



IBM Optim Data Privacy Solution, PCI Module

Highlights

- ***Restrict using cardholder data in development, testing and training environments***
- ***Apply contextual, application-aware and persistent masking techniques to de-identify data***
- ***Protect cardholder data retrieved from point-of-sale (POS) and other processing systems***
- ***Implement a proven solution to support your enterprise privacy strategy***

PCI DSS compliance – a high priority

Companies worldwide rely on payment cards as a secure and convenient way to collect revenue. However, the proliferation of high-profile data breaches has exposed the vulnerability of payment card processors, point-of-sale vendors and financial institutions that have not properly secured personal customer information.

Protecting sensitive payment card data is essential to mitigate the risk of data breaches, where the misappropriation and misuse of sensitive personal information can lead to identity theft. Without the appropriate safeguards in place, companies risk losing market share, brand equity, customer loyalty and revenue.

In response to the overwhelming occurrences of data/identity theft from privacy breaches and fraud, the Payment Card Industry Data Security Standard (PCI DSS) was developed to put an end to the millions of dollars in losses from the misappropriation of cardholder data. Conceived by

MasterCard® and Visa®, and later endorsed by American Express®, JCB® and Discover®, the PCI DSS is a multifaceted set of regulations that represents a unified, industry standard for protecting cardholder data that is stored, transmitted or processed.

To achieve compliance with the PCI DSS, companies that handle and process payment card transactions must establish stringent security policies and procedures. The consequences of non-compliance can include fines in the range of \$500,000 per incident. But perhaps the most severe penalty is that payment card companies can limit or even revoke the privilege to accept card payments, which significantly increases a merchant's risk for going out of business. 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!

Table 1. Key provisions of PCI DSS requirements 6 and 7

Requirement 6 – 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]

Requirement 7 – 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

Need to protect cardholder data from the inside out

Although most organizations have a strong lock on their main production systems, sensitive data resides in many other places. The same measures that protect data in production systems, such as firewalls, encryption and network security, simply will not work in non-production (development, testing and training) environments. In this regard, PCI DSS requirements 6 and 7 (see Table 1) pose a particular challenge for organizations. These requirements restrict how companies utilize certain confidential information, and how they develop and test their mission critical systems.

For example, requirement 6.3.4 states that live personal account numbers should not be used in testing and

development. So, companies can no longer simply copy real production data into their test systems. But at the same time, IT staff relies on realistic data to support application development, testing and training. What are the options? How can IT obtain accurate, realistic data to develop and test applications, without violating PCI DSS requirements and compromising customer privacy?

Industry analysts agree that de-identifying data is a best practice for protecting data in non-production environments. In fact, data masking technology can help protect private data in test environments by de-identifying customer, financial or company confidential data. De-identification is the process of systematically masking or transforming sensitive

information before it is migrated from production into a test or other non-production environment. Data that has been scrubbed or cleansed in such a manner can no longer be traced back to an individual and is acceptable to use in non-production environments. Masking data enables developers and testers to use realistic, contextually accurate data and produce valid test results, while still complying with PCI DSS.

IBM Optim satisfies your PCI DSS requirements

The IBM® Optim™ Data Privacy Solution, PCI Module, provides a comprehensive set of data masking techniques that can be used to de-identify many types of sensitive information, such as credit/debit card numbers, bank account numbers, names and addresses. The masked data is contextually accurate and application aware, that is, the results of the transformation are in the appropriate context and respect the application logic.

For example (see Figure 1), in masking payment card data, character and numeric values, as well as date and time values, like payment card expiration dates, can be masked using a random string of values. In

addition, the PCI Module's Payment Card Masking function generates valid and unique, yet de-identified, payment card numbers according to the issuer's format requirements, and supports American Express, Diners Club®, Discover, JCB, MasterCard and Visa.

The PCI Module's application-aware masking capabilities are designed to mask data, like names and street addresses, in a way that resembles the look and feel of the original information. Context-aware, prepackaged data masking routines make it easy to de-identify data elements, such as payment card numbers and e-mail addresses.

The PCI Module offers flexibility in populating a non-production environment with masked values obtained from user-defined substitution values. Predefined replacement values specific to countries worldwide can be used to replace real data with fictitious, but contextually accurate, substitutes. These replacement values are provided to mask first names, surnames, addresses, phone numbers, payment card numbers and date-of-birth information. The replacement feature also makes



Figure 1: Sample credit card before and after data masking.

it possible to mask multiple data elements. For example, it is easy to mask an entire street address/city/state/postal or ZIP code.

To ensure that masked data is propagated accurately throughout the application database, the PCI Module's persistent masking capability generates transformed replacement values for source data elements and propagates the replacement values consistently and accurately across applications, databases, operating systems and platforms. For example, masked payment card information can be propagated accurately across an order entry application that relies on an IBM DB2® database and a billing system that uses an Oracle® database. The data can be propagated accurately even when

each application resides on a different platform. The PCI Module adapts easily into an existing IT infrastructure so companies can comply with PCI DSS requirements and protect the confidentiality of sensitive information across the enterprise.

Make IBM Optim part of your complete privacy strategy

The IBM Optim Data Privacy Solution, PCI Module, is the first solution of its kind developed specifically to address PCI DSS requirements 6 and 7. With data masking capabilities specifically designed for PCI DSS compliance, organizations can mask payment card numbers, as well as other personally identifiable information consistently and accurately. Optim helps companies store, process and transmit cardholder data for compliance with the PCI DSS.

Protecting privacy represents a best practice for managing sensitive data and simply makes good business sense. Data de-identification provides a “safe sandbox” for mission-critical application testing, enabling companies to help protect privacy and safeguard customer loyalty. The IBM Optim Data Privacy Solution, PCI Module provides flexible capabilities that can scale to support your current and future data privacy requirements. In addition to satisfying PCI DSS requirements to protect sensitive data in non-production environments, with Optim an organization is better positioned to satisfy local, state, national and international privacy regulations.

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.



© Copyright IBM Corporation 2008

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

Produced in the United States of America
05-08
All Rights Reserved

DB2, IBM, the IBM logo, and Optim are trademarks or registered trademarks of the IBM Corporation in the United States, other countries or both. All other company or product names are trademarks or registered trademarks of their respective owners.

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.