Enterprise Data Management Solutions
Executive brief
March 2008

IBM Information Management software

Payment Card Industry Data Security Standard (PCI DSS): Addressing the internal threat

Contents

Why the concern over payment cards and privacy compliance?

The use of payment cards as a form of currency in exchange for goods and services is undoubtedly a staple that supports economic growth around the world. For example, in the United States (US) alone, the estimated 641 million credit cards in circulation account for about $1.5 trillion in consumer spending each year.[1] Similarly, between October and December 2007, consumers in the United Kingdom (UK) spent £32.4 billion on credit cards, the second highest sum in history. Over the same period, £59 billion was spent using debit cards, the highest since 2000, when debit spending was were first recorded.[2]

However, the proliferation of high-profile data breaches has exposed the vulnerability of payment card processors, point-of-sale vendors and financial institutions that are not properly securing confidential customer information. In the US, the Privacy Rights Clearing House has reported that more than 218 million personally identifiable records were exposed from January 2005 to March 2008, costing billions of dollars.[3]

Facing increasing risk and financial losses resulting from the misappropriation and misuse of customer information, the payment card industry had to take the initiative. The PCI DSS represents the payment card industry's response to these breaches. Going forward, merchants and retailers who cannot protect consumer payment card information will be held accountable.

About the PCI DSS

The PCI DSS is a multifaceted set of regulations that defines requirements for implementing security management policies, procedures, network architecture, software design and other critical protective measures. With the goal of improving the security of electronic payments, the PCI DSS represents a unified, industry standard for protecting cardholder data that is stored, transmitted or processed.

The Payment Card Industry Data Security Standard (PCI DSS) was initiated by MasterCard International and Visa in January of 2005, and later endorsed by American Express. The Standard has evolved in response to the overwhelming occurrences of data and identity theft from privacy breaches, as well as fraud resulting from the misappropriation of cardholder data.

In September 2006, Visa, MasterCard, JCB International, Discover and American Express formed an independent organization, the PCI Security Standards Council, to oversee the implementation of the Standard. The council's mission is to enhance payment account data security by fostering broad adoption of the PCI DSS.

What are the PCI DSS requirements? The primary objective of the PCI DSS is to ensure that cardholder data is protected. The Standard includes 12 requirements across five categories, concentrating on data authentication, access control, audits and data encryption. To comply, companies that handle payment card information are required to establish stringent security policies, processes and procedures.[4]

The Standard covers a range of issues, such as maintaining a secure network, protecting cardholder information, managing risk, implementing control measures and monitoring test networks (see Table 1).

Table 1. PCI DSS requirements*

	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
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

*Payment Card Industry (PCI) Data Security Standard – Version 1.1. PCI Security Standards Council, Sept. 2006.

Who must comply with PCI DSS? To protect confidential cardholder data, the Standard must be implemented by all members, merchants and service providers that store, process or transmit cardholder information, regardless the size of the entity and volume of transactions processed. However PCI DSS requirements do not only apply to electronic data. Businesses are duty bound to dispose of printed material which contains payment card details and credit cardholder data in an appropriate way.

All merchants that acquire payment card transactions are categorized in the following levels, based on the number of annual transactions processed:

- Level 1: Merchants with more than 6 million card transactions and merchants which cardholder data has been compromised.
- Level 2: Merchants with card transactions between 1 and 6 million
- Level 3: Merchants with card transaction between 20,000 and 1 million
- Level 4: All other merchants

These levels determine the validation processes that a merchant must undertake in order to achieve and maintain compliance.

All service providers that process credit card transactions are categorized in the following levels:

- Level 1: All payment processors and payment gateways
- Level 2: All service providers not in Level 1 but with more that one million credit card accounts or transactions.

- Level 3: Service providers not in Level 1, with fewer than one million annual credit card accounts or transactions.

These levels determine the validation processes that a service provider must undertake in order to achieve and maintain compliance.

Why should you take action to comply?

If you do not have the proper controls in place to protect cardholder data, your organization has a much greater risk of becoming the victim of a data breach. The consequences include, but are certainly not limited to, loss of market share, brand damage, loss of customer loyalty and revenue.

