# Best Practices for Card Reader Security

To comply with the latest PCI DSS physical security standards, the device manufacturers recommend following the guidelines listed in this document to prevent fraudulent activity on your devices.

**When you receive and install a new Cantaloupe card reader or all-in-one payment device, make sure to perform the following checks:**

- Check the tamper-evident physical seals on the device to make sure they are intact.
- Power on the device. Check the display message (if applicable) to make sure there is no indication of tampering.
- Confirm the device's firmware version is correct.
- Check the touchscreen (if applicable) to make sure there is no physical overlay on the touchscreen.
- Check for any holes in the device.
- Look for suspicious objects around the card slot.
- Check the MSR (magnetic stripe) slot (if applicable) to make sure there is no alteration of the device.
- Reference your device's user manual if you see odd/different cabling, or new devices or features you don't recognize.

**You should also regularly check your Cantaloupe card reader or all-in-one payment device to verify their security:**

- Check the tamper-evident physical seals to make sure they are intact.
- Check the touchscreen, device housing, card slot, and MSR slot — as applicable — to verify there are no holes or other suspicious objects.
- Locate the serial number printed on the device and verify that it matches the serial number on file.

If you suspect your device has been tampered with, please contact Cantaloupe at customerservice@cantaloupe.com or +1 888.561.4748.

For more information on PCI Guide to Safe Payments, please visit pcisecuritystandards.org.