PCI Security Standards Council™

Standard: PCI Data Security Standard (PCI DSS)
Version: 2.0
Date: March 2011

Information Supplement:

Protecting Telephone-based Payment Card Data

Table of Contents

Executive Summary

The following information and guidance is intended to provide payment security advice for merchants and service providers who accept and/or process payment card data over the telephone. This information highlights the key areas organizations with call-center operations need to address in order to process payment cards securely, and how best to protect their business and their customers from the risks of data compromise and fraud.

The intent of this document is to provide supplemental guidance, and the information provided here does not replace or supersede PCI DSS requirements. The PCI Security Standards Council (PCI SSC) is not responsible for enforcing compliance or determining whether a particular implementation is compliant. Merchants and service providers should work with their acquirers or payment card brands, as applicable, to understand their compliance validation and reporting responsibilities.

Why Telephone Card Payment Security is Important

In face-to-face and e-commerce environments, risk-mitigating technologies have helped significantly reduce fraud rates, resulting in a shift of card fraud towards the Mail Order / Telephone Order (MOTO) space.

Additionally, a number of regulatory bodies are requiring some companies to record and store telephone conversations in a range of situations. The Payment Card Industry Data Security Standard (PCI DSS), however, stipulates that the three-digit or four-digit card verification code or value printed on the card (CVV2, CVC2, CID, or CAV2) cannot be retained after authorization, and full primary account numbers (PANs) cannot be kept without further protection measures.

As such, there is a risk that organizations taking customer payment card details over the telephone may be recording the full cardholder details to comply with various regulatory bodies, thereby causing them to be in contravention of PCI DSS requirements and potentially exposing cardholder data to unnecessary risk.

Note that PCI DSS does not supersede local or regional laws, government regulations, or other legislative requirements.

Clarification of the PCI DSS Guidelines for Voice Recordings

The impact of PCI DSS has been far-reaching, and its goal to minimize payment card data loss (malicious or otherwise) from merchant and service provider environments is becoming a reality.

For all merchants and service providers, this requires appropriate measures to protect any systems that store, process and/or transmit cardholder data. This impacts call-recording management and storage, and control of the agent/caller interface within the physical call-center space. The PCI SSC produced this Information Supplement to clarify the PCI DSS requirements on voice recordings, to provide some best practices, and to promote consistency among merchants, service providers and the assessor community.

Recap: The PCI SSC FAQ

PCI SSC FAQ 5362 – **Are audio/voice recordings containing cardholder data and/or sensitive authentication data included in the scope of PCI DSS?**

This response is intended to provide clarification for call centers that record cardholder data in audio recordings, and applies only to the storage of card validation codes and values (referred to as CAV2, CVC2, CVV2 or CID codes by the payment brands).

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 that 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 PCI 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.

PCI DSS Requirements for Stored Cardholder Data

In general, no cardholder data should ever be stored unless it is necessary to meet the needs of the business. Sensitive data on the chip or magnetic stripe must never be stored after authorization. If an organization stores the primary account number (PAN), it is crucial to render it unreadable (see PCI DSS Requirement 3.4). Organizations also must comply with Requirements 3.1 through 3.6 of the PCI DSS with respect to protection of stored data.

It is important to understand the various elements that are classified as cardholder data, and especially what constitutes sensitive authentication data.

The following table gives a summary of the PCI DSS guidelines for cardholder data elements:

		Data Element	Storage Permitted	Render Stored Account Data Unreadable per Requirement 3.4
Account Data	**Cardholder Data**	Primary Account Number (PAN)	Yes	Yes
		Cardholder Name	Yes	No
		Service Code	Yes	No
		Expiration Date	Yes	No
	Sensitive Authentication Data[*]	Full Magnetic Stripe Data[†]	No	Cannot store per Requirement 3.2
		CAV2/CVC2/CVV2/ CID	No	Cannot store per Requirement 3.2
		PIN/PIN Block	No	Cannot store per Requirement 3.2

What this means: Essentially, sensitive authentication data must not be retained after authorization (Requirement 3.2); and for telephone operations, “sensitive authentication data” means the CAV2/CVC2/CVV2/CID and/or PIN values that may be taken during a telephone call.

