

Key Steps to Meeting PCI DSS 2.0 Requirements Using Sensitive Data Discovery and Masking

SUMMARY

The Payment Card Industry Data Security Standard (PCI DSS) defines 12 high-level security requirements directed at helping to stem credit card fraud. These include requirements to protect cardholder data, to maintain secure systems and applications, and to ensure that cardholder information is available internally on a strict need-to-know basis. Companies that handle cardholder data must adhere to these requirements and validate their compliance with regular external audits. Dataguise products DgDiscover™, DgMasker™ and DgDashboard™ help companies with their PCI DSS compliance programs by enabling them to quickly identify cardholder data in networks and systems, facilitate safe testing of applications with masked production data, and manage sensitive data risks in their environments.

OVERVIEW

The Payment Card Industry Data Security Standard (PCI DSS) was first announced December, 2004 as a response to the growing costs associated with credit card fraud through data exposure. American Express, Discover, JCB, MasterCard Worldwide and Visa International worked together through the auspices of the Payment Card Industry Security Standards Council to establish the guidelines to help organizations who process card payments secure their environments to prevent credit card fraud, hacking and various other security breaches.

The PCI DSS defines twelve high-level security requirements broken down into six control objectives. The latest iteration of the standard (PCI DSS version 2.0) released October, 2010, must be adopted by all organizations with payment card data by January 1, 2011.

WHO MUST COMPLY?

Even though PCI DSS was developed for

the U.S., it has become a global standard for all entities handling cardholder data. A company processing, storing, or transmitting credit card data must be PCI DSS compliant or they risk losing the ability to process credit card payments. Entities handling cardholder data are broken down into two distinct categories:

- Merchants who are authorized acceptors of cards for the payment of goods and services.
- Service Providers who are organizations that process, store, or transmit cardholder data on behalf of card members, merchants or other service providers.

Merchants and Service Providers are classified at different levels based on the number of annual transactions processed – although this can differ depending on the credit card issuer. In general, Level 1 Merchants and Level 1 and 2 Service Providers submit the greatest number of transactions and therefore must validate

Control Objective	Requirement
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

Control Objectives and Requirements for the Payment Card Industry Data Security Standard (PCI DSS)

compliance with an audit by a PCI DSS Qualified Security Assessor (QSA). Level 2, 3, and 4 Merchants and Level 3 Service Providers must complete an annual self-assessment questionnaire and quarterly network scans to demonstrate compliance.

PENALTIES FOR NON-COMPLIANCE

Due to the financial impact of credit card fraud and the additional cost of card re-issuance, credit card companies are imposing fines on non-compliant entities. In November 2007, for example, TJ Maxx agreed to pay \$40.9 million in a settlement with Visa for a loss of 45.7 million cardholder records. In the wake of the TJ Maxx incident, Visa announced that it has started fining Level 1 Merchants \$25,000 per month for PCI non-compliance.

In addition to fines, merchants who fail to maintain PCI compliance can face termination by the payment card association. Termination can list the merchant in the industry's MATCH registry (Member Alert To Control High-Risk) which could make it nearly impossible to get a new merchant account elsewhere.

DATAGUISE SOLUTIONS FOR MANAGING SENSITIVE DATA RISK

The Dataguise solution for data protection is organized around four critical data protection functionalities:

- Finding databases deployed on the network,
- Searching databases and shared file systems for sensitive data,
- Remediating sensitive data risk in application data sets with a next generation, high-speed data masking, and
- Reporting on the existence of sensitive data risks in the enterprise.

These are implemented with a unique suite of integrated solutions including DgDiscover, DgMasker, and DgDashboard.

