What PCI – DSS Really Means for your Contact Center

September 2014

Sponsored By:

cognia

Table of Contents

Executive Summary

There have been lots of discussions and debates about the Payment Card Industry – Data Security Standard (PCI-DSS), due to the lack of clarity regarding these requirements, particularly for call and contact centers who are actively engaged in many credit/debit card payments. PCI-DSS came about when the top 5 credit/debit card brands decided to align their fraud prevention guidelines to benefit their issuers and processors around the world. In 2004, they released their first set of guidelines, which resulted in so much confusion that an entire industry and ecosystem developed to help companies comply with these regulations.

This white paper is intended to help call center and contact center managers understand the impact of PCI-DSS on their agents and their ability to record and store these transactions. And for organizations that must comply with these regulations, this paper gives insights into methods for maintaining adherence. DMG Consulting recommends that all affected organizations involve their legal and auditing teams in the PCI-DSS compliance process, even though it is not federal or state law (although a few state laws do reference these guidelines).

What is PCI-DSS?

The Payment Card Industry Data Security Standard was developed through the combined efforts of 5 of the largest payment card brands: American Express, Discover Financial Services, JCB International, MasterCard and Visa Inc. The goal of this standard is to reduce credit/debit card fraud. These 5 companies are known as the Payment Card Industry Security Standards Council (PCI SSC); they consider themselves a “global open global forum that is responsible for the development, management, education, and awareness of the PCI-DSS and other standards that increase payment data security.” (Source: www.pcisecuritystandards.org/pdfs/13_11_06_DSS_PCI_DSS_Version_3_0_Press_Release.pdf.)

PCI-DSS was created to provide guidance to merchants and payment card processors (all organizations that process, store or transmit cardholder information) about securing personal customer data located on cards and on the cards’ magnetic strip. Any company accepting or processing American Express, Discover Financial Services, JCB International, MasterCard and Visa Inc. brand credit and debit cards must be PCI-DSS compliant. (This does not mean that all companies that process credit/debit payments must follow these guidelines; the volume of activity is an important criterion.) Version 1.0 of PCI-DSS was released on December 15, 2004. The PCI SSC has issued a number of releases and clarifications to the original standard to help members understand it in order to comply. In October 2010, version 2.0 was released and will be active from

January 1, 2011 through December 31, 2014. In November 2013, version 3.0 was released and will be active from January 2, 2014 through December 31, 2016. The timing of these standards overlaps to give the approximately 650 participating organizations time to review and comply. See Appendix A for the complete list of the 12 high-level PCI-DSS requirements.

The Challenge of PCI-DSS for Call Centers/Contact Centers

The PCI SSC's objective in establishing the security-related guidelines is to help companies involved with credit/debit/payment cards reduce fraud. The concept is outstanding, but the roll-out of these guidelines has been greatly challenged by the lack of clarity. To address the shortcomings of the regulations, the PCI SSC has issued a number of frequently asked questions (FAQs). FAQ 5362, dated February 18, 2010, specifically addresses the question: "Are audio/voice recordings containing cardholder data and/or sensitive authentication data included in the scope of PCI-DSS?" The response to this question is directed at "call centers that record cardholder data in audio recording, and applies only to the stored card validation codes and values (referred to as CAV2, CVC2, CVV2 or CID codes by the payment brands)." The answer continues that "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. It is therefore prohibited to use any form of digital audio recording (using formats such as wav, mp3, etc.) for storing CAV2, CVC2, CVV2 or CID codes after authorization if the data can be queried; recognizing that multiple tools exist that potentially could query a variety of digital recordings. Where technology exists to prevent recording of these data elements, such technology should be enabled. If these recordings cannot be data mined, storage of CAV2, CVC2, CVV2 or CID codes after authorization may be permissible as long as appropriate validation has been performed. This includes the physical and logical protections defined in PDI-DSS that must still be applied to these call recording formats. This requirement does not supersede local or regional laws that may govern the retention of audio recordings."

This important FAQ is an excellent example of the challenges surrounding the application of PCI-DSS. Even documents issued to clarify the meaning and intent of the regulations are confusing. It's obvious that the PCI SSC has made a great effort to limit its legal exposure and to avoid conflict with local, state and federal laws.

