PART 1

The Fundamentals

CHAPTER 1

PCI Fundamentals

The Payment Card Industry Data Security Standards (PCI DSS) is commonly referred to as *PCI compliance*. Although this is one of the hottest topics of discussion among business and technology professionals alike, the spirit of PCI compliance is nothing new. In fact it has been around for several years. However, with the rise of information security–related legislation, privacy concerns, confirmed data breaches, and the overall prevalence of e-commerce in today's society, PCI compliance is of the utmost concern for a wide assortment of people, organizations, and businesses.

Although the rise of e-commerce has had a profound economic impact on our daily lives at both the personal and professional levels, it brings a host of new challenges, including the challenge of properly protecting sensitive cardholder data. In all business activities, a certain amount of risk is assumed in order to gain the benefits associated with that business activity. In the world of payment cards and electronic commerce, the risk-and-reward model involves properly protecting cardholder data during payment card transactions. The importance of protecting cardholder data can't be overstated.

Many of the key players in the payment card industry got together to develop a series of best practices that could be implemented by those utilizing payment cards. In today's world of new legislation, regulation,

and compliance, the payment card industry sought to develop a program where the industry could be self-regulated and proactively manage the risks associated with payment card programs. The goal of this initiative was to reduce governmental legislation and build confidence and trust among the participants (including consumers) that rely on payment cards to conduct commerce.

PCI compliance is important for a number of reasons, and no single reason outweighs any other. Their combined weight is what drives us toward compliance. Each reason falls under one of two headings: consumer confidence or effective business operations. From a consumer perspective, it is all about confidence. Consumers place enormous trust in those who use their sensitive cardholder data as part of their daily commerce. Although a majority of us take advantage of the convenience and efficiency associated with today's electronic commerce, we do so with the expectation that our transactions will be performed in a secure manner. In a world of significant choice, consumers can easily select other vendors to provide their services if they are not comfortable in the security of their personal information. From a business perspective, organizations want to transact commerce in a secure manner so that they can maintain their customer's confidence, have reduced operational costs, and protect organizational assets from fraud and abuse. On a larger scale, our economy depends on efficient trade markets. When commerce can be conducted electronically, there are tremendous gains in efficiency and globalization. When these daily operations are threatened by potential fraud and abuse, businesses are at risk of not being able to effectively operate in today's e-commerce–based markets. The importance of these factors led to the establishment of the PCI and the corresponding data security standards.

There are numerous specific measures organizations can take to create a secure operating environment for the processing of payment cards. The PCI Security Standards Council has established 12 detailed control objectives, which are grouped into 6 broader categories:

1. Build and maintain a secure network.
2. Protect cardholder data.

3. Maintain a vulnerability management program.
4. Implement strong access control measures.
5. Regularly monitor and test networks.
6. Maintain an information security policy.

These six categories are the critical foundation for creating, protecting, maintaining, and operating in a secure manner.

HISTORY OF PCI

The PCI DSS is a standard that has evolved over many years by the efforts of the major payment card brands. Prior to PCI DSS, the major payment card brands individually developed various standards to improve the security of sensitive information used by the payment card industry. Visa USA had originally launched the Cardholder Information Security Program (CISP) in June 2001. From then until March 2004, these audit procedures underwent several revisions and continued to grow and evolve to address the many facets of protecting sensitive cardholder data.

There was also early collaboration between MasterCard and Visa in an attempt to validate and protect cardholder data. During these early attempts at collaboration, some gaps and inconsistency occurred between the separate programs. Although well intentioned, the relationship had a number of problems. The list of approved vendors was not well maintained and there was no clear way for security vendors to get added to the list. Another significant problem was that the other major payment card brands, such as Discover, American Express, and JCB (Japan Credit Bureau), were running their own programs and there was little collaboration across the entire industry.

This lack of collaboration caused tremendous hardships for merchants and service providers, as many of them spent a significant amount of resources to comply with the individual security programs offered by all of the major payment card brands. In order to overcome the challenges and offer a comprehensive information security program for the payment card industry, all of the major brands worked together

and developed PCI DSS 1.0. To further solidify the ownership of the standards, the PCI Security Standards Council was founded. The council maintains the ownership of the PCI DSS, the approved vendor lists, training programs, and other relevant program details.

