

## INTRODUCTION TO PAYMENT CARD INDUSTRY DATA SECURITY STANDARDS (PCI DSS)

### QUESTIONS AND ANSWERS

#### What is PCI DSS?

The *Payment Card Industry Data Security Standards (PCI DSS)* are data and record storage, transmission and system testing requirements designed to help ensure the safe handling of credit card information.

The PCI Data Security Standards are comprised of 12 general requirements.

- Build and maintain a secure network
  - Install and maintain a firewall configuration
  - Do not use vendor-supplied defaults for system passwords and other security parameters
- Protect cardholder data
  - Protect stored cardholder data
  - Encrypt transmission of cardholder data across open, public networks
- Maintain a vulnerability management program
  - Use and regularly update anti-virus software
  - Develop and maintain secure systems and applications
- Implement strong access control measures
  - Restrict access to computing resources and cardholder data to those whose job requires access, a business need-to-know
  - Assign a unique ID to each person with computer access
  - Restrict physical access to cardholder data
- Regularly monitor and test networks
  - Track and monitor all access to network resources and cardholder data
  - Regularly set security systems and processes
- Maintain information security policies.

#### Who set the standards and why does UK have to comply?

The standards are set by the *PCI Security Standards Council*. The PCI Council was created in 2006 to align the separate security programs and standards of major card programs American Express, Discover Financial Services, JCB, MasterCard Worldwide, and Visa International. The PCI Council is led by a policy-setting Executive Committee composed of representatives from the founding credit card companies. A Board of Advisors represents the 279 participating organizations and provides feedback to the PCI Counsel.

#### What are Merchant Levels and why does it matter?

There are four merchant categories, “Levels”, based on the number of transactions processed. The Merchant Level designation (1, 2, 3, or 4) determines the required date of compliance and complexity and frequency of required compliance validations. The compliance requirements include, at a minimum, annual PCI Self-Assessments and quarterly network scans. The PCI self assessment is designed to evaluate data storage and security processes and to identify weaknesses if they exist. A network scan

is a tool that remotely tests operating systems, networks and devices that could be used by hackers to target the private network. The highest level of compliance requirement is Level 1. The lowest level of compliance requirements is Level 4.

A merchant is any organization that accepts credit cards. So, instead of UK as a whole being a merchant, each office or department that accepts credit cards is considered a merchant. UK's merchant card processor has identified all UK card acceptance sites as Level 4 merchants.

### **What are the costs of non-compliance with PCI DSS?**

The costs of non-compliance will result primarily from a security breach if cardholder information is compromised. These costs may include:

- Notifying affected cardholders
- Paying for credit monitoring for the affected parties
- Paying for unauthorized charges
- Implementing needed hardware or software upgrades to comply with a higher level of security that would be required post-breach
- Fines from credit card companies
- Litigation from cardholders, vendors or credit card companies.
- Unfavorable publicity
- Damage to UK's reputation

The Treasury Institute for Higher Education estimates an expected cost of \$182 per account compromised and that a small breach (~5,000 accounts) can cost \$1 million.

### **How do Credit Card Security Breaches Happen?**

#### **Types of Breaches**

- Hacking into networked computers
- Lost or stolen PCs, Media
- Improper Disposal of Records (Paper records not shredded or disposed).
- Fraud
- Mistakenly posting information on the Web

#### **Sources of Breaches**

- Improper storing of data
  - Integrated Point of Service (POS) systems, especially older ones
  - System logs, back-ups
- Insecure applications
- No network segmentation and/or firewalls
- Unpatched systems and/or default configuration
- Insecure wireless access points
- Use of default passwords
- No intrusion monitoring
- Unsecured point of sale technology.

### **What is next?**

Staff from Information Technology, Internal Audit, UK Healthcare, Office of Legal Counsel and the Office of the Treasurer is developing a compliance plan. Some of the future items to expect are:

- New business procedures related to credit card acceptance and processing, including a required application to become a credit card merchant.
- Required training session on PCI compliance for credit card merchants.
- Self Assessment Survey. All Departments will be required to complete a comprehensive PCI Self Assessment Survey based on the type of transactions processed and the level of activity.

For more information on PCI DSS please visit [www.pcisecuritystandards.org](http://www.pcisecuritystandards.org).