

Complying with Payment Card Industry Security Standards

BY DONNA FLUSS

Data security has long been a serious concern for enterprises across all verticals, particularly for the financial services, healthcare and insurance industries. It is also a matter of great importance to contact centers, which handle credit card data and other personal customer information. Recent, highly publicized data security breaches involving the handling of stored credit card information have propelled this issue to even higher levels of importance for enterprises and the technology vendors that support them. Retailers, which have traditionally underinvested in technology, face serious fines from credit card companies and their merchant banks if they are not in compliance with the new Payment Card Industry (PCI) Security Standards. Eventually, non-compliance with PCI standards may result in not being able to accept credit cards.

Customer calls recorded to meet compliance and regulatory requirements for sales verification, dispute resolution or for quality assurance and training often include a great deal of sensitive customer credit card information. Most call centers have implemented procedures to prevent security breaches, such as not allowing agents to bring any personal items in or out, but other vulnerabilities remain.

PCI standards have been around for a few years but became a requirement for many contact centers in 2007. As a result, PCI received little attention until this year, when the QA/Recording vendors realized they needed to make changes to their applications to

The amount of sensitive customer credit card information that is recorded in the contact center requires special safeguarding strategies and technologies to avoid penalties for PCI noncompliance.

comply with PCI requirements. The major challenge with PCI is that the interpretation of the requirement is left up to each enterprise or auditor, and therefore, no standard approach has been developed.

WHAT ARE PCI DATA SECURITY STANDARDS?

All of the payment card associations recognize the need to safeguard customer information by ensuring that members, merchants and service providers meet minimum levels of data security. Before PCI security standards became a requirement, each association established, maintained and enforced its own policies. In December 2004, American Express, Discover Financial Services, MasterCard Worldwide and Visa International joined forces to align their separate policies and develop a unified set of security standards. In January 2005, the alliance released the first version of the Payment Card Industry Data Security Standard (PCI DSS). The revised standard, PCI DSS 1.1, became effective September 7, 2006.

PCI DSS 1.1 is a worldwide data security requirement that applies to all members, merchants, service providers and organizations that store, transmit or process cardholder data. As of January 1, 2007, all new PCI certifications and newly initiated recertifications must comply with PCI DSS version 1.1. The standard provides 12 general data security requirements:

BUILD AND MAINTAIN A SECURE NETWORK

1. Install and maintain a firewall configuration to protect data.
2. Do not use vendor-supplied defaults for system passwords and other security parameters.

PROTECT CARDHOLDER DATA

3. Protect stored data.
4. Encrypt transmission of cardholder data and sensitive information across public networks.

MAINTAIN A VULNERABILITY MANAGEMENT PROGRAM

5. Use and regularly update antivirus software.
6. Develop and maintain secure systems and applications.

IMPLEMENT STRONG ACCESS CONTROL MEASURES

7. Restrict access to 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.

Information in the table (see next page), taken from the PCI DSS 1.1, provides a partial list of cardholder

and sensitive authentication data, along with storage and protection requirements.

Full details about PCI requirements, as well as a copy of the PCI DSS 1.1, can be obtained at the PCI Security Standards Council's Web site, www.pcisecuritystandards.org.

PCI COMPLIANCE

It's important to point out that, while the PCI Security Standards Council manages the standards, it is the individual card brands that enforce compliance and issue penalties for noncompliance. Due to differences in level definitions, risk levels and the local payments architecture, each card brand — and potentially each region — may have a different validation deadline.

While the best answer to the question of compliance deadlines is to check with your acquirer and card brand, the following general

deadlines apply for U.S. merchants:

SEPTEMBER 30, 2007 — The date by which all level 1 merchants (those processing six million or more transactions annually) were expected to be fully PCI DSS compliant.

DECEMBER 31, 2007 — The date by which all level 2 merchants (1,000,000-5,999,999 transactions annually) were expected to be fully PCI DSS compliant.

To some extent, compliance with PCI DSS is interpretive — organizations' definitions of "business need-to-know" may differ. Each business is responsible for ensuring that it is in compliance with the current PCI standard, federal and state regulations, and internal/external auditing requirements for data security.

VENDORS RESPOND TO MARKET NEED

Many of the Quality Management/Liability Recording suite

providers, also known as Workforce Optimization vendors, have introduced product enhancements to the recording, security, encryption and auditing capabilities of their suites to enable customers to comply with PCI standards. Some vendors are investing in enhanced encryption functionality. Others are investing in tagging to notify the application when it should stop recording. Some vendors are using speech analytics to prevent recording and/or to mask sensitive customer data. The list of vendors that have addressed or are working on enhancements to support PCI standard compliance includes (but is not limited to): Autonomy etalk, CallCopy, NICE, OnviSource, TeleDirect, Verint and VPI.

DON'T DELAY

Organizations that do not meet PCI data security requirements run the risk of financial or operational consequences and/or the possibility of class action suits, as well as a public relations debacle. Contact center managers should work with their compliance officers, internal and external auditors, merchant banks, IT groups and Quality Management/Recording vendors to ensure compliance with these important standards. ●

Partial List of PCI Requirements

	Data Element	Storage Permitted	Protection Required	PCI DSS Req. 3.4
Cardholder Data	Primary Account Number (PAN)	Yes	Yes	Yes
	Cardholder Name*	Yes	Yes	No
	Service Code*	Yes	Yes	No
	Expiration Date*	Yes	Yes	No
Sensitive Authentication Data**	Full Magnetic Stripe	No	N/A	N/A
	CVC2/CVV2/CID	No	N/A	N/A
	PIN/PIN Block	No	N/A	N/A

* These data elements must be protected if stored in conjunction with the PAN. This protection must be consistent with PCI DSS requirements for general protection of the cardholder environment. Additionally, other legislation (for example, related to consumer personal data protection, privacy, identity theft or data security) may require specific protection of this data, or proper disclosure of a company's practices if consumer-related personal data is being collected during the course of business. PCI DSS, however, does not apply if PANs are not stored, processed or transmitted.

** Sensitive authentication data must not be stored subsequent to authorization (even if encrypted).

SOURCE: PCI DSS 1.1 (September 2006)



DONNA FLUSS is the Founder and President of DMG Consulting LLC.
donna.fluss@dmgconsult.com