cardconnect®
PARADISE

PCI-DSS Security Awareness

What you need to know
to protect your customers' data

PCI DSS – What is it?

Payment Card Industry,
Data Security Standard

Developed by the five major card brands, to address potential areas of vulnerability and guide organizations in best practices to maintain the integrity of cardholder data.

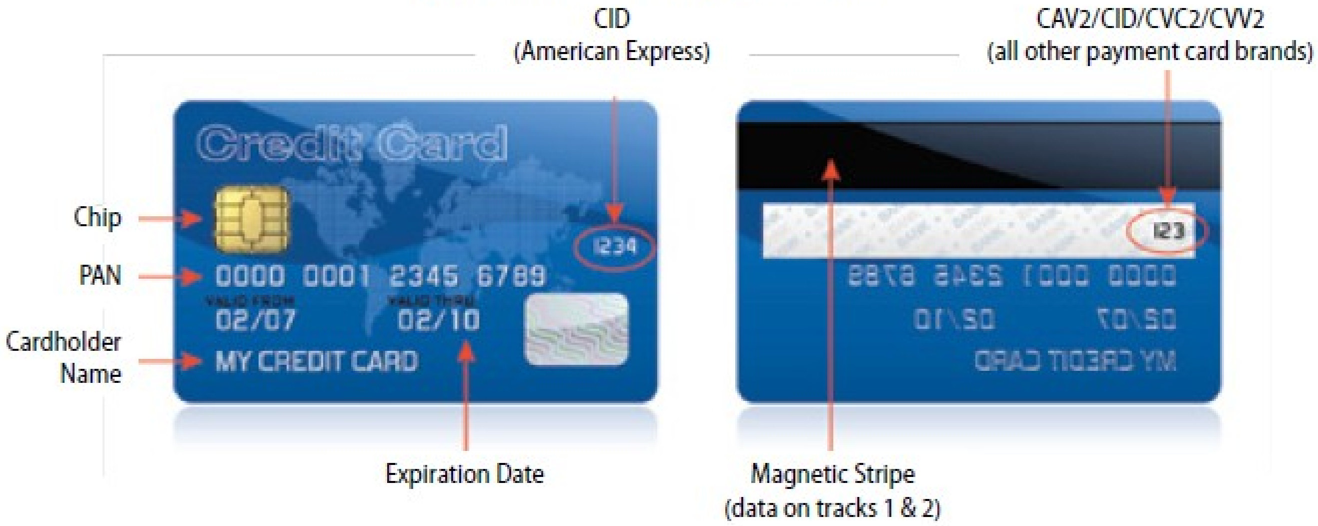
The Cost of Noncompliance

- Fines, penalties, and increased fees
- Lost revenues, customers, jobs
- Negative market image
- Cost of reissuing credit cards
- Lawsuits, insurance claims
- Average cost of each stolen card or record = **$141***
- Global average cost of a data breach = **$3.62 million***

*2017 Ponemon Cost of Data Breach Study

Verify Card Elements & Security Features

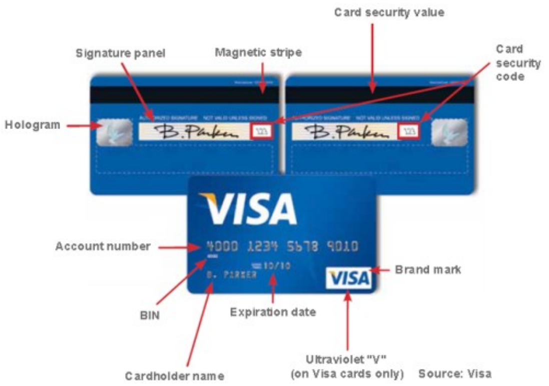
Types of Data on a Payment Card



When processing a credit card transaction…

Verify the following:

- The card is signed.
- The expiration date has not passed.
- The signature on the receipt matches the card signature.
- The receipt does not show the full 16-digit account number or card validation code.



Source: Visa

PCI DSS Requirements

Goals	PCI DSS 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.

Focus on:

Implementing Strong Access Control Measures which Include:

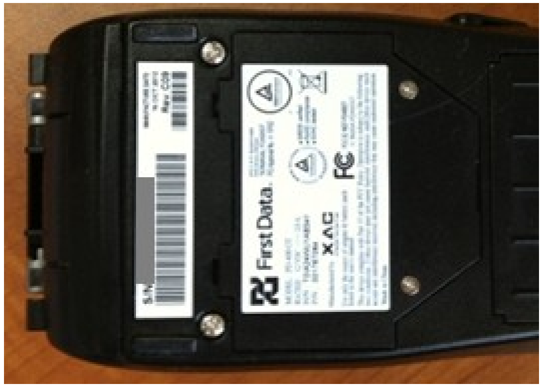
Restricting physical access to cardholder data.

