### Merchant Guideline for Protecting Cardholder Data

The following guidelines are provided to help merchants protect cardholder (customer) card data payment by proactively managing the payment terminals that are in the merchant’s care, custody, and control.

#### Primary precaution

To help prevent tampering, do not allow third parties to access or use your payment terminals under any circumstances. If there are any indicators that a terminal has been tampered with, manipulated, or exchanged:

1. Do not use the terminal.
2. Contact Customer Support immediately for assistance.

Adhering to these guidelines enables us to assist you in addressing issues with compromised terminals.

#### When receiving your terminal and before using your terminal for the first time:

* Only accept the package if it is not damaged and does not show signs of prior opening (tampering).
* After you have opened the terminal shipping box, check the terminal’s serial number (S/N) and write it down in your records.
* Retain shipping documents for possible warranty and inspection issues.

#### Before using the terminal

* Check to see if your payment terminal shows signs of tampering, damage, or manipulation (such as loose or missing screws, an unusual appearance, extra cables).
* If any signs of tampering, damage, or manipulation are present, do not use the terminal and contact Customer Support immediately.

#### When the terminal is not in use

* Never leave your terminal unattended. Store it in a secure location, such as a locked cabinet, when it is not in use such as during breaks or outside of business hours.
* Always store terminals out of reach for third parties.

#### If the terminal has been lost or stolen

* Contact Customer Support immediately. We will disable the terminal, so that it cannot be used by third parties.

#### Managing your terminals

* Do not modify the terminal, give it away to unauthorized individuals, or operate it in an unauthorized manner.
* Maintain an inventory list for all your terminals that includes, as the minimum, the serial number, brand, and model name / number for each terminal. Include other unique identifying information such as logos, color of the case, if applicable.
* Regularly check the terminals in your inventory for possible signs of manipulation or tampering and to detect lost or stolen equipment.

**1**