# PCI Data Storage Do's and Don'ts

Requirement 3 of the Payment Card Industry's Data Security Standard (PCI DSS) is to "protect stored cardholder data." The public assumes merchants and financial institutions will protect data on payment cards to thwart theft and prevent unauthorized use. But merchants should take note: *Requirement 3 applies only if cardholder data is stored*. Merchants who do not store any cardholder data *automatically* provide stronger protection by having eliminated a key target for data thieves.

For merchants who have a legitimate business reason to store cardholder data, it is important to understand what data elements PCI DSS allows them to store and what measures they must take to protect those data. To prevent unauthorized storage, only Council certified PIN entry devices and payment applications may be used. PCI DSS compliance is enforced by the major payment card brands who established the PCI DSS and the PCI Security Standards Council: American Express, Discover Financial Services, JCB International, MasterCard Worldwide and Visa Inc.

### PCI SSC FOUNDERS

American Express
Discover Network
JCB
MasterCard Worldwide
VISA

### PARTICIPATING ORGANIZATIONS

Merchants, Banks, Processors, Hardware and Software Developers and Point-of-Sale Vendors

## Basic PCI Data Storage Guidelines for Merchants

Cardholder data refers to any information contained on a customer's payment card. The data is printed on either side of the card and is contained in digital format on the magnetic stripe embedded in the backside of the card. Some payment cards store data in chips embedded on the front side. The front side usually has the primary account number (PAN), cardholder name and expiration date. The magnetic stripe or chip holds these plus other sensitive data for authentication and authorization.

In general, no payment card data should ever be stored by a merchant unless it's necessary to meet the needs of the business. Sensitive data on the magnetic stripe or chip must never be stored. Only the PAN, expiration date, service code, or cardholder name may be stored, and merchants must use technical precautions for safe storage (see back of this fact sheet for a summary). The matrix below shows basic "do's" and "don'ts" for data storage security.

| Data Do's | Data Don'ts |
|---|---|
| Do understand where payment card data flows for the entire transaction process | Do not store cardholder data unless it's absolutely necessary |
| Do verify that your payment card terminals comply with the PCI personal identification number (PIN) entry device (PED) security requirements | Do not store sensitive authentication data contained in the payment card's storage chip or full magnetic stripe, including the printed 3-4 digit card validation code on the front or back of the payment card after authorization |
| Do verify that your payment applications comply with the Payment Application Data Security Standard (PA-DSS) | Do not have PED terminals print out personally identifiable payment card data; printouts should be truncated or masked |
| Do retain (if you have a legitimate business need) cardholder data only if authorized, and ensure it's protected | Do not store any payment card data in payment card terminals or other unprotected endpoint devices, such as PCs, laptops or smart phones |
| Do use strong cryptography to render unreadable cardholder data that you store, and use other layered security technologies to minimize the risk of exploits by criminals | Do not locate servers or other payment card system storage devices outside of a locked, fully-secured and access-controlled room |
| Do ensure that third parties who process your customers' payment cards comply with PCI DSS, PED and/or PA-DSS as applicable. Have clear access and password protection policies | Do not permit any unauthorized people to access stored cardholder data |

## PROTECT STORED CARDHOLDER DATA

**Use Encryption**

Encrypted data is unreadable and unusable to a system intruder without the property cryptographic keys. See the PCI DSS Glossary for more information: www.pcisecuritystandards.org/pdfs/pci_dss_glossary.pdf

**Use Other Measures**

Do not store cardholder data unless there is a legitimate business need; truncate or mask cardholder data if full PAN is not needed and do not send PAN in unencrypted emails, instant messages, chats, etc..

**Use Compensating Controls as Alternatives**

If stored cardholder data cannot be encrypted, consult PCI DSS Appendix B: Compensating Controls and Appendix C: Compensating Controls Worksheet.

**Verify 3rd Party Compliance**

Approved PIN Entry Devices www.pcisecuritystandards.org/pin/pedapprovallist.html

Validated Payment Applications https://www.pcisecuritystandards.org/security_standards/pa_dss.shtml

## Technical Guidelines for Stored Payment Card Data

PCI DSS Requirement 3 details technical guidelines for protecting stored cardholder data. Merchants should develop a data retention and storage policy that strictly limits storage amount and retention time to that which is required for business, legal, and/or regulatory purposes.

Sensitive authentication data must never be stored after authorization – even if this data is encrypted.

- Never store full contents of any track from the card's magnetic stripe or chip (referred to as full track, track, track 1, track 2, or magnetic stripe data). If required for business purposes, the cardholder's name, PAN, expiration date, and service code may be stored as long as they are protected in accordance with PCI DSS requirements.
- Never store the card-validation code or value (three- or four-digit number printed on the front or back of a payment card used to validate card-not-present transactions).
- Never store the personal identification number (PIN) or PIN Block. Be sure to mask PAN whenever it is displayed. The first six and last four digits are the maximum number of digits that may be displayed. This requirement does not apply to those authorized with a specific need to see the full PAN, nor does it supersede stricter requirements in place for displays of cardholder data such as on a point-of-sale receipt.

## Technical Guidelines for PCI Data Storage

| | Data Element | Storage Permitted | Protection Required | PCI DSS Req. 3.4 |
|---|---|---|---|---|
| Cardholder Data | Primary Account Number (PAN) | Yes | Yes | Yes |
| | Cardholder Name[1] | Yes | Yes[1] | No |
| | Service Code[1] | Yes | Yes[1] | No |
| | Expiration Date[1] | Yes | Yes[1] | No |
| Sensitive Authentication Data[2] | Full Magnetic Stripe Data[3] | No | N/A | N/A |
| | CAV2/CVC2/CVV2/CID | No | N/A | N/A |
| | PIN/PIN Block | No | N/A | N/A |

[1] These data elements must be protected if stored in conjunction with the PAN. This protection should be per PCI DSS requirements for general protection of the cardholder data environment. Additionally, other legislation (e.g., related to consumer personal data protection, privacy, identity theft, or data security) may require specific protection of this data, or proper disclosure of a company's practices if consumer-related personal data is being collected during the course of business. PCI DSS, however, does not apply if PANs are not stored, processed, or transmitted.

[2] Sensitive authentication data must not be stored after authorization (even if encrypted).

[3] Full track data from the magnetic stripe, magnetic stripe image on the chip, or elsewhere.

## Technical Guidelines for Protecting Stored Payment Card Data

At a minimum, PCI DSS requires PAN to be rendered unreadable anywhere it is stored – including portable digital media, backup media, and in logs. Software solutions for this requirement may include one of the following:

- **One-way hash functions based on strong cryptography** – also called hashed index, which displays only index data that point to records in the database where sensitive data actually reside.
- **Truncation** – removing a data segment, such as showing only the last four digits.
- **Index tokens and securely stored pads** – encryption algorithm that combines sensitive plain text data with a random key or "pad" that works only once.
- **Strong cryptography** – with associated key management processes and procedures. Refer to the PCI DSS and PA-DSS Glossary of Terms, Abbreviations and Acronyms for the definition of "strong cryptography."

Some cryptography solutions encrypt specific fields of information stored in a database; others encrypt a singular file or even the entire disk where data is stored. If full-disk encryption is used, logical access must be managed independently of native operating system access control mechanisms. Decryption keys must not be tied to user accounts. Encryption keys used for encryption of cardholder data must be protected against both disclosure and misuse. All key management processes and procedures for keys used for encryption of cardholder data must be fully documented and implemented. For more details, see PCI DSS Requirement 3.