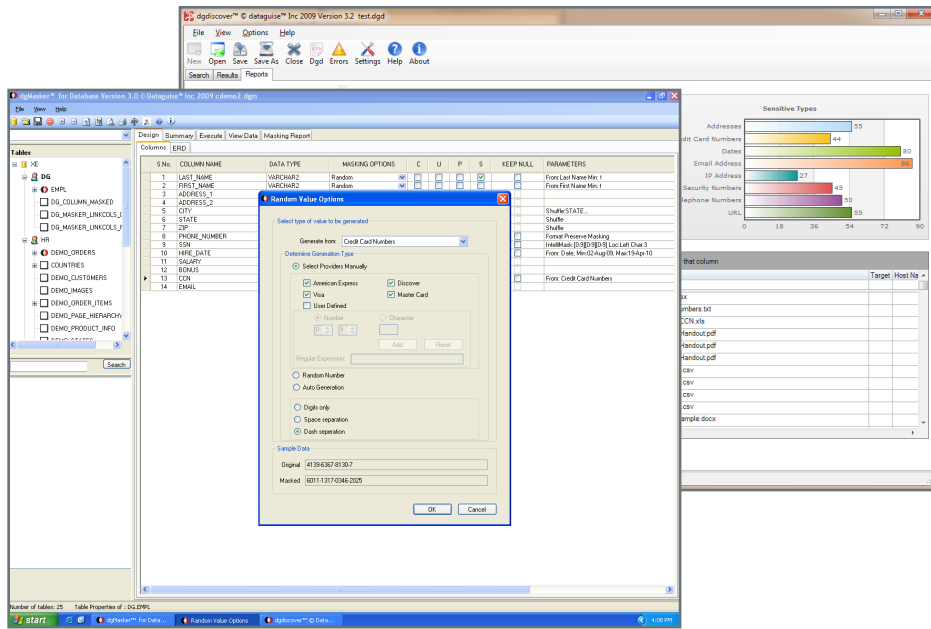
DGDISCOVER

Typical large enterprises have thousands of development and test databases deployed in their IT environment. DgDiscover identifies Oracle, SQL Server, MySQL, DB2, and other database instances

deployed in the network. It then searches for sensitive and potentially sensitive data within these databases. DgDiscover employs sophisticated pattern matching algorithms to automatically identify data such as credit card numbers, expiration dates, social security numbers, and phone numbers, and creates detailed reports showing where this information resides in database tables. In addition to databases, DgDiscover has the unique ability to apply the same policies to search unstructured data on shared file systems such as text files, Word, Excel, PowerPoint documents, and other file formats.

DGMASKER

DgMasker is an advanced data security solution which helps enterprises protect data and address compliance requirements by selectively masking, or de-identifying sensitive data in databases which are cloned, or copied, for development, test, QA or business analysis uses. DgMasker automatically determines data relationships and ensures that the masked data preserves data integrity and meets application business rules. Its unique,



Dataguise DgDiscover and DgMasker identify sensitive data in production data sets, and protect that data with next-generation, masking-in-place technology.

masking-in-place architecture delivers high performance and can be run interactively or in batch mode on a remote server to support automated software development processes.

DGDASHBOARD

Understanding and effectively managing the risks to sensitive data under their care is a major security challenge for managers. DgDashboard (available Q1, 2011) is an enterprise management console which leverages the results generated by DgDiscover and DgMasker to provide managers with a comprehensive view of their sensitive data disclosure risks. DgDashboard provides information about sensitive data found in production and non-production environments, providing them with a reliable inventory of the types and locations of sensitive data under their care. DgDashboard also helps managers manage risk by providing them with a view of whether or not sensitive data found in non-production environments is protected by masking. DgDashboard also shows where the greatest exposures are with regard to sensitive data contained in document files hosted on

shared file systems and SharePoint servers on the network.

DATAGUISE SOLUTIONS HELP ORGANIZATIONS ADDRESS PCI DSS REQUIREMENTS

As a state-of-the-art solution for managing the exposure risks for sensitive data, Dataguise solutions can help organizations improve the way they protect sensitive PCI data. Organizations that use Dataguise solutions have a better knowledge of where sensitive information such as cardholder data resides, can support key business processes such as application development, test and deployment without exposing cardholder data, and have a more complete view of the organization's activities in protecting cardholder data. In addition to improving an organization's sensitive data management practices, Dataguise solutions can also be applied to address specific PCI DSS requirements. The included tables provide details for each applicable subrequirement.

Requirement 3: Protect Stored Cardholder Data

The PCI DSS requirements are focused on the prevention of intentional or unintentional disclosure of cardholder data such as personal account numbers (PANs), cardholder names, service codes and card expiration dates. The developers of the PCI DSS requirements understood that threats to sensitive data could come from internal as well as external sources. As a result, the requirements mandate that practices need to be followed to restrict access to card data to employees who have a need to know based on business requirements, and that other employees have access only to the minimum amount of cardholder information they need to perform their jobs. In addition, businesses need to take measures so that in the event a hacker gains access to an internal network he can't retrieve any useful information.

