

BP Payment Guide

Securing Cardholder
Information



12.0 Securing Cardholder Information

As a BP merchant, your location is responsible for keeping sensitive cardholder data secured. Keep cardholder account numbers and personal information confidential. The rising incidence of stolen cardholder account data is a major concern for all merchants. To protect your business and your customers (cardholders), the credit card companies have developed a set of requirements governing the safekeeping of account information. Effective September 30, 2007, the Payment Card Industry (PCI) Data Security Standard (DSS) was launched as a global forum for implementation and management of data security standards.

Summary of Requirements Governing the Security of Cardholder Information

Storage of Cardholder Information

- Store only that portion of the customer's account information that is essential to your business: i.e., name, account number or expiration date.
- Store all materials containing cardholder information in a locked and secure area limited to authorized personnel. Materials include, but are not limited to:
 - Receipts
 - Manual Tickets
 - Journal Tapes
 - Batch Reports (including EPS Terminal Detail and Acquirer Detail Reports)
 - Back-up disks and/or electronic media
- Release cardholder data only to BP, their representative (i.e. Accenture), merchant banks, card processors or as specifically required by law. Never send cardholder data in an e-mail.
- The materials containing cardholder information described above should be retained for a minimum of 6 months and a maximum of 9 months or the length required for your business or legal purposes. Appropriately destroy (i.e., shred) these materials after the retention time has elapsed.

Destruction of Cardholder Information

- Destroy (i.e., shred) all materials that contain cardholder information after the retention times described in this Guide. Never simply discard these materials in the garbage. Materials include, but are not limited to:
 - Receipts
 - Manual Tickets
 - Journal Tapes
 - Batch Reports (including EPS Terminal Detail and Acquirer Detail Reports)
 - Back-up disks and/or electronic media

Restrict Physical Access to Cardholder Information

- Ensure that physical access to areas where the cardholder information is located is limited to authorized personnel.
- Ensure that access to Point of Service terminals is limited to authorized personnel.
- Do not allow employees to bring laptop computers or other electronic equipment to your site. Laptops and other electronic equipment can be used for "skimming" or "cloning" or "sniffing" of cardholder account information to be used fraudulently elsewhere.
- Do not disconnect or connect any equipment to either the network switch or the satellite inside unit (PES) or modem unless specifically instructed to by a BP Help Desk Analyst or a BP network engineer. Changes to the connection of card processing equipment or the card processing network are not permitted.
- Ensure that any third party hardware/applications at your location are PCI compliant. Also, ensure the hardware/applications are installed in a compliant manner.

12.0 Securing Cardholder Information

Reporting a Security Incident

- Immediately contact BP Elite Customer Solutions if a security breach is suspected or confirmed. A security breach would include, but is not limited to:
 - Loss or theft of materials that contain cardholder information.
 - Loss or theft of Point of Sale devices or EPS devices.