Payment Card Industry Data Security Standard

PCI DSS Training Course101 for

Work Force and IT – Risk Staff

Why Does PCI DSS Exist

- PCI DSS was born out of necessity by the Card Brands as a measure to allow for self regulation and hope to prevent the Federal Government from dictating what is required for data protection.
- It started in 2002 by Visa as Visa CISP after several major breaches occurred and the Federal Government showed signs of wanting to regulate this activity
- It is the International Requirements for what is to be done to protect Cardholder Data (CHD)
- It has grown since the 2002 start to become the international standard of the world for Credit Card Data Protection as it relates to the Five Participating Card Brands as release in version 1.0 in 2004

Who Companies Make Up PCI SSC

- The Five Participating Card Brands are
  - American Express
  - Discover
  - JCB
  - MasterCard
  - Visa

What Does PCI Cover?

- PCI DSS Covers
  - ***People*** – All people that can or do interact with the CHD and/or the CDE
  - ***Process*** – All Processes that touch or impact the CHD
  - ***Technology*** – All Technologies that are used to Secure, Administer, Manage, or Touch the CDE and CHD

What are the Requirements

PCI DSS Requirements Overview

Six Goals, Twelve Requirements

Six Goals, Twelve Requirements	
Build and Maintain a Secure Network and Systems	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. Protect all systems against malware and regularly update anti-virus software or programs 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. Identify and authenticate access to system components 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 for all personnel

What Is PCI Cardholder Data?(CHD)

- PCI CHD is
  - Full Track Data (Track 1, 2, and 3)
  - Full Primary Account Number (PAN)
  - Sensitive Authentication Data (SAD)

Why am I Required to Comply With PCI DSS

- For your company to conduct business someone decided that accepting Credit Cards for Payments was a method of choice for payments
- Your company went to your processor or acquirer and requested the ability to accept credit cards for payments
- Your company signed a contract for this ability that stated you will be compliant with the PCI DSS requirements and all other regulations and requirements related to this business use of credit card payments

Where Do You Interact With Cardholder Data (CHD)

- Your interaction with CHD occurs when
  - You take a payment card for payment
    - Credit
    - Debit
  - When the customer gives you the card number orally or in written format
- When you find a payment card

What if the CHD is Old?

- Old does not matter if it is CHD you are required to protect it, PAN, or remove it SAD
- Old data is generally found in older DR tapes and Backups
- In Older Emails
- On Local Drives
- On Receipts for Historic Stored Records
- On the Hotel Folios

Point of Sale (POS) Devices

- POS devices are the devices used to read the credit card data
  - They can be standalone
  - They can be attached to a register
  - They can be wireless hand held devices
  - The can be dongles like but not limited to
    - Square
    - PayPal

Point of Sale Devices (POS)

- PCI requires the POS devices to have
  - Inspection for Substitution
  - For Tampering
- Your role is the first line user of these devices and you should be aware of what they look like and what to watch for to ensure they have not been
  - Substituted
  - Tampered With

I am Not Technical-How Can I Inspect a POS Device?

- PCI Requirement 9.9 is the one that you should know as this is the one for the inspection and substitution
  - To this end you can check that the seals
    - Are the same as when you started your shift or work day
      - These will be placed on the device by management and have tamper proof ability
    - The devices should not be used if it looks like the one on the following page
  - Any suspected or known issue should be reported to management immediately