A Ponemon Institute study of retail banking customers suggests that consumers will only do business with retailers that can protect their privacy. The study indicates that it would take only a single privacy breach for 34 percent of customers to cease doing business with a company. That number goes up to 45 percent when personal information is breached twice. According to the study, "Trust translates into strong brand loyalty, but the lack of confidence in a bank's data security capability may result in significant customer attrition."[5] A significant reason for this attrition is that American consumers lost about $49.3 billion USD to identity theft in 2006. On average, these consumers spent $535 USD per person just to clean up the aftermath and restore their credit history.[6]

Avoid costly penalties for non-compliance. The big sting of non-compliance with PCI DSS includes fines that can range up to $500,000 USD per incident. For example, during 2006, Visa fined 77 companies for a total of $4.7 million USD, up from 32 fines totaling $3.4 million USD in 2005. However, the most severe penalty is one that can put a merchant out of business. Payment card companies can limit or even revoke a merchant's ability to accept card payments.

Often overlooked are the costs associated with responding appropriately in the aftermath of a data breach. There are costs for more personnel to handle customer inquiries and concerns, public relations to repair a damaged reputation in the media, as well as lawsuit expenses incurred as a result of inadequate data protection.

The bottom line is that protecting consumer information from fraud and misuse is not optional. If your organization manages, stores, transmits or processes cardholder data, you must have safeguards in place to protect this confidential information. Businesses are built on consumer trust and loyalty; any breach of that trust will have devastating financial consequences.

Take steps to reduce the risk of a data breach. Several major retailers have unfortunately been the victims of multiple data breaches. T.J. Maxx[7], BJ's Wholesale Club, DSW and Polo Ralph Lauren have all experienced data breaches that have put the personal data of a significant number of their customers at risk.

With the T.J. Maxx incident, which was first discovered in December 2006, the company experienced an "unauthorized intrusion" into its computer systems that process and store customer transactions including credit card, debit card, personal check and merchandise return transactions. Hackers may have fled with information from transactions in the US, Canada and Puerto Rico. In the end, the hack may affect a wide range of credit card companies and thousands of consumers in the US, UK, Ireland and other countries.[8]

According to the Federal Trade Commission, BJ's Wholesale Club's lax data security led to a series of fraudulent purchases at non-BJ's stores. These purchases were made using counterfeit credit cards that contained personal information that BJ's had previously collected from the magnetic stripes of customers' credit cards. As a result of the fraud, the affected financial institutions filed suit against BJ's to recover damages. Under terms of the settlement, BJ's will implement a comprehensive information security program subject to third-party audits every other year for the next two decades.[9]

In the case of DSW, information about more than 1.4 million credit card and 96,000 check transactions were stolen from 108 DSW shoe stores, according to its parent company, Retail Ventures. The Polo Ralph Lauren breach compromised the credit card data of as many as 180,000 people.[10]

Capita Financial Administrators Limited (CFA), a third party investment administrator in the UK, discovered that client information had been altered and fraudulent requests for payment had been made to client accounts. The transactions were facilitated by colluding CFA staff, and requests for more than £1 million were detected and stopped, but not before more than £300,000 in fraudulent payments had been made. The company was subsequently fined £300,000 by the UK's Financial Services Authority (FSA) for failures in its anti-fraud systems and controls.[11]

What are internal threats to data privacy?

While companies spend a great deal of time and money to secure their systems from external attacks, many do not realize that 70 percent of data breaches are from internal sources![12]

Customer data is particularly vulnerable to an internal breach – whether by disgruntled employees or careless service providers. Companies may have a strong lock on their main processing systems, but sensitive data resides in many other places. Non-production environments, such as development, testing, backup, quality control and training, are especially vulnerable. For example, charged with delivering new and enhanced business applications, your internal development and quality assurance staff require access to realistic test data. Typically, this data is copied or cloned directly from the production environment for use in non-production databases. This practice opens the possibility for any number of internal data breaches resulting from unrestricted access to confidential customer information, as well as your company's internal financial and human resources information.

