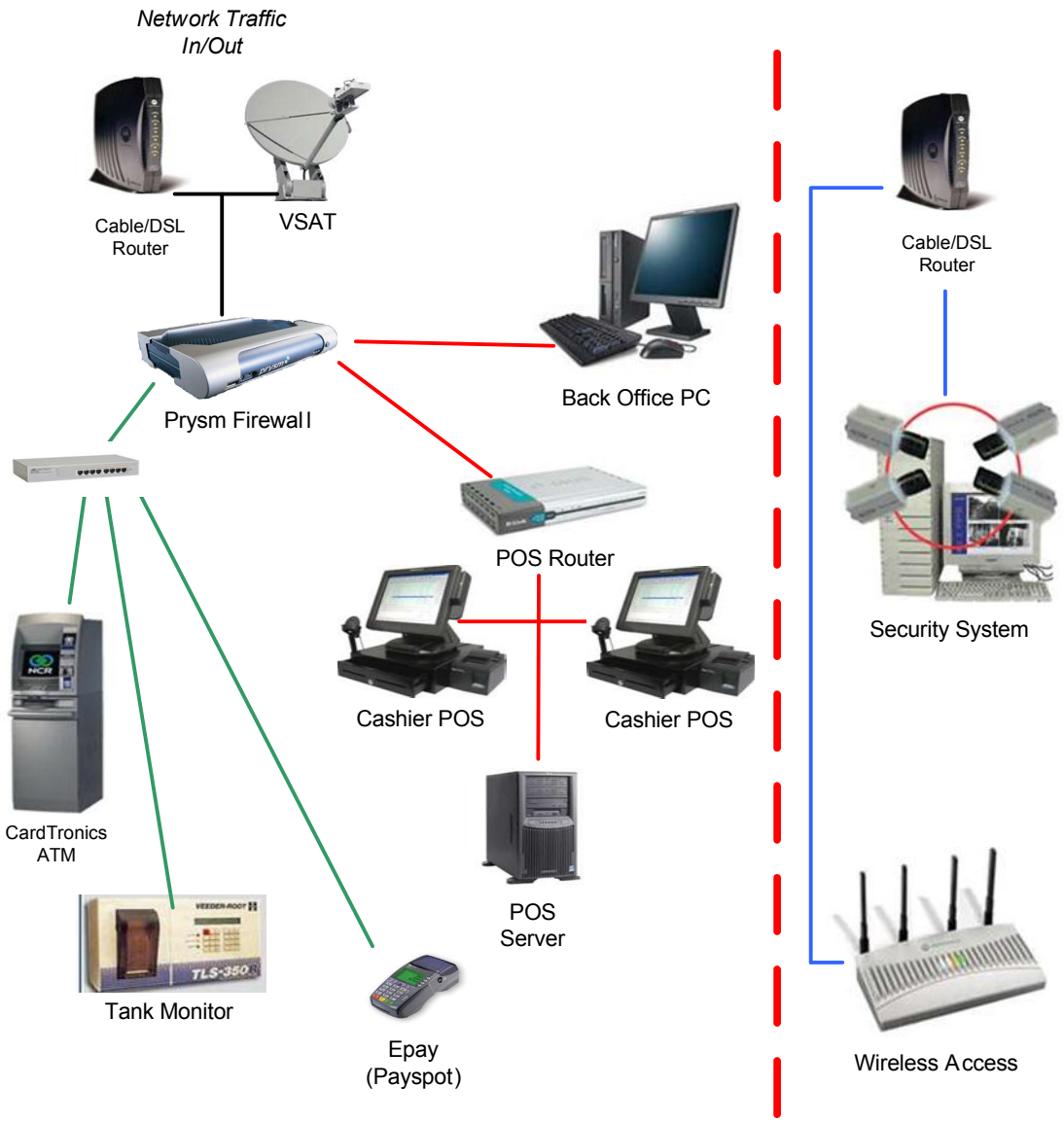
Your network also allows your site to talk to the outside world, including the Internet, your banks, Sunoco, and your credit card authorizer.

Configured incorrectly, your network is a big vulnerability to hackers and data thieves. If a router allows incoming traffic, a thief could get to any of your files. If a firewall is vulnerable, a hacker could get into your network and into any of your files. (note: this is why best practices suggest you limit the amount of data on these machines).

Two new pieces of equipment are discussed here. One is a firewall, the other is a router. A router is a device that sends data packets to their destinations. Each data packet has an 'address' and the router 'reads' the address, checks it against its table of addresses, and sends the data packet on its way. Think of a sorting machine at the post office and you have a good idea how a router works.

A firewall is a device that sits between a private network (your store) and a public network (the Internet), allowing or denying network traffic each way. A firewall has 'rules' telling it which traffic can come or go.

