PIN Pad Security Training and Procedures
# Table of Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>PIN Pad Security</td>
<td>2</td>
</tr>
<tr>
<td>Objectives</td>
<td>2</td>
</tr>
<tr>
<td>Inspection Frequency</td>
<td>2</td>
</tr>
<tr>
<td>Schedule of Submission</td>
<td>3</td>
</tr>
<tr>
<td>Inspection Process</td>
<td>3</td>
</tr>
<tr>
<td>PIN Pad Serial Number Inspection</td>
<td>3</td>
</tr>
<tr>
<td>PIN Pad Tampering Inspection</td>
<td>3</td>
</tr>
<tr>
<td>Verify Identity of Third-Party Persons</td>
<td>4</td>
</tr>
<tr>
<td>Evidence of Cable Substitution Inspection</td>
<td>4</td>
</tr>
<tr>
<td>Physical Security Inspection</td>
<td>4</td>
</tr>
<tr>
<td>PIN Pad Security Best Practices</td>
<td>5</td>
</tr>
<tr>
<td>PIN Pad Pictures</td>
<td>6</td>
</tr>
<tr>
<td>References</td>
<td>7</td>
</tr>
<tr>
<td>Appendix – PIN Pad Inspection Log</td>
<td>8</td>
</tr>
</tbody>
</table>
PIN Pad Security

Payment Card Industry Data Security Standard (PCI DSS) is an externally driven mandate from the Payment Brands (i.e. Visa, MasterCard, Amex, JCB and Discover) imposed on all merchants accepting credit cards for payment of goods or services. Every organization that retains, transmits, or processes card holder data must comply with the PCI DSS. This is enforced by our “acquiring bank” who has the right to de-activate your ability to accept credit card payment.

As part of this compliance, there are specific requirements around the physical and logical security of PIN Pads or Point-of-Sale (POS) devices or terminals. These requirements are in place to protect against fraud by way of tampering.

Merchants are required to have controls in place to protect any device that captures payment card data used in card-present transactions (not manual key-entry) against direct physical tampering and substitution.

Objectives

- To comply with PCI DSS Requirements 9.9, 9.9.1, 9.9.2, 9.9.3, 12.4, 12.6, and 12.10.1
- To communicate training and awareness of Point-of-Sale (POS) or PIN Pad security responsibilities to all persons who have direct contact with PIN Pads

Inspection Frequency

PCI DSS version 3.2 requires that merchants:

- Maintain a listing of all devices (PIN Pad, POS) that capture payment card data
- Conduct regular inspections of such devices for tampering and substitution,
- Train personnel to be aware of suspicious behaviour and to report tampering or substitution of PIN Pads or POS devices

As outlined in the Procedures for the Acceptance of Credit and Debit Cards, regular inspection of Point-Of-Sale (POS) and PIN Pad devices must be conducted on a weekly basis, at minimum, to detect tampering or replacement of a device, and thereby minimize the potential impact of using fraudulent devices. If a PIN Pad or POS device is not locked up at night, it should be inspected daily.

An inspection log is to be submitted to the PCI Coordinator on a quarterly basis showing documentation of these formal weekly inspections in compliance with PCI DSS Requirements (version 3.2) 9.9.1 and 9.9.2.

DO NOT USE a PIN Pad or POS device if there is any suspicion or evidence of tampering.
Schedule of Submission

<table>
<thead>
<tr>
<th>Quarter</th>
<th>Month</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>June</td>
</tr>
<tr>
<td>2</td>
<td>September</td>
</tr>
<tr>
<td>3</td>
<td>December</td>
</tr>
<tr>
<td>4</td>
<td>March</td>
</tr>
</tbody>
</table>

Failure to submit the inspection log on a quarterly basis may result in the suspension or revocation of your merchant account.

Inspection Process

- Conduct daily checks – routine inspections of your PIN Pad as well as the premises will help you uncover card-reading devices and other illegal equipment such as unauthorized cameras
- Take care of your PIN Pad – treat your PIN Pad as you would cash – it is just as valuable
- Know your Staff – practice due diligence when hiring and supervising employees – fraudsters can operate within your business as well as outside your business

PIN Pad Serial Number Inspection
Check the serial number of both the PIN Pad and the base/terminal to ensure that both devices haven’t been switched for a fraudulent device that will send criminals payment card information every time a card is entered.

PIN Pad Tampering Inspection
Check for the following:

- **Skimming devices** added to the outside of devices which are designed to capture payment card details before they even enter the device – for example, an additional card reader on top of the legitimate card reader so that the payment card details are captured twice: once by the criminal’s equipment and then by the device’s legitimate equipment.
- **Skimming devices** inserted in a terminal (hidden by the SIM card cover plate)
- **Handheld Skimmers** used by corrupt staff – check the SIM card cover plate for any attached devices
- **Screw holes or seams** – this may indicate that the device has been opened
- **Unfamiliar electronic equipment** connected to the PIN Pad or device or network connections – examine any connection of strange or unusual equipment
- **Do not** install, replace, or return devices without verification and authorization from the PCI Coordinator
- Look for **broken or differently coloured casing**, or other external markings
- Report any indications of device tampering or substitution to the PCI Coordinator immediately.