Dataguise solutions help organizations protect stored cardholder data in a number of ways. DgDiscover allows application administrators and analysts to prepare

Requirement 3: Protect stored cardholder data		
Requirement	Testing Procedures	Dataguise Capabilities
<p>3.2 Do not store sensitive authentication data after authorization (even if encrypted). Sensitive authentication data includes the data as cited in the following Requirements 3.2.1 through 3.2.3: Note: It is permissible for issuers and companies that support issuing services to store sensitive authentication data if there is a business justification and the data is stored securely.</p>	<p>3.2.c For each item of sensitive authentication data below, perform the following steps:</p>	
<p>3.2.1 Do not store the full contents of any track (from the magnetic stripe located on the back of a card, equivalent data contained on a chip, or elsewhere). This data is alternatively called full track, track, track 1, track 2, and magnetic-stripe data.</p>	<p>3.2.1 For a sample of system components, examine data sources, including but not limited to the following, and verify that the full contents of any track from the magnetic stripe on the back of card or equivalent data on a chip are not stored under any circumstance:</p> <ul style="list-style-type: none"> • Incoming transaction data • All logs (for example, transaction, history, debugging, error) • History files • Trace files • Several database schemas • Database contents 	<p>DgDiscover automatically locates sensitive data in unstructured sources such as file, documents and log files, as well as in structured database schemas and contents.</p>
<p>3.2.2 Do not store the card verification code or value (three-digit or four-digit number printed on the front or back of a payment card) used to verify card-notpresent transactions.</p>	<p>3.2.2 For a sample of system components, examine data sources, including but not limited to the following, and verify that the three-digit or four-digit card verification code or value printed on the front of the card or the signature panel (CVV2, CVC2, CID, CAV2 data) is not stored under any circumstance:</p> <ul style="list-style-type: none"> • Incoming transaction data • All logs (for example, transaction, history, debugging, error) • History files • Trace files • Several database schemas • Database contents 	<p>DgDiscover can leverage the user defined expression feature to automatically locate card verification codes in log files, documents and database schemas and contents.</p>

Requirement 3: Protect stored cardholder data		
Requirement	Testing Procedures	Dataguise Capabilities
3.2.3 Do not store the personal identification number (PIN) or the encrypted PIN block.	3.2.3 For a sample of system components, examine data sources, including but not limited to the following and verify that PINs and encrypted PIN blocks are not stored under any circumstance: <ul style="list-style-type: none"> • Incoming transaction data • All logs (for example, transaction, history, debugging, error) • History files • Trace files • Several database schemas • Database contents 	DgDiscover can leverage the user defined expression feature to automatically locate likely PIN numbers in log files, documents and database schemas and contents.
3.3 Mask PAN when displayed (the first six and last four digits are the maximum number of digits to be displayed). Notes: This requirement does not apply to employees and other parties with a legitimate business need to see the full PAN. This requirement does not supersede stricter requirements in place for displays of cardholder data—for example, for point-of-sale (POS) receipts.	3.3 Obtain and examine written policies and examine displays of PAN (for example, on screen, on paper receipts) to verify that primary account numbers (PANs) are masked when displaying cardholder data, except for those with a legitimate business need to see full PAN.	DgMasker integrates into application development and testing processes and provides a number of options for masking PAN (primary account number) information in databases. For example, DgMasker can mask PANs with character masking to selectively display digits in a customer support database. It can also employ more sophisticated options such as “intelli-masking,” which masks only selected characters within a string with random values, generating masked values which can be consumed by downstream applications.
3.4 Render PAN unreadable anywhere it is stored (including on portable digital media, backup media, and in logs) by using any of the following approaches: <ul style="list-style-type: none"> • One-way hashes based on strong cryptography (hash must be of the entire PAN) • Truncation (hashing cannot be used to replace the truncated segment of PAN) • Index tokens and pads (pads must be securely stored) • Strong cryptography with associate key-management processes and procedures 	3.4.b Examine several tables or files from a sample of data repositories to verify the PAN is rendered unreadable (that is, not stored in plain-text).	DgDiscover searches databases and files to verify that PAN data is adequately protected. DgDashboard summarizes the search results across multiple databases to help managers prepare for PCI audits. DgMasker protects translation tables with strong hashing algorithms to prevent potential exposure of PANs while providing consistency and repeatability in masking operations.
	3.4.c Examine a sample of removable media (for example, back-up tapes) to confirm that the PAN is rendered unreadable.	DgDiscover examines documents and text files from removable media to identify readable PAN data.
	3.4.d Examine a sample of audit logs to confirm that the PAN is rendered unreadable or removed from the logs.	DgDiscover examines audit log files (both unstructured files and logs stored in databases) to identify where they might contain readable PAN data.

