PCI DSS AWARENESS TRAINING

TRAINING SCOPE

- What is PCI DSS?
- The 12 Principles
- What are we protecting?
- Consequences of non-compliance
- Accepting, Storing and Disposing Card Data
- Signs of Suspicious Activity
- Basic Security Measures
- PCI Audit
- Your Responsibilities
- Incident Response
- Conclusion and Additional Resources

WHAT IS PCI DSS?

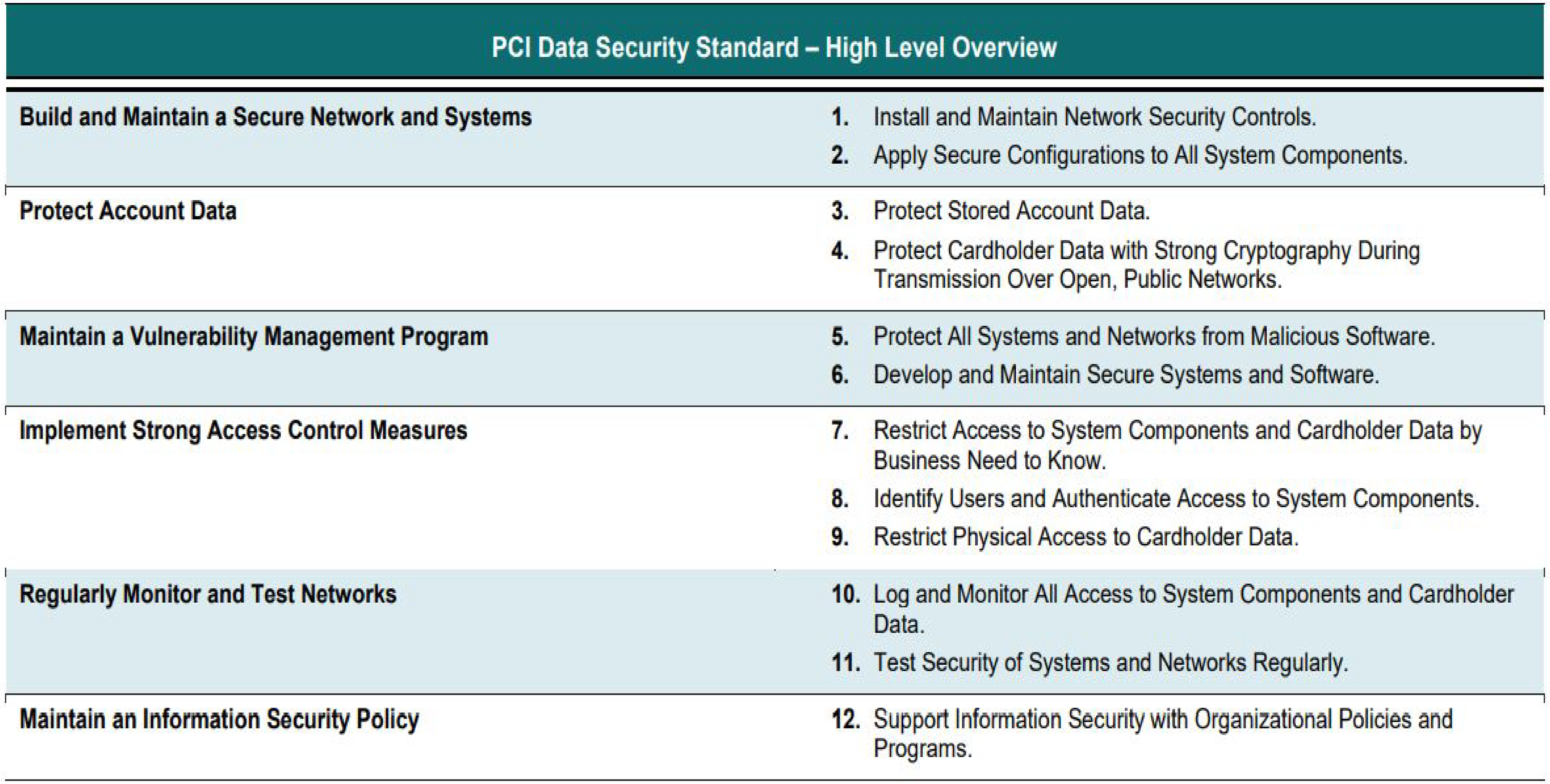
Payment Card Industry Data Security Standard (PCI DSS) is a comprehensive set of controls, processes, and other requirements designed to enhance payment card data security around the collection, storage, retrieval, and handling of cardholder data.

