Merchants have the responsibility to ensure that Point of Sale (POS) devices are secure while in their possession. Periodic inspections help detect tampering and substitution of POS Devices. Merchants can achieve appropriate levels of security at the point of sale by taking all necessary countermeasures against fraudsters.

This document can help merchants to:

- ☑ Be aware of the risks relating to skimming - both physical and logical.
- ☑ Be aware of the vulnerabilities inherent in the use of point-of-sale terminals and terminal infrastructures.
- ☑ Be aware of the vulnerabilities associated with staff that has access to consumer payment devices.
- ☑ Prevent or deter criminal attacks against point-of-sale terminals and terminal infrastructures.
- ☑ Identify any compromised terminals as soon as possible and notify the Bank to respond and minimize the impact of a successful attack.

Skimming is a method of credit card fraud that involves the transfer of data using foreign devices that are discretely placed on or within a Point-of-Sale (POS) device/terminal. These foreign devices are discretely placed with the intent of obtaining customer payment card information during a payment card transaction.

Fraudsters have resorted to **swapping devices** and replacing it with another device and using your device to commit fraud.

PCI-DSS requirement 9* calls for the protection of devices that capture payment card data via direct physical interaction from tampering and substitution. This includes maintaining a device inventory log and the periodic inspections of POS devices/terminals.

Maintain an up-to-date list of devices (PCI-DSS Req. 9.9.1*):

Upon receiving your POS device, review the invoice and order to validate that the correct device was received prior to using it.

Record the device name, model, serial # and the location of where the device will be used on the PCI-DSS Compliance Spreadsheet – Device Inventory Tab.

Periodic inspections of POS devices/terminals (PCI-DSS Req. 9.9.2):
At least weekly, perform an inspection of all POS devices

Use the attached Point-of-Sale (POS) Device Inspection Checklist to document all inspections. Keep the checklist easily accessible in the event of an assessment or an audit.

Be sure to date and initial each item you have checked. Additional pages may be added, as needed.

If you suspect or have found signs of skimming or tampering, immediately discontinue the use of the device and contact:
SBJ_MerchantSupport@Sagicor.com
Any devices or terminals that have been inactive for over 3 months must be returned to Sagicor Bank for inspection or closure.

Click here to download the Inspection Checklist

* Payment Card Industry Data Security Standard (PCI DSS) are security standards that companies who accept, process, store or transmit credit card information must maintain.

A copy of the Inspection Checklist must be sent to Sagicor Bank monthly at SBJ_MerchantSupport@sagicor.com as verification that the devices are being properly inspected.