Implications of PCI-DSS for Call Centers/Contact Centers

While all 12 of the high-level requirements in Appendix A may have some relevancy to call centers/contact centers and their systems, the most significant requirements are:

- *Requirement 3:* Protect stored cardholder data
- *Requirement 4:* Encrypt transmission of cardholder data across open, public networks
- *Requirement 12:* Maintain a policy that addresses information security

In addition, many of the sub-requirements also appear to apply to call centers/contact centers. This includes Requirement 3, which obliges businesses that store payment card data to ensure their storage solution is highly secure. Companies need to:

- Store payment card data only when absolutely necessary, and have a disposal procedure in place
- Display only as much of the card number as necessary, such as the last four digits of the number for verification purposes
- Ensure that customer information is stored as encrypted data using strong cryptography protocols
- Allow access to the personal identification number and the CVV within the record only on a need-to-know basis, and prevent users from being able to search for the code by encrypting it

Requirement 4 targets the transmission of payment card data across networks. It requires companies to:

- 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 unencrypted medium such as chat, SMS/text or email

Requirement 12 targets how PCI-DSS is communicated and monitored. It requires companies to:

- Establish, publish, maintain and disseminate a security policy that:
  - Addresses all PCI-DSS requirements
  - Includes an annual process that identifies threats and vulnerabilities and results in a formal risk assessment
  - Includes annual reviews and updates when the environment changes
- Develop daily operational security procedures that are consistent with PCI-DSS requirements
- Develop usage policies for critical employee-facing technology to define proper use of these technologies for all employees and contractors
- Ensure the information security policies and procedures clearly define the responsibilities of all employees and contractors
- Assign specific security responsibilities to an individual or team
- Implement a formal security awareness program so that all employees are conscious of the importance of payment card security
- Screen potential employees prior to hiring, to minimize the risk of attacks from internal sources

Methods for Adhering to PCI-DSS

Call and data recording solutions, customer relationship management (CRM)/ customer tracking solutions, Voice over Internet Protocol (VoIP) phone systems (automatic call distributors (ACDs) and dialers) must be “hardened” to allow their users to comply with PCI – DSS standards. Contact center solution vendors, such as workforce optimization providers, must ensure that their solutions provide appropriate security protocols and operate within a secure network.

There are many approaches and applications to help companies that process credit/debit/payment cards be compliant. The solutions vary with regard to the level of automation used to protect each caller’s sensitive data. Some of the vendors utilize speech, text and desktop analytics to facilitate the automated triggering of pause/resume controls to the voice and screen recorder. Another common option is to use secure payment processing via interactive voice response (IVR). Still another approach is to introduce tones to mask customer

entry of sensitive payment card data on their keypads, so that it cannot be heard by agents. Other important features to help organizations comply with PCI-DSS requirements include end-to-end encryption (from time of capture), full audit trail, watermarking and password management.

The full extent of the work required for an organization to be PCI – DSS compliant can be time consuming and costly, impacting people, processes and systems. As importantly, maintaining compliance is an ongoing effort; call/contact centers must undergo an annual audit to prove their adherence, which is an expensive proposition for many companies. Figure A lists the different approaches that companies are using to enable them to adhere to PCI-DSS, and also reviews their pros and cons. Please keep in mind that companies may need to use a number of these methods to be fully compliant.

Figure A: Approaches to PCI-DSS Compliance

Capability	Description	Pros	Cons
Pause/Resume (Manual)	A manual pause/resume capability is provided for agents. When a customer starts to share sensitive data, the agent manually presses a button (hardware or software-based) that pauses the recording. The agent presses it a second time to resume recording.	• Prevents sensitive data from being recorded	• Dependent on the agent to manually pause and resume the call • This approach may negatively impact the customer experience
Pause/Resume (Automated)	An API is used to integrate the recording solution with the CRM/servicing application. When an agent accesses a sensitive field in the servicing application, such as the location or the credit card number or security code, the recording is automatically paused. Recording	• Prevents sensitive data from being recorded • Fully automates the process, eliminating the potential of human error (e.g., agents pushing the delay button too slowly) • Is transparent to	• IT resources from either the vendor, enterprise or both may be required to implement and maintain this solution • A customer can start sharing their sensitive data before the automated trigger for pause

Figure A: Approaches to PCI-DSS Compliance			
Capability	**Description**	**Pros**	**Cons**
	automatically resumes when the agent moves away from these fields.	the customer	begins
DTMF Suppression (Manual/Automated)	The company's sales system is integrated via an API to a third-party cloud-based payment processing interface (screen). Customers use their touch-tone keypad to input their sensitive payment card data. The dual-tone multi-frequency (DTMF) tones are automatically masked so that the agent cannot hear them and they are not recorded. The conversation between the agent and customer continues without disruption throughout this process.	• Prevents sensitive data from being recorded or heard by agents • Provides a seamless customer experience	• Dependent on the agent to access the third-party interface
Desktop Analytics-Enabled (Automated)	Desktop analytics (DA) is used to automate the process of pausing and resuming the recording.	• Prevents sensitive data from being recorded • Fully automates the process • Is transparent to the customer • Does not require code-level changes	• Requires the purchase of a DA application • Requires resources who know how to implement the DA solution
Real-Time Speech Analytics-Enabled	Speech analytics is used to identify	• Fully automated	• Requires a real-time speech