It applies to all entities that accept, store, process and/or transmit cardholder data.

The Payment Card Industry (PCI) was founded in 2006 by American Express, Discover, JCB International, MasterCard & Visa Inc. to help organizations understand and implement standards for protecting cardholder data. It is currently governed by the PCI Security Standards Council.

THE 12 PRINCIPLES

The PCI Standards are broken down into 6 primary standards that are further broken down into 12 secondary standards that must be adhered to, in order to ensure that our environment and customers remain safe.



PCI Data Security Standard – High Level Overview

Build and Maintain a Secure Network and Systems	1. Install and Maintain Network Security Controls. 2. Apply Secure Configurations to All System Components.
Protect Account Data	3. Protect Stored Account Data. 4. Protect Cardholder Data with Strong Cryptography During Transmission Over Open, Public Networks.
Maintain a Vulnerability Management Program	5. Protect All Systems and Networks from Malicious Software. 6. Develop and Maintain Secure Systems and Software.
Implement Strong Access Control Measures	7. Restrict Access to System Components and Cardholder Data by Business Need to Know. 8. Identify Users and Authenticate Access to System Components. 9. Restrict Physical Access to Cardholder Data.
Regularly Monitor and Test Networks	10. Log and Monitor All Access to System Components and Cardholder Data. 11. Test Security of Systems and Networks Regularly.
Maintain an Information Security Policy	12. Support Information Security with Organizational Policies and Programs.

WHAT ARE WE PROTECTING?

PCI-DSS is not a substitute for overall security practices. It is aimed at one thing - protecting card and transaction information no matter how it is collected, stored or transmitted.

Protecting credit card and transaction information no matter how it is
collected
stored
transmitted