In addition, outsourcing application development and testing functions has become commonplace. Once you create copies of your production data for use in non-production environments in an out-sourced location or overseas, it is even more difficult to impose control over who has access to confidential consumer information.

Lastly, laptops and other portable devices that can store or manage confidential information outside a secured location add another level of vulnerability. The loss of data on laptops, USB devices or other types of media containing sensitive data has become all too common. For example, Nationwide Building Society, the UK's largest building organization, was fined £980,000 after an employee's laptop was stolen from his home. The laptop contained the names, addresses and account numbers of nearly 11 million of the building society's customers, exposing them to the risk of financial crimes.[13] Similarly, a laptop containing data from 26.5 million military veterans and their families was stolen from the home of an employee working for the US Department of Veterans Affairs.

Why are non-production environments so vulnerable?

Non-production, like development, testing and training, are popular targets for attack. Why? Because the same measures to protect data in production systems, such as firewalls, encryption and network security, simply will not work in non-production environments. To develop or test applications, your staff must use accurate, realistic data that does not violate the application logic. Real customer data from the production system meets that requirement, but exposing that information compromises privacy. More importantly, companies that use production data for testing purposes violate the PCI DSS Requirements 6 and 7 (see Table 2). These requirements restrict access to and utilization of cardholder data.

Table 2. PCI requirements 6 and 7

Develop and maintain secure systems and applications
6.3 – Develop software applications based on industry best practices and incorporate information security throughout the software development lifecycle
6.3.4 – Production data (live PANs) are not used for testing or development [PANS - personal account numbers]
Restrict access to cardholder data by business need-to-know
7.1 – Limit access to computing resources and cardholder information only to those individuals whose job requires such access

Developers and quality assurance staff do not require access to “real” cardholder data. Rather, they need realistic, contextually accurate data that mimics the information stored in the application database without compromising privacy. Ultimately, merchants need capabilities for masking confidential data so that it can be safely used for application development and testing.

What is the best way to protect consumer data?

Industry analysts agree that an effective solution for protecting confidential data is to apply de-identification techniques when migrating data from production into a test or other non-production environment. De-identification is the process of systematically masking or transforming Personally Identifiable Information

(PII), such as Social Security numbers, bank account numbers, birth dates and addresses. Data that has been scrubbed or cleansed in such a manner is acceptable to use in testing.

Data de-identification enables developers and testers to use realistic test data and produce valid test results, while still complying with PCI DSS. However, it is important to note that the results of the data transformation have to be appropriate in the context of the application. That is, the results of data transformation have to respect the business logic of the application. For example, data that contains alphabetic characters should be substituted with other alphabetic characters, in the appropriate pattern. In addition, the transformed data must be within the range of permissible values.

In addition to providing several ways to mask or de-identify complex relational data, an effective solution should support multiple applications, databases, operating systems and hardware platforms. In short, you need a solution that scales to meet your current and future needs.

IBM Optim supports your PCI compliance initiatives

The IBM® Optim™ Data Privacy Solution offers proven technology that allows organizations to create, mask and maintain realistic, “right-sized” test databases using referentially intact subsets of related test data. Optim provides a variety of data transformation algorithms and built-in lookup tables, and even supports custom data masking routines. Optim produces masked data that is both contextually accurate and application aware.

IT staff can leverage Optim to generate valid, masked values for payment card numbers, national identifiers, names, addresses and other forms of PII. Masking data not only renders the card information useless to thieves, but also enables compliance with PCI DSS Requirements 6 and 7. Additionally, masked data elements can be propagated across related tables to ensure the referential integrity of the database.

Optim supports the leading database management systems and provides federated access capabilities that allow developers to extract and mask appropriate test data from various data sources in a single process. Optim can satisfy your current requirements and can easily adapt to changes in your IT environment. In addition to helping you satisfy compliance initiatives, Optim's capabilities allow can help you reduce the time and costs associated with development and testing throughout the application lifecycle.