The following drawing shows the pieces of a network installed to Sunoco's best practices:



The cable router, the VSAT, or DSL (and the phone line for dial back-up) enter the store through the Prysm firewall. The Prysm is a firewall that separates traffic between the Internet, the store's internal LAN, the secure network used to process credit cards, and the vendor network used to maintain your equipment. It is very important that devices be plugged into the proper location on the Prysm, and that other devices are not put between it and the broadband connection.

The back office PC also comes into the Prysm firewall. This machine is used to perform basic computing tasks necessary to run your business (accounting, for instance) and should never be connected to the

same LAN segment as a point-of-sale system without going through the Prysm.

All of these devices, the router, VSAT, and back office PC connect to the point-of-sale router. The POS router is a separate device that ensures devices in the store can communicate and correctly pass information necessary to make the technology at the store function properly.

Properly connected, your store network allows you to conduct your business more efficiently. Incorrectly connected, your store network could provide a wealth of information to a data thief.

If you have questions about your store network, contact the operations help desk, your equipment vendor, or an ASC technician.

FIREWALLS

DON'T – Open the firewall to allow "All Traffic Anywhere." Only allow necessary ports and addresses into the firewall.

DO – Change the default firewall and router administrative login passwords.

DON'T – Tape the password to the outside of the router.

STORE OPERATIONS

Update your store operating policies, procedures, training materials to reflect the PCI Digital Dozen, found on page 5. Specifically address the items 7 through 12:

7. ***Restrict access to cardholder 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.***

Treat personal information (customer and employee) like it is hazardous waste. If you don't need it, don't keep it. Destroy unnecessary hard copies by shredding and move records you have to keep offsite using a secure storage facility.

Receipt/Report/Record Storage

Credit card receipts and journal information are no longer needed after seven (7) months. For the time you keep these records, keep them in a locked, secure place and limit access to them. Ideally, use a secure off-site storage facility.

After seven months, destroy the records by shredding, redacting, or hiring a qualified record storage/destruction company.

Training

Employees should be trained on how to handle sensitive information and credit card data. New employees should immediately understand how to handle customer's payment and private information. All employees should receive refresher training annually.

Store IT

Any one who works on your POS equipment, back office, dispensers, ATMs, or network must have training on PCI compliance and data security. It's very easy to add a device to a store's network that voids all of your hard work.

Only use certified ASC technicians and NEVER allow a stranger access to any computer, records, router, network, dispenser, or PIN pad.

User IDs

DON'T - use default or vendor-provided passwords

DON'T – Share user accounts or passwords. Each person should have his/her own account.

DO - use complex passwords (see page 17)

DO - change passwords every 90 days.

DO - disable accounts when people quit or are terminated.

DON'T – Write the passwords down on a sticky note attached to the monitor, stuck in a drawer, or in a notebook next to the machine!

Applications & Updates

DON'T – add any other applications, programs, games or utilities to Sunoco-supplied machines.

DO - install security patches as available from the software vendor.

DO- run virus scans and keep the virus scan utility updated

DON'T – Surf areas that you would not go with your family present.

DON'T – Download any information from an un-trusted source.

IN CASE OF A BREACH

In the event of a breach or compromise, immediately call 1-800-SUN-CALL to report the incident. If you suspect a stolen record, a compromised POS or back office computer, or that anything is amiss, you should immediately report it to 1-800-SUN-CALL.

FOR MORE INFORMATION

www.PCISecurityStandards.org - Homepage of the PCI Security Council

www.SunocoNet.com – Sunoco portal under a separate tab labeled 'Compliance.'

www.Microsoft.com – information about all Microsoft products.

www.PaymentSecurityPros.com – payment security program management resource.

DEFINITIONS

PCI Council

The PCI Council was originally founded by the major credit card brands (Visa, MasterCard, AMEX, Discover, JCB). Today, the council is an independent organization devoted to payment account data security. This effort is intended to provide data security standards as an industry to avoid icky, nasty government intervention.

Strong Passwords

A strong password is sufficiently long, random, and difficult to guess (by both humans and computers) effectively protecting a computer from unauthorized access.

The following are some hints to make a strong password:

- Use BOTH upper- and lower-case letters
- Use numbers and punctuation marks
- Use between 8 to 20 characters
- Use special characters: i.e., ! @ # $ % * (+ = , < > : " '
- Consider using a phrase or a song title. For example, "Somewhere Over the Rainbow" becomes "Sw0tR8nBO" or "Smells Like Teen Spirit" becomes "sMll10nspT"
- Make your password easy to type quickly

Triple DES

An encryption scheme which involves applying the DES algorithm to a text three times.