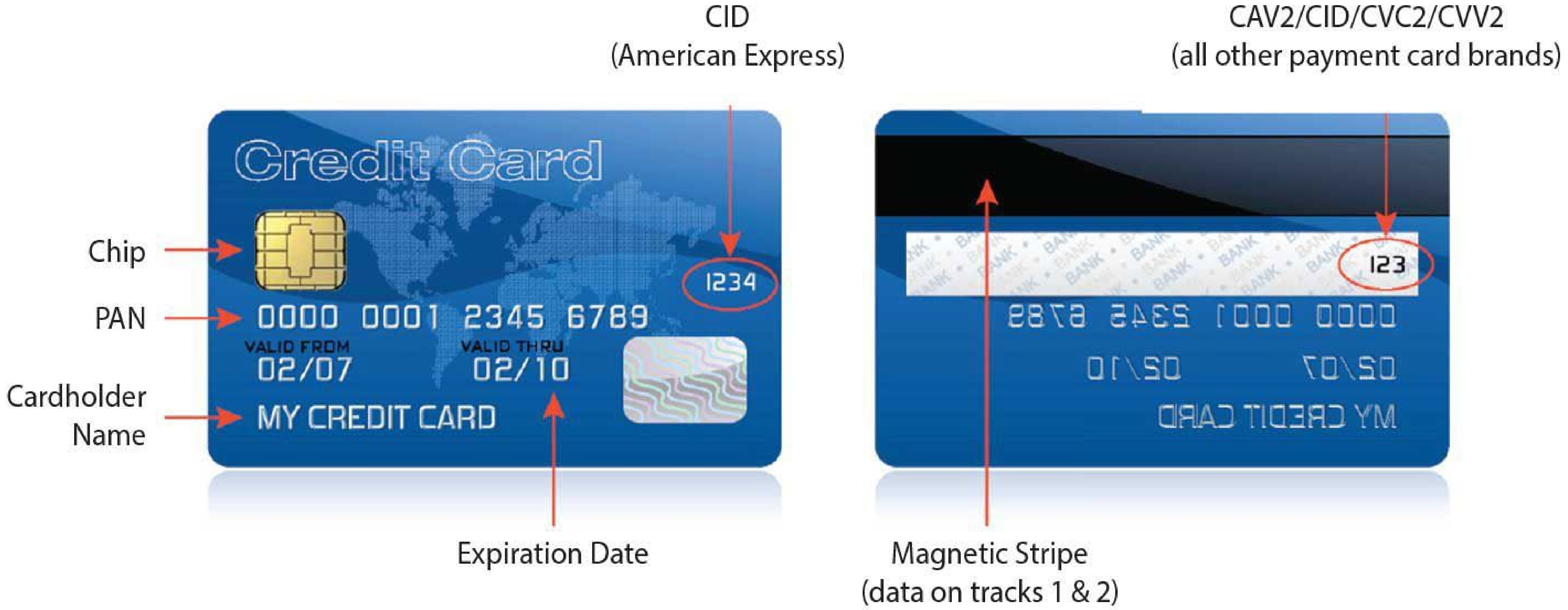
© The Security Awareness Company, LLC

WHAT ARE WE PROTECTING?

Hackers want cardholder data. By obtaining the Primary Account Number (PAN) and sensitive authentication data, a thief can impersonate the cardholder, use the card, and steal the cardholder's identity.

Take a look at the payment card diagram below. Everything at the end of a red arrow is sensitive cardholder data. The PIN (Personal Identification Number), information on the magnetic stripe and CVV2 are regarded as Sensitive Authentication Data (SAD) and must never be stored, even when encrypted. You must have a good business reason for storing anything else, and that data must be protected.

Types of Data on a Payment Card



CONSEQUENCES OF NON-COMPLIANCE

As a business who accepts and issues payment cards, we are responsible for protecting the data of our customers. If we do not, some (if not all) of the following could happen:

- Loss of revenue and downtime for systems that are breached.
- Fines to Queen's University by the Acquirers and stricter PCI requirements.
- Liability for damages.
- Potential loss of payment card acceptance privileges.
- Reputational damage.

ACCEPTING, STORING AND DISPOSING OF CARD DATA

Any business process that does not involve the customer entering their data directly into a payment acceptance terminal like a web portal or POS, adds additional vulnerability. For example, accepting a card number over the phone, writing it down, and processing later.

You are responsible for the chain of custody for any payment card data that you write down. This data is to be destroyed immediately after the transaction is completed.

When card data is no longer needed, it should be destroyed by shredding paper copies, wiping media or hard drives and wiping back-up copies.

Payment card information is never to be received via end user messaging such as voicemail, e-mail, instant message, or social media platforms.

© The Security Awareness Company, LLC

SIGNS OF SUSPCIOUS ACTIVITY

- A secured, locked cabinet with payment card data has been broken into or looks damaged.
- Lost paper forms containing payment card data.
- Suspicious behaviour around devices.
- A skimming device or unusual attachment on a POS device.
- A broken tamper proof seal on a POS device.
- Multiple small transactions through an online store or e-commerce account.
- Multiple refunds going to the same card.
- Different serial numbers on the PIN pad machine indicating the device has been switched.
- Unfamiliar equipment surrounding your PCI terminal or POS device.
- A vulnerability appears in the weekly network scans.
- ITS finds a possible issue during their daily checks of the PCI network and hosting environment.

BASIC SECURITY MEASURES

- Always complete a visual inspection on every device to be used for payment acceptance for any signs of tampering. This includes your PCI terminal for keyloggers.
- Where card data is written down, it must be stored in a locked cabinet in a secured area. Remember to destroy cardholder data once transactions are completed using a cross-cut shredder.
- DO NOT write down or share passwords. Passwords are confidential and should be protected.
- Remember the incident response plan and report all incidents accordingly.

PCI AUDIT

Annually, we are required to go through a PCI DSS audit with an external Qualified Security Assessor (QSA). This process validates that our internal controls meet the requirements of PCI DSS.

The audit involves evidence collection, in-person/remote interviews and onsite inspections.