**Verify Identity of Third-Party Persons**
Criminals will often pose as authorized maintenance personnel in order to gain access to PIN Pad devices.

- Verify the identity of any third-party persons claiming to be repair or maintenance personnel, prior to granting them access to devices by having them sign in, verify their identity with photo ID, and contact the PCI Coordinator at finpcico@queensu.ca or extension 32050 (Financial Services Front Desk) to ensure the third-party person is authorized
- Ensure that the third-party person remains accompanied by staff during any work on PIN Pads
- Be aware of suspicious behaviour around devices (for example, attempts by unknown persons to unplug or open devices)
- Report any suspicious behaviour and indications of device tampering or substitution to the PCI Coordinator immediately.

**Evidence of Cable Substitution Inspection**
Criminals will also try to install or tamper with the connections to PIN Pads.

- Examine the cable attached to the device for any small equipment (Key loggers) that can look like part of the normal cabling
- Examine any changes to the cable used to connect the PIN Pad to the base unit or any additional wires not part of original cabling
- Inspect telephone boxes for devices that record transmissions such as voice recorders or MP3 players

**Physical Security Inspection**

- Ensure PIN Pads are securely attached to the counter or keep out of reach from unauthorized users
- Complete a visual inspection on every device to look for potential signs of tampering
- Keep spare devices under lock and key to prevent unauthorized removal
- If you have security cameras in place, ensure cameras have a clear line of sight to the PIN Pads to potentially aid investigators in the event of a security breach
- Require all visiting repair or maintenance personnel to sign in with their name and company information and obtain verification from PCI Coordinator at finpcico@queensu.ca or extension 32050 (Financial Services Front Desk) that they have been authorized
- Change the device’s default admin password
- All requests for PIN Pads must go through the PCI Coordinator
• Report any suspicious behaviour and indications of device tampering or substitution to the PCI Coordinator immediately

PIN Pad Security Best Practices

• Ensure you provide your customers enough room around the PIN Pad device to comfortably shield the PIN Pad when entering their number
• Inspect your PIN Pad and cabling regularly – if anything looks different or unfamiliar, altered, or missing, notify your supervisor immediately
• Make sure if you have security cameras, that they don’t capture the PIN that customers are entering
• Never enter a PIN for a customer
• Allow the customer to hold the PIN Pad until the transaction is complete
• Inspect the area around the PIN Pad looking for holes in the ceiling, walls or shelves, that could conceal a small camera
• PIN Pads not in use should be placed under the counter or out of customers’ reach (do not unplug)
• Develop a process to monitor devices that consistently don’t work properly such as high magstripe read failures as these can be indicators of tampered devices
• Implement a procedure that requires all visiting repair and maintenance personnel to sign in with their name and company information and to track the serial numbers of any devices that they are installing, removing or replacing (provided you first obtain verification from the PCI Coordinator at finpcico@queensu.ca or extension 32050 (Financial Services Front Desk))
PIN Pad Pictures

Verifone

Ingenico
References

Skimming - A Resource Guide:

Skimming Prevention – Best Practices for Merchants:

Skimming Prevention: Overview of Best Practices for Merchants:

Chase Merchant Operating Manual:

Fraud Prevention Program – Reference Guide:
https://www.moneris.com/-/media/Files/Moneris-Fraud-Prevention-Reference.pdf?la=en

Protecting Against Fraud:
## Appendix – PIN Pad Inspection Log

The PIN Pad Inspection Log is located on the Financial Services Website

### PIN Pad Inspection Log

**INSTRUCTIONS:**

- Please print in BLOCK LETTERS (except initials/signature column)
- To be filled out weekly and submitted to pdcoordinator@queensu.ca quarterly as per the PIN Pad Security Training and Procedures
- If you answered "No" in columns labeled A, B, and/or E, contact the PCI Coordinator immediately as per the PIN Pad Security Training and Procedures
- If you answered "Yes" in columns labeled C and/or D, contact the PCI Coordinator immediately as per the PIN Pad Security Training and Procedures

<table>
<thead>
<tr>
<th>Date (YY-MM-DD)</th>
<th>Employee Name</th>
<th>Employee Initials/Signature</th>
<th>Merchant Account #</th>
<th>Building</th>
<th>Room #</th>
<th>Model #</th>
<th>Base/Terminal Serial Number/IMEI (yes/no)</th>
<th>Base/Terminal Serial Number</th>
<th>PIN Pad Serial Number</th>
<th>PIN Pad Serial Number Confirmation</th>
<th>PIN Pad Serial Number Confirmation (yes/no)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

---