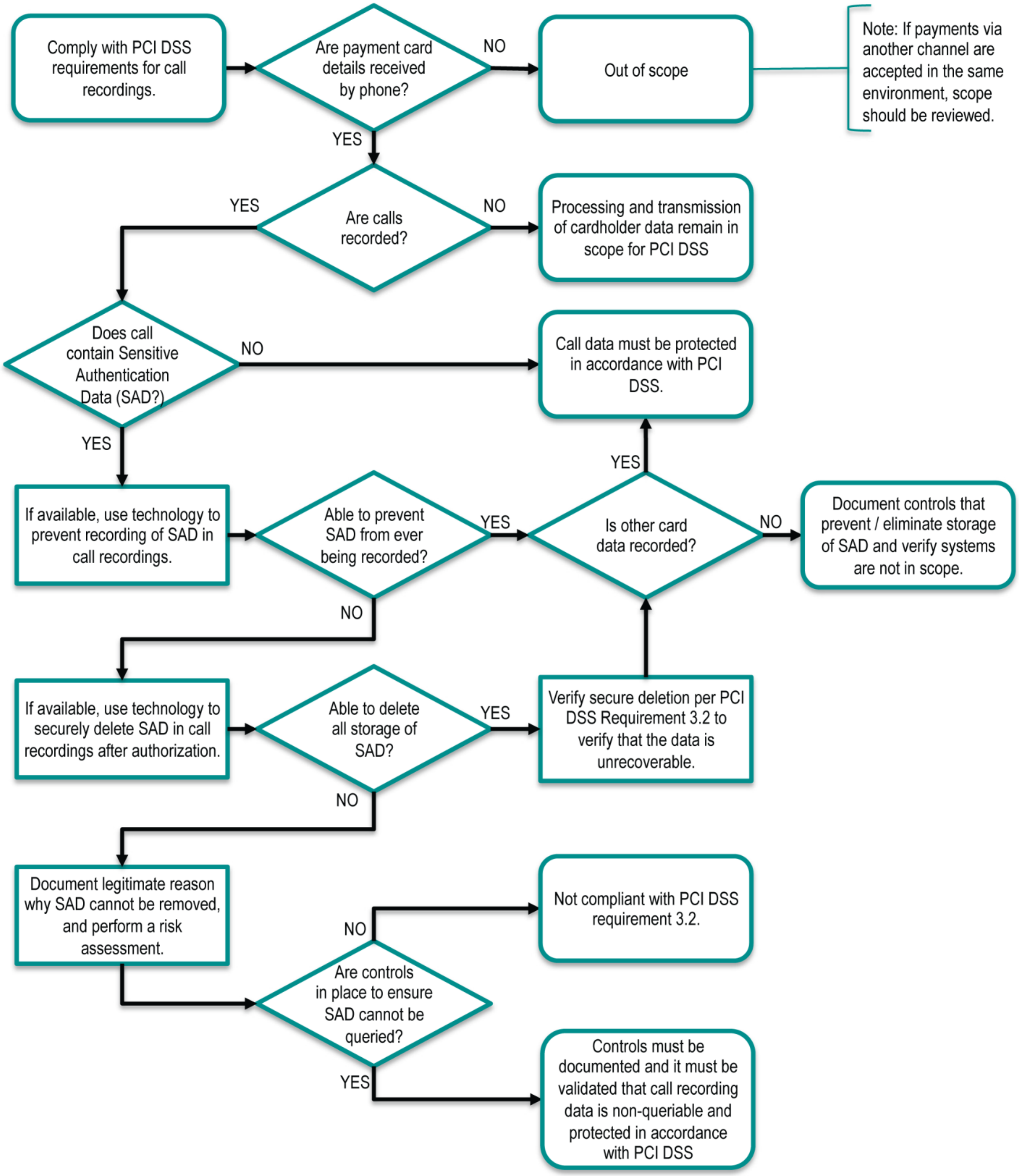
Where to Start

The following page shows the process a merchant should follow when assessing the risk for their call center operations and aims to further clarify the FAQ above.