Restrict physical access to cardholder data

- Periodically inspect all credit card devices for tampering or substitution.
- Never allow direct physical access to the credit card device, without supervisor approval.
- Be aware of suspicious behavior.
- Immediately report tampering or evidence of "skimming" or any breach to your supervisor.

Periodically inspect all credit card devices for tampering or substitution

Tampering / Substitution – What to look for



Your credit card terminal will have a sticker on the back that provides the serial number for the device.

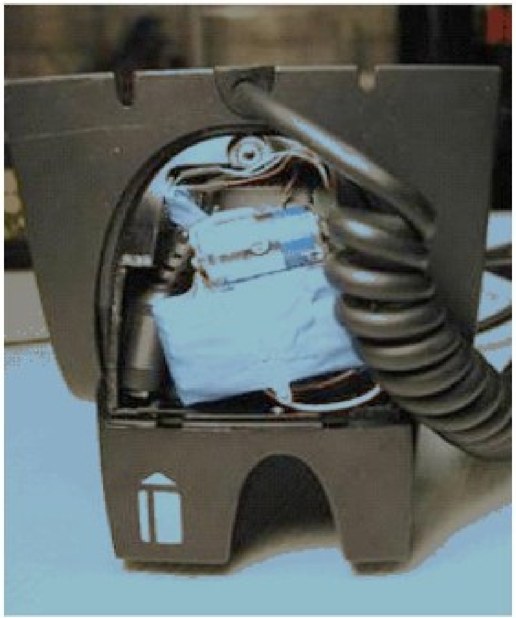
Regularly check for altering or tampering. If the numbers do not match, the terminal may have been replaced.

Periodically inspect all credit card devices for tampering or substitution.

Tampering / Substitution – What to look for

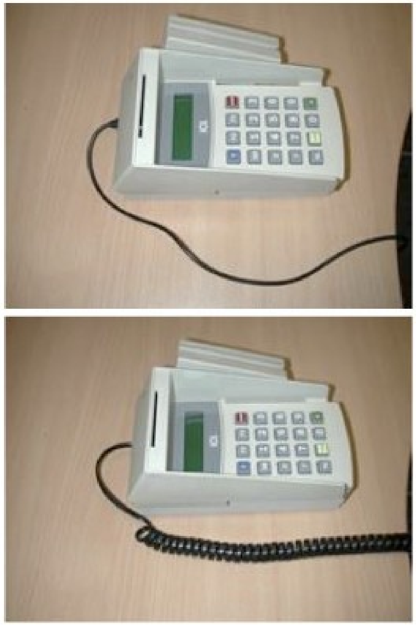
Be aware of all access points to the inside of the device.

A skimming device has been added to the inside compartment of this device.



Periodically inspect all credit card devices for tampering or substitution.

Tampering / Substitution – What to look for



In the bottom picture, the cord has been replaced, this could allow capture of credit card data, if left unnoticed.

Never allow direct physical access to the credit card device without owner/manager approval.

Never allow access to credit card terminals without owner/manager approval.

Always verify with your supervisor the identity of any third-party claiming to be repair or service personnel.

Be aware of suspicious behavior.

Be aware of suspicious behavior around devices (for example, attempts by unknown persons to unplug or open devices).

Immediately report tampering or evidence of skimming or any breach to your owner/manager.

If you become aware of evidence of tampering, replacement, or any other breach of credit card data, **contact your owner/manager immediately**.

PCI DSS – helpful links

- PCI DSS: https://www.pcisecuritystandards.org/
- American Express: www.americanexpress.com/datasecurity
- Discover: www.discovernetwork.com/fraudsecurity/disc.html
- JCB International: http://partner.jcbcard.com/security/jcbprogram
- MasterCard: www.mastercard.com/sdp
- Visa Inc: www.visa.com/cisp

Supervisor Name	Signature	Email	Date

PCI DSS Security Awareness Training has been reviewed with the following staff.

Staff Name (Print)	Signature	Email	Date

Questions? Visit: **Charge-it-now.com** or call Dan Arndt at **480.289.6304**