Although the primary focus of this text is compliance with PCI DSS, it should also be noted that each payment card brand also maintains its own security program in addition to the PCI DSS. These programs go beyond the data protection charter of PCI and include activities such as fraud prevention. The details of such programs can be found in the Resources section of this text. It is highly recommended that organizations adopt the specific card brand recommendations (as applicable to your organization) in addition to PCI DSS to further strengthen their overall security posture.

At the time of this writing, the PCI organization is in its early stages and evolving, and it will continue to grow and improve over time. Inevitably, this maturation process will strengthen the council's ability to deliver security-minded services to merchants and service providers. Due to this fact, it is recommended that organizations continuously monitor and consult the PCI Council's resources and Web site (pcisecuritystandards.org) on a regular basis to ensure that appropriate levels of compliance are achieved and maintained by your organization.

WHY PCI DSS?

The short answer is because it is required. Fortunately, there are many additional benefits to achieving PCI DSS compliance. Fundamentally, many of the methodologies and specific requirements associated with PCI DSS are actually industry standards or best practices. Any organization that can implement and manage the components of PCI DSS will significantly improve its overall security posture and fortify its protection of sensitive cardholder data. Also, PCI DSS compliance offers many organizational benefits and specific risk mitigation solutions.

The cardholder data environment has an aggregated risk based on the subrisk categories of *reputation, financial, compliance*, and *operational*. Exhibit 1.1 represents how each category of risk is tied together to create an overall level of risk for the cardholder data environment.

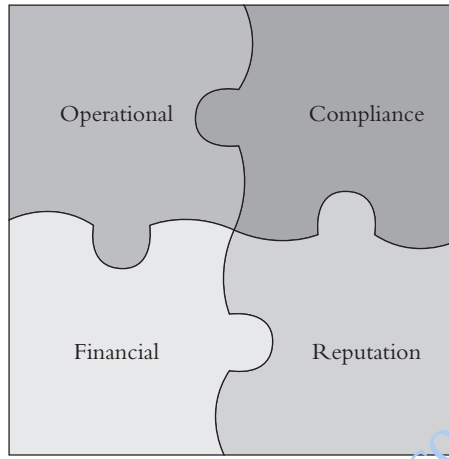

EXHIBIT 1.1 Aggregated Risk for Cardholder Data Environment

Risk	Example
Reputation	What is the impact of a PCI DSS compliance violation on your institution's brand?
Financial	• The fines from specific credit card issuers (i.e., Visa, MasterCard, and American Express) • Litigation costs associated with security breach • Merchant banks will receive fines as a result of a security breach.
Compliance	• Risk of noncompliance with PCI DSS • The fines from specific credit card issuers (i.e., Visa, MasterCard, and American Express)
Operational	• Credit card company–imposed operating restrictions • Loss of card processing privileges

EXHIBIT 1.2 Examples of Cardholder Data Environment Risk

Exhibit 1.2 provides examples of the risks that organizations face within their cardholder data environment.

Furthermore, the direct costs associated with a data breach are significantly increasing on an annual basis. In fact, research from the

Ponemon Institute has shown that the cost of a data breach continues to rise and has done so by 43 percent since 2005. Highlights from the institute's *2007 Annual Study: U.S. Cost of a Data Breach* follow:

- **Total costs increase.** The total average costs of a data breach grew to $197 per record compromised, an increase of 8 percent since 2006 and 43 percent compared with 2005. The average total cost per reporting company was more than $6.3 million per breach and ranged from $225,000 to almost $35 million.
- **Cost of lost business accelerates.** The cost of lost business continued to increase at more than 30 percent, averaging $4.1 million, or $128 per record compromised. Lost business now accounts for 65 percent of data breach costs compared with 54 percent in the 2006 study.
- **Third-party data breaches increase, and cost more.** Breaches by third-party organizations such as outsourcers, contractors, consultants, and business partners were reported by 40 percent of respondents, up from 29 percent in 2006 and 21 percent in 2005. Breaches by third parties were also more costly than breaches by the enterprise itself, averaging $231 compared with $171 per record.
- **Increased customer churn rates help drive lost business costs higher.** In 2007, the average resulting abnormal customer churn rate was 2.67 percent, an increase from 2.01 percent in 2006. Greater customer turnover leads to lower revenues and a higher cost of new customer acquisition resulting from increased marketing to recover lost customer business.
- **Legal defense, public relations costs increase.** Indicating continued growing dissatisfaction and action over a data breach, the costs that organizations expended for legal defense and public relations grew to 8 percent and 3 percent of total breach costs, respectively.
- **Financial services firms impacted most.** The cost of a data breach for financial services organizations was $239 per compromised record, or more than 21 percent higher than the average, demonstrating that organizations with high expectations of trust and privacy have more to lose from a data breach.