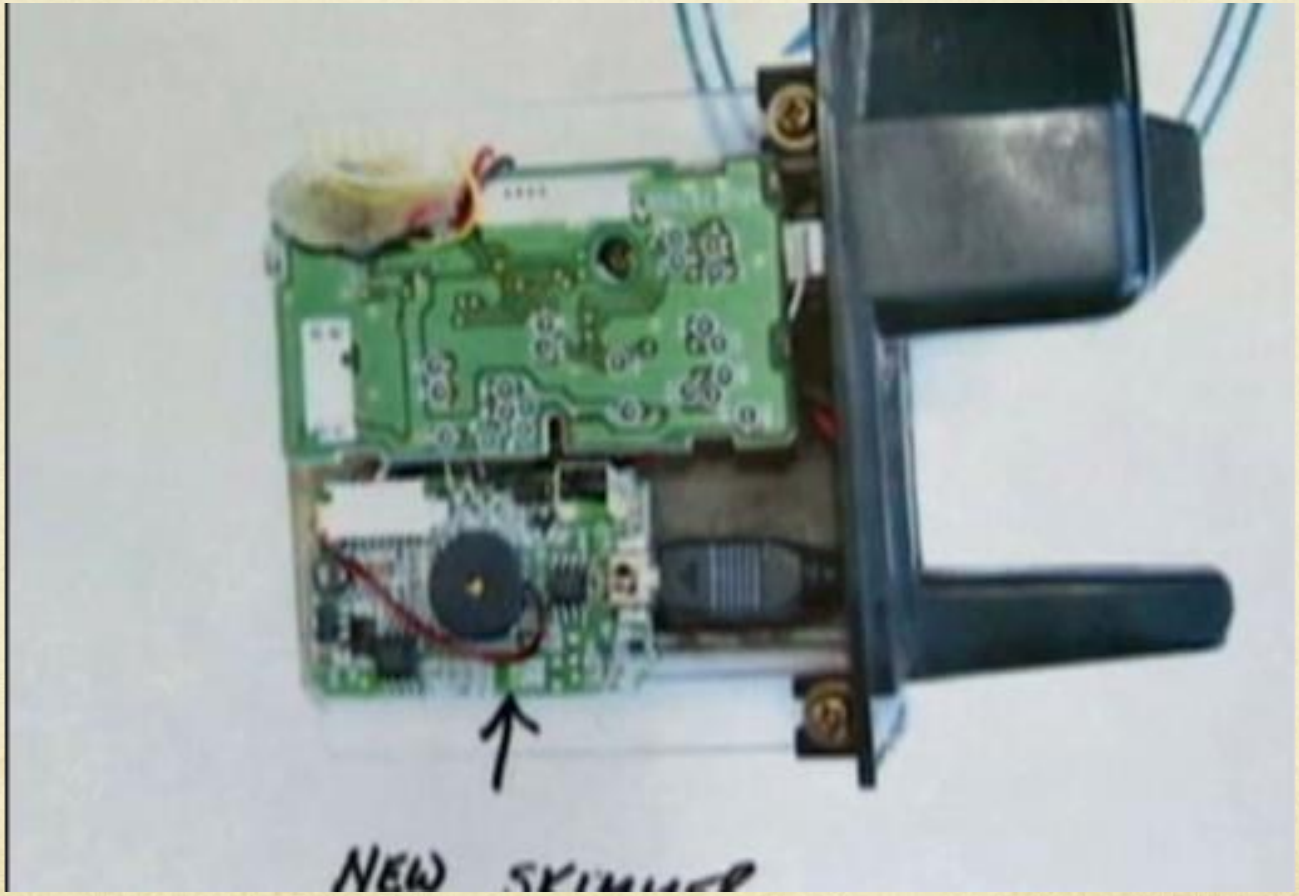
A Bad POS for Use

Another Bad POS

POS Above

- The photo above is of a “SKIMMER” that was in place at a grocery chain
- This shell overlays the real device but has a chip built into it as well that records all of the CHD that the real device captures
- The inspection process this grocer did not catch this device until their was a breach
- Security Seals like you see on fuel pumps would have caught this immediately if anyone was looking

Skimmer on Fuel Pump



ATMs Have Been a Skimmers Gold Mine

- ATMs have an implicit Trust
- Some are free standing Kiosks
- Some are in Kiosk enclosures where you need to swip your card to enter
- Some are Built into the side of buildings
- All are easy Targets for Theft and Skimmers

Programming the ATM

- Most ATMS have the ability to be programmed and managed from
  - The back of the device by attaching a Laptop
  - The front side keyboard
    - Has the ability to change the denomination
      - Generally they are set to 20 dollar bills
        - A thief will reprogram for a 1 dollar bill thus a request for 200 dollars now yields 2,000 dollars

