PCI DSS Compliance

7/18/2011

Americas Headquarters
OAISYS
7965 South Priest Drive, Suite 105
Tempe, AZ 85284
USA
www.oaisys.com
(480) 496-9040

OVERVIEW

The Payment Card Industry (PCI) Data Security Standard (DSS), a set of comprehensive requirements for enhancing payment account data security was developed by the founding payment brands of the PCI Security Standards Council, including American Express, Discover Financial Services, JCB International, MasterCard Worldwide, and Visa Inc. International to help facilitate the broad adoption of consistent data security measures on a global basis.

The PCI DSS is a multifaceted security standard that includes requirements for security management, policies, procedures, network architecture, software design, and other critical protective measures. This comprehensive standard is intended to help organizations proactively protect customer account data.

As it relates expressly to the use of call recording technology, OAISYS recording solutions offer several unique feature capabilities that are specifically designed to address the PCI DSS. This document outlines the core requirements that make up the current PCI DSS, the specific requirements that are relevant to the use of call recording and how OAISYS solutions can help organizations to achieve PCI DSS compliance.

PCI DSS CORE PRINCIPLES AND REQUIREMENTS

The core of the PCI DSS is a group of principles and accompanying requirements, around which the specific elements of the DSS are organized as outlined below:

BUILD AND MAINTAIN A SECURE NETWORK

Requirement 1: Install and maintain a firewall configuration to protect cardholder data

Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters

PROTECT CARDHOLDER DATA

Requirement 3: Protect stored cardholder data

Requirement 4: Encrypt transmission of cardholder data across open, public networks

MAINTAIN A VULNERABILITY MANAGEMENT PROGRAM

Requirement 5: Use and regularly update anti-virus software

Requirement 6: Develop and maintain secure systems and applications

IMPLEMENT STRONG ACCESS CONTROL MEASURES

Requirement 7: Restrict access to cardholder data by business need-to-know

Requirement 8: Assign a unique ID to each person with computer access

Requirement 9: Restrict physical access to cardholder data

REGULARLY MONITOR AND TEST NETWORKS

Requirement 10: Track and monitor all access to network resources and cardholder data

Requirement 11: Regularly test security systems and processes

MAINTAIN AN INFORMATION SECURITY POLICY

Requirement 12: Maintain a policy that addresses information security

CALL RECORDING AND PCI DSS

It is important to note that no software or solution is actually PCI compliant with the exception of software that actually accepts and processes payment cards, such as card readers and online payment card validation solutions. While software solutions like call recording and customer relationship management (CRM) software and hardware such as business communications systems cannot actually be deemed PCI DSS compliant, those products that are properly designed and developed with respect to PCI DSS can help businesses to facilitate compliance with the guidelines.

OAISYS call recording solutions when used properly, provide the appropriate security protocols and feature capabilities that can enable organizations to comply with PCI DSS. If your business takes card payments over the telephone, implementing PCI DSS can help protect you and your customers against fraud. If PCI DSS is ignored, you could be fined, and ultimately merchant service privileges could be withdrawn, resulting in a significant loss of business.

All twelve PCI DSS standards are important to any business concerned with ensuring PCI compliance, but a few of the requirements are particularly important as it relates to call recording. These specific requirements are highlighted in the table on the following page.

PCI DSS REQUIREMENT	KEY POINTS
Requirement 3: Protect stored cardholder data.	Keep cardholder data storage to a minimum. Develop a data retention and disposal policy. Ensure that customer information is stored as encrypted data using strong cryptography protocols.
Requirement 4: Encrypt transmission of cardholder data across open, public networks.	Use strong encryption protocols such as Secure Socket Layer and Transport Layer Security (SSL/TLS) or Internet Protocol Security (IPSEC) to provide secure transmission of data over the network. Never send payment card information over an unexpected medium such as chat, SMS/text or email.
Requirement 7: Restrict access to cardholder data by business need-to-know.	Limit access to system components and cardholder data to only those individuals whose job requires such access.
Requirement 8: Assign a unique ID to each person with computer access.	Assigning a unique identification (ID) to each person with access ensures that each individual is uniquely accountable for his or her actions.

