PCI and TransArmor

Dave Bisco

December 2010

Payment Card Industry (PCI) Security Standards Council (SSC)

- The Payment Card Industry Security Standards Council is compromised of Visa, MasterCard, Discover, JCB and American Express.
- Each card brand originally had their own security program.
- A single set of security controls was created which the individual card brands adopted.
- The PCI requirements are now on a 3-year life cycle. The latest version was just released in Nov of 2010.

First Data™

What is PCI Data?

		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

- All of the fields in the table above are examples of PCI data and handling of the data must meet the PCI requirements.
- PCI DSS applies to any organization that processes, stores or transmits the PAN.

First Data.

PCI Data Security Standards

PCI Data Security Standard – High Level Overview

Build and Maintain a Secure Network	1. Install and maintain a firewall configuration to protect cardholder data 2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	3. Protect stored cardholder data 4. Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	5. Use and regularly update anti-virus software or programs 6. Develop and maintain secure systems and applications
Implement Strong Access Control Measures	7. Restrict access to cardholder data by business need to know 8. Assign a unique ID to each person with computer access 9. Restrict physical access to cardholder data
Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data 11. Regularly test security systems and processes.
Maintain an Information Security Policy	12. Maintain a policy that addresses information security for all personnel.

- There are 250+ individual PCI requirements – they are organized into 12 major categories which are further organized into 6 strategies.

First Data.

Why Comply with the PCI DSS?

A security breach and subsequent compromise of payment card data has far-reaching consequences for affected organizations, including:

- Regulatory notification requirements
- Loss or reputation
- Loss of customers
- Potential financial liabilities (e.g., regulatory & other fees/fines)
- Litigation

First Data

What is the Risk to Merchants?

Risk	Outcome
Losses from fraud	Banks and payment processors may reclaim losses they sustain as a result of a merchant's data breach.
Expenses for credit monitoring	Customers whose data is stolen may be entitled to credit monitoring for at least a year.
Fines by card brands	Card companies may issue fines for PCI DSS noncompliance and prohibited data storage practices.
Remediation costs	Capital expenditures may be necessary to replace or upgrade compromised hardware, software, applications and communications.
Brand damage	Public reporting of a breach often is required by law, making it impossible to escape widespread bad publicity and loss of confidence in merchant's brand.
Expense of forensic exam and in-depth PCI audit	A forensic investigation could take months with very high costs.
Potential lawsuits	From customers, financial institutions, ISOs, payment processors, card brands, state attorneys general, and more.
Drop in market cap	When damages are high, a merchant's stock value and overall market capitalization can drop.

First Data™

Who Owns the Liability?

- Any entity that touches sensitive cardholder data for payment processing assumes liability.
- These are the payment processors, service providers, gateways, third party agents, presenters and merchants!
- PCI DSS compliance mandates are costly, time consuming, and do not limit the merchant's liability.

First Data

Cost Effective Ways to Fight Back

- Build layers of security around cardholder data when it must be present
- Render the data useless to thieves when possible
- Do not store cardholder data in your environment

First Data™

First Data™

The Solution

•The First Data solution with help to dramatically improve data security and reduce organizational risk.

•Merchant no longer have to transmit unencrypted cardholder data or store the data within their POS or their systems environments.

•Sensitive data is stored in a secure and PCI compliant repository, called a vault, managed by First Data.

First Data™

Advantages

•Token Format –Simple integration of the tokenized number preserves the format of the original PAN. Keeping the token value the same number of characters as the original number and preserving the last 4 digits makes continued reporting and marketing efforts easy with no disruption to current processes.

•Hardware agnostic –makes the integration into current processes easy and cost effective.

•Token supports all current operational processes such as settlement, reconciliation, chargeback's and analytics.

First Data™

Advantages

•Warranty protection on the token value -First Data warrants that if the token is lost or stolen, it cannot be used to initiate a fraudulent transaction from outside the merchant payment processing environment.

•Public/Private Key encryption –using a public/private key encryption adds another layer of security that many encryption solutions are not providing today with a public key to encrypt the data at the POS and a private key that is separate to decrypt the data at First Data.

•RSA Partnership –The combination of using First Data's technology and experience in processing with RSA's experience as a leader in security technology is a winning combination.

First Data™

Competitive Information

"End- to- End" Encryption

•What it is:

–Encrypting card data at point of capture for secure transmission to processor.

•Who offers it:

–Heartland, RBS, Chase Paymentech

•Why it is insufficient:

–Secures card data in motion, but adds no security when card number is returned to the merchant after authorization.

–Card data stored using encryption is card data that is still present.

First Data™

Competitive Advantage

"In-house" Tokenization and Encryption

•What it is:

–Using the same back-end technologies to encrypt or tokenize data internally within a merchant's own systems environment.

•Who offers it:

–RSA*, Voltage, nuBridges, and a variety of Value Added Reseller offerings and CNP Gateways

•Why it is insufficient:

–"In house" protections increase card data security, but real card data still exists in the merchant's environment.

•Note: RSA no longer selling direct –contractually will now sell the integrated First Data® TransArmor℠ solution.

First Data™