Bell Canada

University Of British Columbia

Point of Sale – Security Recommendations Version 1.0

Date Published: 5 May 2013

Ron Borsholm
Senior Security Consultant, QSA, PMP
Bell Canada

Phone: (250) 634-4005
Email: Ron.Borsholm@bell.ca

Bell

Notices

Confidentiality

This document contains information confidential and proprietary to the University of British Columbia. The University of British Columbia requires that this Information be held in strict confidence by the recipient and be protected with the same degree of care as the recipient uses to protect its own confidential and proprietary information, which in any event shall not be less than a reasonable degree of care. The recipient shall not, without the prior written consent of the University of British Columbia, disclose the Information to any person or entity except its own authorized employees or agents, and only after such personnel have been advised of the confidential and proprietary nature of the Information and have agreed to protect same.

Table of Contents

List of Appendices

1 Purpose of Document

This document outlines security recommendations with regard to the use of Point of Sale (POS) devices within the University of British Columbia.

2 Background

The University of British Columbia, as a vendor who accepts payment cards is required to be compliant with the PCI Security Council Data Security Standard (PCI DSS).

The Payment Card Industry (PCI) Data Security Standard (DSS) was developed to encourage and enhance cardholder data security and facilitate the broad adoption of consistent data security measures globally. PCI DSS provides a baseline of technical and operational requirements designed to protect cardholder data. PCI DSS applies to all entities involved in payment card processing – including merchants, processors, acquirers, issuers, and service providers, as well as all other entities that store, process or transmit cardholder data. PCI DSS comprises a minimum set of requirements for protecting cardholder data, and may be enhanced by additional controls and practices to further mitigate risks

3 Ensure your Business is Secure

- Treat your PIN pads as cash. Do not keep them out in the open or on the counter. Ensure they are secured or kept out of site when not used. This includes PIN pads at back-up checkouts that are not used as frequently.
- Regularly inspect all cash register stations. Criminals will target PIN pads that are easily accessible.
- Secure terminal and PIN pad wires by bolting wire cabling to the PIN pad and the terminal. This will deter fraudsters from stealing your PIN pads and POS terminals and make it more difficult to plant a compromised unit at your business. An alternative is to use a secure stand in which the POS is bolted to the stand and wiring is not easily accessible.
- Place an identifying mark or sticker on back of PIN pads or somewhere visible to the clerk so they can verify throughout the day that the PIN pad has not been swapped out with a compromised unit.
- Use a POS Terminal Description Form to help with inspections by educating staff on what the terminal and PIN pad should normally look like. (eg. color and number of wires attached, etc.)
- Use a POS Terminal Inspection Log to ensure inspections are completed regularly. If a skimming attack does occur, the log will aid in determining when the device may have been planted, or when a PIN pad was stolen.

4 POS and the PCI DSS

The PCI Security Council has created the document **"Information Supplement: Skimming Prevention – Best Practices for Merchants"** to assist and educate merchants regarding security best practices associated with POS security and skimming attacks.

Though currently not mandated by the PCI SSC, guidelines and best practices documents are produced to help educate and create awareness of challenges faced by the payment industry. The guidelines are the result of industry and law enforcement understanding of the current and evolving threat landscape associated with skimming. In addition the document has incorporated known best practices, currently conducted by many merchants, to mitigate skimming attacks taking place in their respective point-of-sale environments.

5 Recommended Physical Security Approaches

5.1 POS Security Stand

The POS security stand is secured to the counter and the POS is locked down to keep the device in place. Different types of stands are available – some of which still allow the POS to be handed to a customer by easily unlocking POS and harness from the stand itself (pictured below).

5.2 POS Tethering

The tether provides more flexibility than a stand and allows the device to be handed to a cardholder to enter their PIN and the POS to be stored under the counter, out of sight when not in use. When using a tether, the device can be easily inspected for the recommended integrity checks and serial number validation. In the event the cable is cut during the theft of a device, the fraudster is less likely to return to install the tamper as the cable will not be intact.

5.3 Security Seals

Security seals provide an added layer of security. The seals should be placed over seams (where the front and back cover meet) or over an access entry point. Any cuts through the seal or removal of the seal indicate the device may have been tampered with. Some seals also have a security feature that imprints “VOID” on the device if the seal has been removed.

5.4 Labels

For merchants completing a SAQ D and attestation of compliance it is required that usage policies require labeling of devices with information that can be correlated to owner, contact information and purpose.

Although not required for lower SAQ's it is still recommended that such labeling be implemented for all POS devices to ensure that ownership is easily communicated.

6 Recommended Procedures

6.1 POS Terminal Description Form

A POS terminal description form should be created which will assist with inspections by educating staff on what the terminal and PIN pad should normally look like.
This form may contain photos of the terminal itself and the cables which are attached to it.

6.2 POS Terminal Inspection Log

Physical reviews of the POS devices should be completed regularly. This may range from daily reviews where high POS volumes are realized to monthly reviews where there is less traffic.

If the POS is compromised or substituted, the log will aid in determining when the PIN Pad was affected.

The inspection log should contain at a minimum the following information:

- Review of the POS serial number to verify it is correct
- Review of the security stickers to ensure they are intact
- Review of the connection cable to ensure that it has not been subsidized
- Review of the physical security to ensure that the POS cannot be removed

6.3 Incident Response Plan

It is recommended that the Incident Response Plan also include POS devices and their operators as potential sources of an incident.

An incident may be raised arising from the determination that a POS has been compromised as part of the physical inspections or from information received from the POS operator.

7 Reviews and Document Control

Document Control

Date	Version	Change Reference	Reviewed by
May 5, 2013	1.0	Final Document	Ron Borsholm

Appendix A: Attachments

A.1 Attachment 1: PCI Security Council - Information Supplement Skimming Prevention – Best Practices for Merchants

This document was created to assist and educate merchants regarding security best practices associated with skimming attacks.

A.2 Attachment 2: MasterCard – Understanding Terminal Manipulation at the Point of Sale

The MasterCard Analysis Laboratory was established more than 10 years ago to investigate card security. In recent years, it has also focused on identifying and understanding attacks against terminals. Working with police forces throughout the world and using a wide range of state-of-the-art equipment along with extensive engineering expertise, MasterCard's laboratory has successfully analyzed many compromised terminals.