The PCI Working Group distributes declaration documents to all existing merchant accounts to gather information on payment streams. It is imperative that these be filled out accurately and kept updated throughout the year. The declaration document contains information such as:

- Technical description of how card data is accepted
- Business description of why card data is accepted
- Current representation of the users
- Roles of each user
- Devices used to accept card data
- URL of e-commerce applications used
- Third-party service providers (TPSPs)
- Diagram of the credit card handling process

The information provided is used to maintain an accurate inventory and is used to pre-fill the Self-Assessment Questionnaires (SAQ) and Attestation of Compliance (AOC) documents, required for the audit.

PCI AUDIT

For the in-person interviews/onsite inspections, the QSA typically will, depending on payment stream type:

- Inspect any devices used (PIN Pad devices, PCI terminals).
- Confirm their locations and inventory are as stated in the declaration document.
- Check to see that card data is secured in locked cabinets when written down.
- Ensure PIN Pads are physically secure when not in use.
- Confirm that passwords are not written down.
- Verify processes for payment stream are accurately described.
- Confirm inspection logs for devices.
- Verify incident response processes with staff.

For evidence gathering, the QSA typically will, depending on payment stream type:

- Collect evidence of Quarterly ASV Scans (e-commerce).
- Request for evidence of patching activities (e-commerce).
- Collect Attestation of Compliance documents and responsibility matrix for all TPSPs.
- Collect inspection logs.
- Validate code snippets for URL redirects or iFrame calls.

YOUR RESPONSIBILITIES

Based on how you accept payment, you are also responsible for the following:

SAQ A (E-commerce)	**SAQ C-VT (Virtual Terminals)**	**SAQ B-IP/P2PE (Pin Pads)**
Changing vendor default passwords	Inspecting PCs and Wyse boxes before use	Inspecting PIN Pads before use
Applying applications, OS and firmware patches	Submitting quarterly inspection logs	Submitting quarterly inspection logs
Ensuring vulnerability scans are running and results are remediated within proper timelines		
Ensuring Quarterly ASV scans are completed (Applicable for Self-hosted)		
Ensuring user IDs and passwords meet PCI DSS requirements		

YOUR RESPONSIBILITIES CONT'D

You are also responsible for the following:

- Completing all required trainings and signing the Payment Card Security & Ethics Agreement annually (for a fillable version of the form save the form to your device then open with Adobe).
- Protecting cardholder data in accordance with Queen's Policy and Procedure.
- Reporting suspected incidents or breaches following the Incident Response sections of the Procedure listed above.
- Directing questions about PCI to either your departmental PCI Merchant Contact or to the PCI Compliance Officer.
- Updating the PCI Compliance Officer of any changes to your payment stream, including:
    - ✓ Change of URL, application used or architecture for E-Commerce payment streams.
    - ✓ Change of Third-Party Service Provider.
    - ✓ Change of Users, PIN pads, PCI Terminals and/or location.

INCIDENT RESPONSE

If you notice anything suspicious or unusual surrounding your merchant account, you should:

- Immediately stop taking payments on the compromised station and disconnect from the PCI network (if applicable). Only shut down the device if this is the only way to prevent the system from being connected to the network (ex. a cellular PIN pad).
- Report the suspected breach or incident to:
  - ✓ During Business Hours: IT Support Centre at 613-533-6666.
  - ✓ After Business Hours: IT On-Call by emailing spnotice@queensu.ca. If you don't receive a response within 30 min, contact 613-217-2474.
- Notify your manager and await further instruction. The PCI Compliance Officer will advise when payment processing may resume.

CONCLUSION AND ADDITIONAL RESOURCES

This concludes the PCI DSS Awareness training. Remember, if you have any payment-related questions or notice anything suspicious or unusual, contact the PCI Compliance Officer by sending an email to: finpcico@queensu.ca

If you would like additional information on these standards, please visit the PCI website.

The PCI Team…

Financial Services
Queen's University
355 King St W, 3rd Floor | Kingston, ON | K7L 3N6
e-mail: finpcico@queensu.ca
http://www.queensu.ca/financialservices/publications-policies-procedures/PCI