What About ATMs

An Altered PIN Pad Mask

Altered Mask Part 2

Card Skimmers in ATM

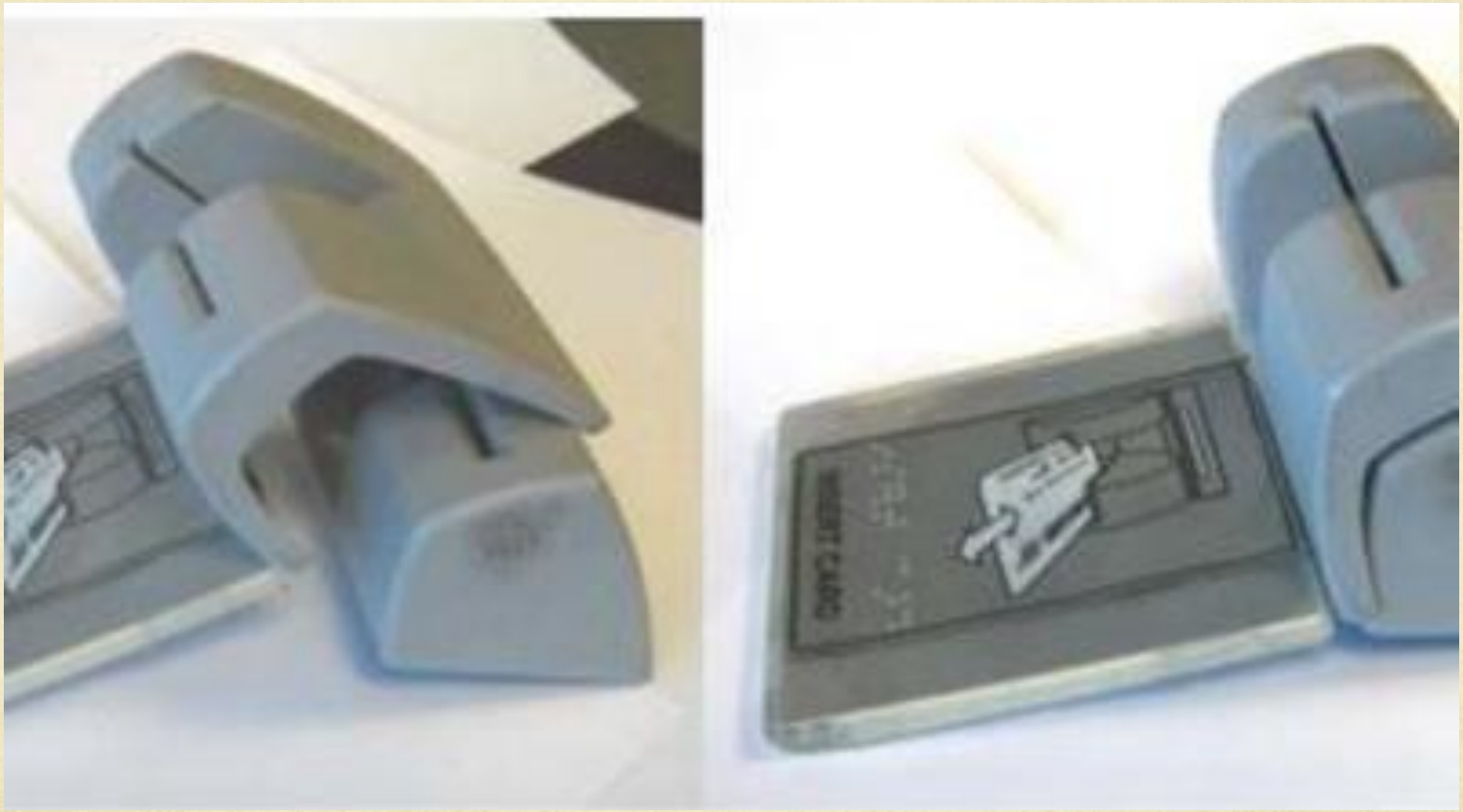
Skimmer

No Skimmer

More Fun With ATMs

The Card Slot

Installed From Gizmo AU Post



How to Inspect?

- What to Look For When You Are "Inspecting"
  - Yes, it is a POS device
  - Is the Serial Number the Same?
  - Have the Cables been Unplugged?
  - Has The Case Been Opened?
- A key for this inspection is to use a serialized ***"Tamper Proof Seal"*** to allow for proof of no tampering or substitution
- Key for substitution is the serial number or your property tag that is not removable easily for this proof

Bad POS Continued

- Yes the POS was in use at a fast food restaurant
- Yes customers were swiping their payment cards in it
- Yes this is stupid and should have be shout down
- Yes things like this should be reported immediately and you should not use a device in this condition

What Should You Do if the POS shows signs of Tampering or Substitution

- Actions to take
  - Stop the use of the device
  - Notify Security and IT
  - Gather the inspection records to see when this could have occurred
  - Unplug the device from the equipment it is attached too
  - Remove the devices from public and general staff access
  - Report this to the appropriate internal staff member for action

What You Should Not Do?

- Do not reset the POS to its default settings by use of the reset input from the number pad
- Do not reset the POS to its default settings by use of the reset button
- Allow the POS device to stay in use

The latest Skimming

- Recently thieves have been using their smart phone in two ways to get your credit card data.
  - First the turn on video as you pull your card out and place it into the ATM or POS device
  - Then they attach a Flir One to the phone and as soon as you leave they read the heat signature of the key pad you just used to enter your PIN number
- Not bad for a smart phone

Now it is your Turn