Requirement 6: Develop and maintain secure systems and applications		
Requirement	Testing Procedures	Dataguise Capabilities
6.4 Follow change control processes and procedures for all changes to system components. The processes must include the following:	6.4 From an examination of change control processes, interviews with system and network administrators, and examination of relevant data (network configuration documentation, production and test data, etc.), verify the following:	
6.4.3 Production data (live PANs) are not used for testing or development	6.4.3 Production data (live PANs) are not used for testing or development.	DgMasker masks sensitive information including PANs in production data sets so that they may be safely leveraged for non-production applications including testing and development. DgDiscover finds database instances on the network and searches databases to identify and locate sensitive data (including PANs), enabling managers and auditors to verify that sensitive data is not being used in non-production environments.

for PCI DSS audits by locating and then searching systems which are potential repositories for cardholder data. DgMasker protects cardholder data contained in application data sets so these can be safely leveraged to support application development, test, support activities as well as business analysis.

Requirement 6: Develop and Maintain Secure Systems and Applications

The developers of the PCI DSS requirements understood that vulnerabilities in systems and applications are a major means through which cardholder data is compromised. As a result, the requirements direct that organizations take specific steps to ensuring systems and applications are developed and implemented to a high minimum standard of security.

Dataguise solutions help organizations securely develop, test and maintain their applications handling sensitive cardholder data. DgDiscover analyzes the data contained in application data sets to automatically identify where the application maintains information such as cardholder

names, account numbers and expiration dates. Next, this information can be used to specify appropriate masking policies which can be applied to protect the sensitive data quickly and efficiently. The resulting masked data set can then be used to develop and test applications with the goal of making them more robust and secure without exposing the cardholder data to unauthorized internal users or leaving it vulnerable to hackers who might gain access to data repositories.

Requirement 7: Restrict Access to Cardholder Data by Business Need to Know

Best practice for handling sensitive data in the enterprise requires that organizations implement the principle of “least privilege” when exposing sensitive data to users and systems. For example, in most organizations there is no reason that developers and application support analysts should have access to live cardholder data. However, this requirement also directs that people who do have a requirement to access cardholder data are restricted to as little of it as possible in order to accom-

plish the business mission. For example, a customer support analyst may need to view only the last few digits of a personal account number (PAN) in order to verify a customer’s account.

DgMasker allows organizations to implement a least privileges policy by masking sensitive data so it is not exposed to users lacking a business need to know. In addition, the masking policies supported by DgMasker are fast and flexible enough to masking the same data multiple different ways. For example, a masked data set generated to support development and test may contain realistic but fictitious PANs, while a data set generated to support customer support organizations or business analysts may mask all but the last four digits of PANs.

CONCLUSION

The Payment Card Industry Data Security Standard has been successful in that it has motivated organizations that handle cardholder information to examine and in many cases make significant improvements to their information systems pro-

Requirement 7: Restrict access to cardholder data by business need to know		
Requirement	Testing Procedures	Dataguise Capabilities
7.1 Limit access to system components and cardholder data to only those individuals whose job requires such access. Access limitations must include the following:	7.1 Obtain and examine written policy for data control, and verify that the policy incorporates the following:	
7.1.1 Restriction of access rights to privileged user IDs to least privileges necessary to perform job responsibilities	7.1.1 Confirm that access rights for privileged user IDs are restricted to least privileges necessary to perform job responsibilities.	Data masking with DgMasker helps organizations implement a policy of least privilege access to cardholder data by allowing the custodians of the data to create realistic-looking data sets where the sensitive information is protected from view. As a result, individuals involved in functions such as test, development and support can work from application instances running on masked data sets, reducing the number of IDs required for production application instances.

grams and practices. PCI DSS requires such organizations to take specific steps to protect cardholder data, harden applications and systems that maintain cardholder data against attacks, and restrict access to this data within the organization on a strict, need to know basis. Dataguise solutions help administrators, managers and internal auditors with their PCI DSS compliance programs by identifying cardholder information within systems, protecting them with next-generation masking technology, and manage their sensitive data risks by providing a consolidated view of their data protection processes.

ABOUT DATAGUISE

Dataguide helps organizations safely leverage their enterprise data with a comprehensive risk-based data protection solution. By automatically locating sensitive data, transparently protecting it with high performance Masking on Demand™, and providing actionable intelligence to managers, Dataguide improves data risk management, operational efficiencies and regulatory compliance costs. To learn more, visit www.dataguide.com.



Dataguide™ Inc.
2201 Walnut Ave. #260
Fremont, CA 94538
Phone: 510-824-1036
Email: info@dataguide.com

©Dataguide Inc. 2010. All Rights Reserved