

Payment Card Industry Data Security Standard (PCI DSS)

Briefing for National
Restaurant Association
Members

July 20, 2007

Type of merchant at greatest risk of card data security breach:

- Not Internet-based e-commerce merchants
- Highest risk merchants have following profile:
 - Single location or part of chain
 - Predominantly card-present, “retail” transactions
 - Unsecured Internet-accessible store network
 - DSL, Cable Modem, Wireless
 - Non-compliant POS software
 - Storing card data elements

PCI Data Security Standards (DSS)

- Developed by major payment card brands
 - Visa, MasterCard, American Express, Discover
- PCI DSS is a common standard
 - PCI DSS is the foundation
 - Each brand has their own data security rules based on PCI-DSS
- All U.S. merchants subject to brands' rules
 - Acceptance of card brand's rules a condition of accepting each brands' cards

Merchant levels - summary

- Level One
 - 6 million+ annual Visa or MC transactions
 - 2.5 million+ American Express transactions
 - Merchants with known compromises
- Level Two
 - Between 1 and 6 million annual transactions
- Level Three
 - E-commerce merchant / 20,000+ transactions
- Level Four (*)
 - Other merchants (with up to 1 million transactions)

** American Express does not define a level 4. Discover does not use levels.*

Compliance requirements – summary (*)

- Level 1 Requirements
 - On-site annual audit
 - Quarterly network scan
- Level 2 and Level 3 (E-com) Requirements
 - Annual self-assessment
 - Quarterly network scan
- Level 4 - *Recommended*
 - Annual self-assessment
 - Quarterly network scan

* Further information available from sources listed on page 11.

How data security rules are administered

- Visa and MasterCard administer:
 - Through acquiring (merchant) banks
 - Acquirers may work through independent sales groups (“ISOs”)
- American Express and Discover:
 - Directly with merchants
- Card brand’s determine merchant compliance
 - Card brand rules allow penalties to be assessed
- Merchant Card Processing agreements usually
 - Require compliance as a condition of acceptance
 - Allow card brand fines to be automatically charged to merchant.

Merchant liability

- Merchant may experience PCI DSS violations caused by
 - Merchant good-faith reliance on vendors
 - And/or merchant negligence
- Card brands can require security audit at the merchant's expense if compromise is suspected
- If PCI violations are found, the card brand *may hold the acquiring bank responsible, even though there is no direct evidence of how the card data compromise occurred*
 - In turn, the Acquirer will hold the merchant responsible

Common sources of problems

1. Cardholder data is improperly stored on point-of-sales (POS) systems*:
 - Sensitive data being stored on system
 - Card magnetic-stripe information
 - PIN data
 - Often times historical data retained in “log” files

Merchants are prohibited from storing magnetic stripe card data or PINs, even in encrypted form

* POS systems includes Integrated systems and POS terminals.

Common sources of problems

2. POS system software is not updated to the latest compliant versions
3. POS systems and networks use “default” passwords that have not been changed
4. Merchants have unsecured data networks exposed to the public Internet

If your business is a victim of a breach involving payment card data:

- Do not alter the suspected system
 - Attempt to isolate the system
 - If practical, unplug it from the network
 - Change systems' user passwords, yet not 'root' ones
 - Change network passwords
 - Preserve all logs and reports
- Contact your merchant acquirer and other card brands (American Express, Discover)
- Contact law enforcement
- Record in written form all actions taken and when
- Anticipate a forensic data investigation

Additional information resources

- ❑ Contact your merchant acquirer bank, or their agent
- ❑ More information available at the following web sites:

PCI Standards	http://www.pcisecuritystandards.org
PCI Approved Scanning Vendors	https://www.pcisecuritystandards.org/pdfs/pci_qsa_list.pdf
Visa USA	http://www.visa.com/cisp
MasterCard	http://www.mastercard.com/us/merchant/security/index.html
American Express	https://www.americanexpress.com , click on merchants
Discover	http://www.discovernetwork.com/resources/data/data_security.html

PCI DSS - summary

Payment Card Industry Data Security Standard (PCI DSS)

Build and Maintain a Secure Network	<ol style="list-style-type: none">1. Install and maintain a firewall configuration to protect cardholder data2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	<ol style="list-style-type: none">3. Protect stored data4. Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	<ol style="list-style-type: none">5. Use and regularly update anti-virus software6. Develop and maintain secure systems and applications
Implement Strong Access Control Measures	<ol style="list-style-type: none">7. Restrict access to cardholder data by business need-to-know8. Assign a unique ID to each person with computer access9. Restrict physical access to cardholder data
Regularly Monitor and Test Networks	<ol style="list-style-type: none">10. Track and monitor all access to network resources and cardholder data11. Regularly test security systems and processes
Maintain an Information Security Policy	<ol style="list-style-type: none">12. Maintain a policy that addresses information security