Figure A: Approaches to PCI-DSS Compliance			
Capability	**Description**	**Pros**	**Cons**
(Automated)	sensitive information in real time, as it is being spoken. The application automatically pauses the recording when it "hears" certain words, and resumes it after a pre-defined delay or when other words are spoken.	process • Is transparent to the customer • Eliminates risk of capturing and storing sensitive customer information	analytics application and resources to implement/ manage the system
IVR Secure Payment Processing (Manual/Automated)	An IVR is used to capture the credit card information. (When the time comes for the customer to make a payment, the agent transfers the customer into the IVR so that only the IVR "hears" or "sees" the credit card information.)	• Secures the credit card payment process	• Requires a special IVR application • Could have a negative impact on the customer experience, as the customer has to be transferred and then retrieved from the IVR • Could lengthen the average handle time of calls

Source: DMG Consulting LLC, September 2014

Cloud vs. Premise PCI-DSS Solutions

In the last few years, the call/contact center market has been revolutionized by the introduction of a new generation of cloud-based solutions. These solutions are changing the way that private and public organizations acquire and implement mission-critical call/contact center applications, freeing them from making large up-front capital expenditures and the need to continuously invest in maintenance and upgrades. However, when it comes to PCI-DSS, there is another important benefit from using a cloud-based vendor: the responsibility of keeping up-to-date on the regulations also falls on the software provider. This "soft" benefit is one that should be seriously considered by any company in need of a solution to enable PCI-DSS compliance.

Final Thoughts

Fraud is a very serious issue for the credit and debit card industry. According to a 2010 study by LexisNexis on credit card losses, the cost of credit card fraud was in excess of $100 billion for retailers, and this was long before the major scams of 2013. PCI-DSS is a wonderful initiative introduced by the top 5 payment card companies to cooperate and work together to reduce fraud losses. (While credit card companies absorb most of these losses, consumers pay the price in increased annual percentage rates.)

Any company – retail, financial services, insurance, travel, etc. – that is involved in processing a large volume of credit and debit card payments needs to comply with the PCI-DSS regulations or face serious fines. The risk of internal and external fraud can be mitigated and regulatory compliance achieved by using a PCI-DSS compliant solution that prevents the capture of sensitive credit/debit card data. These solutions, which are available on-premise or in the cloud, are mission-critical and an excellent investment when they are properly implemented and monitored.

Appendix: PCI-DSS High-Level Requirements

PCI-DSS is comprised of 12 broad requirements that set a baseline against which to measure and grade a company's data security practices. It also provides a mechanism for members of the payment card industry to self-regulate and self-police. The PCI-DSS does not dictate how a company must provide security. The PCI-DSS requirements are:

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

These requirements have not changed since they were issued, but with each subsequent release of the guidelines, they are enhanced and supported by sub-requirements. Companies are encouraged to review the new requirements on an ongoing basis to ensure they are in compliance. Detailed information about the standards is available at www.pcisecuritystandards.org.

About Cognia

Cognia is a leader in the provision of cloud-based communications intelligence solutions for enterprises and service providers. A single global cloud platform provides secure solutions for multi-channel recording, PCI compliant payment processing and analytics for communications including fixed-line and mobile, as well as all IP communications.

Cognia have achieved the world's first QSA-validated, PCI DSS Level 1 service on a secure global cloud platform. The solutions delivered by Cognia replaces the high upfront capital and support costs of on-premise systems, with the flexibility to lower TCO to a level never before possible with traditional solutions.

Cognia's solutions are used world-wide by a 100 financial institutions, contact centres and services providers including Vodafone. Cognia has over 28 million media assets under management in its cloud.

For more information please go to www.cognia.com.

About DMG Consulting LLC

DMG Consulting LLC is a leading independent research, advisory and consulting firm specializing in contact centers, back-office and real-time analytics. DMG provides insight and strategic guidance and tactical advice to end users, vendors and the financial community. Each year, DMG devotes more than 10,000 hours to producing primary research on IT sectors, including workforce optimization (quality management/liability recording), speech analytics, workforce management, performance management, desktop analytics, surveying/voice of the customer, text analytics, cloud-based contact center infrastructure, dialing, interactive voice response systems and proactive customer care. Our actionable solutions are proven to deliver a lasting competitive advantage, and often pay for themselves in as little as three months. Learn more at www.dmgconsult.com.

DMG Consulting, LLC
6 Crestwood Drive
West Orange, NJ 07052

973.325.2954
www.dmgconsult.com
info@dmgconsult.com

DMG
CONSULTING LLC