OAISYS CALL RECORDING SOLUTIONS & PCI DSS

OAISYS call recording technology meets the exacting requirements of PCI DSS in a number of uniquely effective ways.

1. OAISYS utilizes patent-pending Portable Voice Document (PVD™) technology that securely captures a single media file encompassing all available audio, video, and text data.

2. OAISYS PVD technology delivers media files using encrypted streaming, ensuring IT retains total control over the data.

3. OAISYS user authentication and permissions controls are remarkably granular, which allows provisioning of the minimum access level required to accomplish a user's task.

More detailed explanations of some specific OAISYS features that can support an organization's PCI DSS compliance efforts are listed below.

Permissions-based User Access: Only authorized users can access data, ensuring call recordings are handled properly and in accordance with company and regulatory guidelines. Permissions can be restricted based on user type, or any one or more of the following criteria; outside phone number, call duration, extension, ACD (Automatic Call Distribution) information such as agent or ACD Group ID, account number, or user entered information, and many others.

Blackouts: The PCI DSS require that card security codes (CID, CAV2, CVC2, and CVV2) are not stored. It is a violation of PCI DSS requirement 3.2 to store any sensitive authentication data, including card validation codes and values, after authorization even if encrypted. OAISYS can easily address this requirement via a variety of different methods.

- Agent-initiated manual trigger within the included OAISYS Recording Client that simply adds start and stop points surrounding the targeted data. This requires manual intervention, but allows for flexible start/stop of recording.

- OAISYS Desktop Client Application Programming Interface (API) utilizes a COM (ActiveX) interface to accept client-to-client commands to automatically start/stop recording. Start/stop functionality can be engaged by placement of the cursor in the appropriate field on the client application.

  For example: When the mouse hovers over a credit card number field, call recording can be configured to stop recording. When the Enter key is engaged or the mouse moves away from the field, recording can begin again.

- OAISYS has developed a plug-in utilizing Internet Explorer 7 and the Desktop Client which can automatically start/stop recording based on the position of the cursor in the browser window. This works for ANY website, not just client controlled addresses.

- OAISYS Desktop Port API utilizes server-to-server commands to automatically start/stop recording. This typically applies to systems like predictive dialers that have their own client access software, and provides essentially the same functionality as the OAISYS Desktop Client API, but for different types of applications.

Call Segment Sharing: OAISYS PVD technology provides for selective sharing of specific call segments, ensuring recipients can only listen to the sections they were meant to hear. Sharing permissions limit the length of time a recipient will have access to a recording, or if it can be shared further.

Automated and Secure Recording Management/Archival: Call recordings can be automatically purged based on their age, ensuring compliance with a useful life retention policy. Automated archival capabilities make it possible to transfer recordings from the system to any network storage device, including one with hardware encryption. OAISYS PVD technology also provides an additional layer of security; if a NAS or SAN where recordings are stored were ever accessed without proper authorization, the recordings could not be played back without the OAISYS client software.

Encryption: OAISYS solutions use RSA 1024-bit asymmetric encryption to set up authentication at the start of a session then uses RC2 40-bit symmetric encryption for all

subsequent communication in the session (audio and associated metadata). Enhanced playback encryption can be obtained by setting up the network firewall utilizing IP Security (IPSEC) and Triple Data Encryption Standard (TDES or 3DES). In addition, it is possible to obtain strong encryption for the database, defined by the PCI DSS as 128-bit and higher for Advanced Encryption Standard (AES), by utilizing the Microsoft Windows Encrypting File System on the OAISYS Recording System.

User Security and Audits: The OAISYS solution provides an administrative interface that delivers activity tracking functionality via log files showing the date, time, and user name associated with the access of any call recording.

Digital Watermarking: OAISYS includes a digital watermark on every call recording. This digital watermark ensures a recording has not been altered in any way. If a recording were ever to be used in a court of law, it could be proven that the call recording did NOT include sensitive information at the time of capture.