The Ponemon Institute research clearly demonstrates the costs associated with a data security breach. Since most organizations are not likely to want to absorb these additional costs, we can clearly see the financial benefits of protecting the cardholder data environment and embracing PCI DSS to reduce the likelihood of a data breach. Now that we have an understanding of what exactly drives PCI DSS, we can begin to discuss what it is and what it means to your organization.

A fundamental component of PCI DSS compliance is to understand the terms, definitions, and requirements put fourth by the PCI Security Standards Council. Throughout this text, I will be referring to the terms and definitions that are listed in the Payment Card Industry Data Security Standards Glossary, Abbreviations, and Acronyms document. In Exhibits 1.3, 1.4, and 1.5, I have included selected terms in order to clarify key components of the PCI Data Security Standard. It is strongly recommended that you frequently review the glossary, abbreviations, and acronyms documentation on a regular basis for any updates or modifications. In addition, this document is an invaluable resource for a more detailed understanding of relevant PCI DSS terms and definitions. The link to the complete list is located in the Resources section of this text.

Now that we have an understanding of key payment card industry terms and definitions, we can review a typical payment card transaction. Exhibit 1.6 illustrates a typical payment card transaction:

The following three steps explain a typical payment card transaction and highlight the associated parties required to complete the transaction:

Step 1. A cardholder is made an authorized user of a payment card by the card issuer (a financial institution that issues the card based on predetermined repayment terms).

Step 2. The authorized card user then initiates a transaction with a merchant (an authorized acceptor of the payment card who receives payment for goods and services).

Step 3. The merchant processes the transaction with an acquirer, referred to as a *merchant bank*. This is a financial institution under contract with the card brand to accept and process the payment.

Term	Definition
Account Number	Payment card number (credit or debit) that identifies the issuer and the particular cardholder account. Also called Primary Account Number (PAN).
Cardholder	Customer to whom a card is issued or an individual who is authorized to use the card.
Cardholder Data	Full magnetic stripe or the PAN plus any of the following: ✓ Cardholder Name ✓ Expiration Date ✓ Service Code
Card Validation Value or Code	Data element on a card's magnetic stripe that uses secure cryptographic process to protect its data integrity and to reveal any alteration or counterfeiting. Also referred to as CAV, CVC, CVV, or CSC, depending on the payment card brand. *Note: The second type of card validation value or code is the three-digit value printed to the right of the credit card number in the signature panel area on the back of the card. For American Express cards, the code is a four-digit unembossed number printed above the card number on the face of all payment cards. The code is uniquely associated with each individual piece of plastic and ties the card account number to the plastic.*

EXHIBIT 1.3 Card-Specific Information

Term	Definition
Hosting Provider	Offers various services to merchants and other service providers. Services range from simple to complex: from shared space on a server to a whole range of "shopping cart" options; from payment applications to connections to payment gateways and processors; and hosting dedicated to just one customer per server.
Magnetic Stripe Data (Track Data)	Data encoded in the magnetic stripe used for authorization during transactions when the card is presented. Entities must not retain full magnetic stripe data subsequent to transaction authorization. Specifically, subsequent to authorization, service codes, discretionary data/Card Validation Value/Code (CVV), and proprietary reserved values must be purged; however, account number, expiration date, name, and service code may be extracted and retained if needed for business.
Payment Cardholder Environment	That part of the network that possesses cardholder data or sensitive authentication data.
PIN	Personal Identification Number
POS	Point of Sale
PVV	PIN Verification Value. This is encoded in the magnetic stripe of a payment card.
Sensitive Authentication Data	Security-related information (Card Validation Codes/Values, complete track data, PINs, and PIN Blocks) used to authenticate cardholders, appearing in plaintext or otherwise unprotected form. Disclosure, modification, or destruction of this information could compromise the security of a cryptographic device, information system, or cardholder information or could be used in a fraudulent transaction.

