PCI DSS Data Storage Do's and Don'ts

Requirement 3 of the Payment Card Industry Data Security Standard (PCI DSS) is to "protect stored cardholder data." The public expects that merchants and financial institutions will protect payment card data to thwart data theft and prevent unauthorized use. Requirement 3 addresses protection of stored cardholder data. Merchants who do not store any cardholder data *automatically* provide stronger protection by having eliminated a key target for data thieves. Remember if you don't need it, don't store it!

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. In addition to PCI DSS requirements, PA-DSS and PTS require protection of stored cardholder data for payment applications and payment terminals. To prevent unauthorized storage, only PTS approved PIN entry devices and PA-DSS validated payment applications should be used. PCI DSS, PA-DSS and PTS 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

PARTICIPATING ORGANIZATIONS

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

Basic Payment Card 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 authentication 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) Transaction Security (PTS) requirements	Do not store sensitive authentication data contained in a payment card's chip or magnetic stripe, including the 3-4 digit card verification code or value printed 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 payment 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, PTS 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 proper cryptographic keys. See the PCI DSS Glossary for more information: www.pcisecuritystandards.org/security_standards/glossary.php

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 or otherwise rendered unreadable, consult PCI DSS Appendix B: Compensating Controls and Appendix C: Compensating Controls Worksheet.

Verify 3rd Party Compliance

Approved PTS Devices www.pcisecuritystandards.org/approved_companies_providers/approved_pin_transaction_security.php

Validated Payment Applications www.pcisecuritystandards.org/approved_companies_providers/validated_payment_applications.php

Technical Guidelines for Stored Payment Card Data

PCI DSS Requirement 3 details technical and operational requirements 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 Payment Card Data Storage

		Data Element	Storage Permitted	Render Stored Account Data Unreadable per Requirement 3.4
Account Data	Cardholder Data	Primary Account Number (PAN)	Yes	Yes
		Cardholder Name	Yes	No
		Service Code	Yes	No
		Expiration Date	Yes	No
	Sensitive Authentication Data[1]	Full Magnetic Stripe Data[2]	No	Cannot store per Requirement 3.2
		CAV2/CVC2/CVV2/CID	No	Cannot store per Requirement 3.2
		PIN/PIN Block	No	Cannot store per Requirement 3.2

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

[2] Full track data from the magnetic stripe, equivalent data on the chip, or elsewhere.

Technical Guidelines for Protecting Stored Payment Card Data

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

- **One-way hash functions based on strong cryptography** – converts the entire PAN into a unique, fixed-length cryptographic value.
- **Truncation** – permanently removes a segment of the data (for example, retaining 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, and 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.