# The following guidelines must be followed to reduce risk of POS device tampering.

1. Cash Operations will maintain a list of all POS device models and serial numbers. When new devices are ordered, they will first be received by Cash Operations to be inspected and logged prior to delivering to the merchant.
2. Merchants must change default password on device after initial sign-on.
3. Merchants are responsible for keeping devices in a secure location. When possible, devices should be anchored with secure stands, tethers, or alarms. Access to devices should be kept at a minimum.
4. Merchants must train applicable staff on how to spot POS equipment tampering. This includes, but is not limited to, abnormalities such as a missing seal or screw, extra wiring or holes, and added labels or decals. See the additional resources below.
5. Merchants are responsible for routinely checking devices for signs of tampering. The physical examination of the devices should be incorporated into the merchant’s daily duties.
6. Any sign of tampering must be reported to Cash Operations immediately. Do not access or alter compromised devices and keep handling to a minimum. Do not turn off, restart, or reboot the system but do unplug the device from any network cables, if applicable. Cash Operations will work with the device acquirer and local law enforcement as necessary. See additional resource below.
7. Beginning 2017, Cash Operations will annually send all merchants the PCI Security Standards Council Terminal Evaluation Form. This Form should be completed along with the annual Payment Card Merchant Agreement. Cash Operations will compare this Form to device information maintained and investigate any discrepancies. Additionally, Cash Operations may periodically make unannounced visits to merchants to inspect devices.

## Additional Resources:

PCI DSS Quick Reference Guide

<https://www.pcisecuritystandards.org/documents/PCIDSS_QRGv3_2.pdf?agreement=true&time=1492707763458>

PCI Security Standards Council – Skimming Prevention: Best Practices for Merchants. See Appendix B for Terminal Evaluation Form. <https://www.pcisecuritystandards.org/documents/Skimming%20Prevention%20BP%20for%20Merchants%20Sept2014.pdf>

VISA Protect Your Merchant Terminals From Illegal Tampering:

<https://usa.visa.com/dam/VCOM/download/merchants/data-security-protect-terminals-from-illegal-tampering-020513.pdf>

VISA What To Do If Compromised

<https://usa.visa.com/content/dam/VCOM/download/merchants/cisp-what-to-do-if-compromised.pdf>