EXHIBIT 1.4 Transaction-Specific Information

Term	Definition
Acquirer	The bankcard association member that initiates and maintains relationships with merchants that accept payment cards. (Also referred to as merchant bank.)
Cardholder Data Environment	The area of a computer system network that possesses cardholder data or sensitive authentication data, and those systems and segments that directly attach or support cardholder processing, storage, or transmission. Adequate network segmentation, which isolates systems that store, process, or transmit cardholder data from those that do not, may reduce the scope of the cardholder data environment and thus the scope of the PCI assessment.
Issuer	The financial institution that issues a payment card.
Merchant	Any company that accepts payment cards in exchange for goods or services.
Service Provider	A business entity that is not a payment card brand member or a merchant directly involved in the processing, storage, transmission, and switching of transaction data and cardholder information or both. This also includes companies that provide services to merchants, service providers, or members that control or could impact the security of cardholder data. Examples include managed service providers that provide managed firewalls, IDS, and other services, as well as hosting providers and other entities. Entities such as telecommunications companies that only provide communication links without access to the application layer of the communication link are excluded.

EXHIBIT 1.5 Organization-Specific Information

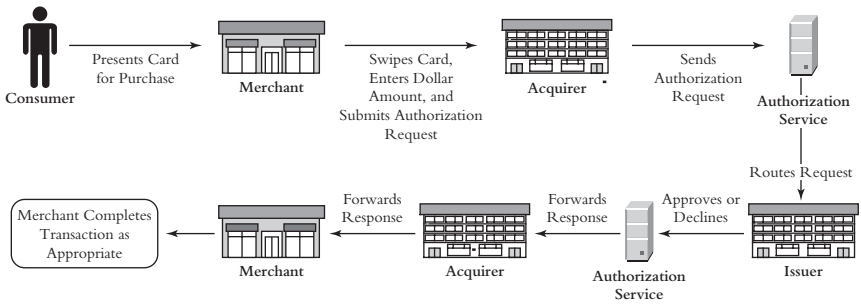

EXHIBIT 1.6 Typical Payment Card Transaction

Each payment card brand has defined a set of merchant levels based on transaction volume over a 12-month period. Exhibit 1.7 summarizes the merchant level definitions based on annual transaction volume for Visa, MasterCard, and American Express. However, if a merchant has been the victim of a hack that resulted in an account data compromise, the merchant may be escalated to a higher level. Note, the JCB and Discover card brands do not classify merchants based on annual transaction volume. Refer to the Resources section for the Web site addresses for these payment card brands.

Level	Visa	MasterCard	American Express
Level 1	≥6,000,000	≥6,000,000 Also, merchants that experienced an account compromise	≥2,500,000 Also, merchants that experienced an account compromise
Level 2	1,000,000–5,999,999	1,000,000–5,999,999	50,000–2,499,999
Level 3	20,000–999,999	20,000–999,999	<50,000
Level 4	<20,000	<20,000	N/A

EXHIBIT 1.7 Merchant Level Definitions Based on Annual Transactions

Based on their level, merchants are required to submit validation of compliance with PCI Data Security Standards. For MasterCard, Visa, and American Express, merchants must submit the following:

Level 1

- Annual on-site PCI Data Security Assessment performed by a Qualified Security Assessor *or* an Internal Audit if signed by an officer of the company.
- Quarterly Network Scan

Level 2

- Annual PCI Self-Assessment Questionnaire (American Express—not required)
- Quarterly Network Scan

Level 3

- Annual PCI Self-Assessment Questionnaire (American Express—not required)
- Quarterly Network Scan (American Express—not mandatory to submit except at the request of American Express)

Level 4 (Visa and MasterCard only)

- Annual PCI Self-Assessment Questionnaire (not mandatory to submit except at the request of Visa or MasterCard)
- Quarterly Network Scan (not mandatory to submit except at the request of Visa or MasterCard)

As you can see from the list above, all merchants are required to complete a Quarterly Network Scan. This scan, which must be completed by an Approved Scanning Vendor, is an automated tool that checks systems for vulnerabilities. It conducts a nonintrusive scan to remotely review networks and Web applications based in the externally facing Internet Protocol (IP) address provided by the merchant.

Like merchants, payment card brands also define levels for service providers. Exhibit 1.8 summarizes these level definitions for Visa and

Level	Visa	MasterCard
Level 1	All VisaNet processors (member and nonmember) All payment gateways	All TPPs All DSEs that store, transmit, or process more than one million annual transactions
Level 2	All providers that store, transmit, or process more than one million annual transactions	All DSEs that store, transmit, or process less than one million annual transactions
Level 3	All providers that store, transmit, or process less than one million annual transactions	N/A

EXHIBIT 1.8 Service-Provider Level Definitions

MasterCard. Note, American Express, JCB, and Discover card brands do not classify merchants based on annual transaction volume. Refer to the Resources section for the Web site addresses for these payment card brands.