Retailers are being targeted by hackers and data thieves alike because of the amount and sensitivity of the customer data they possess. “Expenditure in the name of PCI compliance must be targeted at the most important critical business risks using the philosophy ‘protect the customer’s data and then demonstrate compliance,’ not the reverse.”[14]

The PCI DSS mandates 12 requirements to protect payment card customers. The requirements are clear when it comes to masking confidential data and ensuring that confidential data is only available to those individuals whose job requires it. With comprehensive data masking capabilities that allow you to de-identifying credit card numbers, as well as other PII, IBM Optim can help you protect confidential customer information in your non-production (development, testing, and training) environments to comply with the PCI DSS requirements.

About IBM Optim

IBM® Optim™ enterprise data management solutions focus on critical business issues, such as data growth management, data privacy compliance, test data management, e-discovery, application upgrades, migrations and retirements.

Optim aligns application data management with business objectives to help optimize performance, mitigate risk and control costs, while delivering capabilities that scale across enterprise applications, databases and platforms. Today, Optim helps companies across industries worldwide capitalize on the business value of their enterprise applications and databases, with the power to manage enterprise application data through every stage of its lifecycle.

For more information

To learn more about IBM Optim enterprise data management solutions, contact your IBM sales representative or visit: **www.optimsolution.com**

IBM Software Group
111 Campus Drive
Princeton, NJ
USA, 08540-6400
800.457.7060
609.627.5500
Fax 609.627.7799
www.optimsolution.com

Produced in the United States of America
03-08

[1] CJ Writer, "Credit Cards: What You Need to Know to Avoid Getting Hurt Financially," Associated Content, associatedcontent.com, March 16, 2006.

[2] Grainne Gilmore, "Credit card spend sounds credit crunch alarm," http://business.timesonline.co.uk/tol/business/money/borrowing/article3368934.ece, February 14, 2008.

[3] "A Chronology of Data Breaches," Privacy Rights Clearinghouse, Updated March 17, 2008, www.privacyrights.org

[4] Noel Yuhanna, "Enterprise Databases Need Greater Focus to Meet Regulatory Compliance Requirements," Forrester Best Practices, January 24, 2007.

[5] "2006 Privacy Trust Study for Retail Banking," The Ponemon Institute, LLC and Vontu, Inc., January 2006, as referenced in "Ponemon Institute Names Most Trusted Retail Banks," Vontu Press Release, January 26, 2006.

[6] "Identity Fraud is Dropping, Continued Vigilance Necessary," Javelin Strategy & Research, 2007 Identity Fraud Survey Report, February 2007, as referenced by Jonathan Stempel, "U.S. Identity theft losses fall: study," Reuters, February 1, 2007.

[7] Jaikumar Vijayan, "TJX breach uncovers security holes, wrong practices in retail industry," Computerworld (US online), January 22, 2007.

[8] Paul F. Roberts, "Retailer TJX reports massive data breach," Infoworld.com, January 17, 2007.

[9] Thomas Claburn, "BJ's Wholesale Club Settles FTC Data-Protection Complaint," InformationWeek.com, June 16, 2005.

[10] Alorie Gilbert, "Retailers feel security heat," CNET News.com, April 22, 2005.

[11] "FSA fines Capita Financial Administrators Limited £300,000 in first anti-fraud controls case," Financial Services Authority, FSA/pn/019/2006, March, 16, 2006.

[12] Richard Mogul, "Danger Within – Protecting your Company from Internal Security Attacks," Gartner, August 2002.

[13] "Nationwide fine for stolen laptop," BBC News, News.bbc.co.uk., February 14, 2007.

[14] Avivah Litan and John Pescatore, "Answers to Common Questions about PCI Compliance," Gartner Research, ID Number G00144907, December 7, 2006.

References in this publication to IBM products, programs or services do not imply that IBM intends to make them available in all countries in which IBM operates or does business.

Each IBM customer is responsible for ensuring its own compliance with legal requirements. It is the customer's sole responsibility to obtain advice of competent legal counsel as to the identification and interpretation of any relevant laws and regulatory requirements that may affect the customer's business and any actions the customer may need to take to comply with such laws. IBM does not provide legal advice or represent or warrant that its services or products will ensure that the customer is in compliance with any law.

TAKE BACK CONTROL WITH Information Management

IME14000-USEN-00