[*] *Sensitive authentication data must not be stored after authorization (even if encrypted).*

[†] *Full track data from the magnetic stripe, equivalent data on the chip, or elsewhere.*

Decision Process for Voice Recordings


Comply with PCI DSS requirements for call recordings.
Are payment card details received by phone?
NO
Out of scope
Note: If payments via another channel are accepted in the same environment, scope should be reviewed.
YES
Are calls recorded?
NO
Processing and transmission of cardholder data remain in scope for PCI DSS
YES
Does call contain Sensitive Authentication Data (SAD?)
NO
Call data must be protected in accordance with PCI DSS.
YES
If available, use technology to prevent recording of SAD in call recordings.
Able to prevent SAD from ever being recorded?
YES
YES
Is other card data recorded?
NO
Document controls that prevent / eliminate storage of SAD and verify systems are not in scope.
NO
If available, use technology to securely delete SAD in call recordings after authorization.
Able to delete all storage of SAD?
YES
Verify secure deletion per PCI DSS Requirement 3.2 to verify that the data is unrecoverable.
NO
Document legitimate reason why SAD cannot be removed, and perform a risk assessment.
NO
Not compliant with PCI DSS requirement 3.2.
Are controls in place to ensure SAD cannot be queried?
YES
Controls must be documented and it must be validated that call recording data is non-queriable and protected in accordance with PCI DSS

* Flowchart Notes: Are controls in place to ensure Sensitive Authentication Data cannot be queried?

Sensitive Authentication Data must be secured in a manner consistent with PCI DSS and must not be able to be queried. Data that is queriable may be retrieved through use of a search tool or by issuing a system instruction/task or a set of instructions/tasks. Examples of instructions/tasks that could result in data being retrieved include but are not limited to –

- Defined searches based on character sets or data format
- Database query functions
- Decryption mechanisms
- Sniffer tools
- Data mining functions
- Data analysis tools
- Built-in utilities for sorting, collating or retrieving data

Note: *Encrypting sensitive authentication data is not by itself sufficient to render the data non-queriable.*

For data to be considered "non-queriable" it must not be feasible for general users of the system or malicious users that gain access to the system to retrieve or access the data. Access to the types of functions listed above must be extremely limited, explicitly authorized, documented, and actively monitored. Additionally, controls must be in place to prevent unauthorized access to these functions.

Other methods that may help to render SAD non-queriable include but are not limited to:

a. Removing call recordings from the call recording solution
b. Taking the call recordings offline
c. Vaulting the call recordings
d. Enforcing dual access controls to the vaulted call recordings
e. Allowing only single call recordings to be retrieved from vaults

Before considering this option, every possible effort must first be made to eliminate sensitive authentication data. There must be a documented, legitimate reason why sensitive authentication data cannot be eliminated (for example, a legislative or regulatory obligation), and a comprehensive risk assessment performed at least annually. The detailed justification and risk assessment results must be made available to the acquiring bank and/or payment card brand as applicable.

This option is a last resort only, and the desired outcome is always the elimination of all sensitive authentication data after authorization. If technologies are available to fulfil PCI DSS requirements without contravening government laws and regulations, these technologies should be used.

Hints and Tips for Call Centers

Call centers will need to ensure that an appropriate retention policy is implemented and maintained.

This is part of PCI DSS Requirements 3.1 and 3.2 and includes:

- Ensuring that payment card data is stored only when absolutely necessary, and that a disposal procedure is in place.
- Limiting the amount of time that card information is kept on the quality assurance (QA)/recording server and customer relationship management (CRM) solution databases (both voice and screen recordings); it may be necessary for corporate governance, legal and QA departments to work out a compromise between what is needed to adhere to the PCI DSS and regulatory compliance requirements. However, note that PCI DSS does not supersede local or regional laws, government regulations, or other legislative requirements.
- Never allowing for the card validation code (referred to as CAV2, CVC2, CVV2, or CID) to be stored in a digital audio or video format (e.g., WAV, MP3, MPG, etc.). If the QA/recording solution cannot block the audio or video from being stored, the code must be deleted from the recording after it is stored. If a call-center manager feels that there may be difficulty with achieving this, they must discuss this with their acquiring bank.

Call centers will need to ensure that the PAN is masked when displayed (no more than the first six and last four digits should be displayed).

This is part of PCI DSS Requirement 3.3 and includes:

- Allowing access to the full PAN only on a need-to-know basis.
- Segmenting call-center operations so that the minimum required number of agents have access to payment card data; for example, payment card information can be entered by a sales agent, but a customer service representative may have access only to the masked PAN.
- Considering solutions where the agent does not have to enter card information into the system.
- If the above is not possible, requiring agents to enter payment card information as it is given to them and then mask the information once they verify its accuracy. This may mean sourcing agent desktop applications that can mask card information once it has been entered and verified.

Call centers will need to ensure that PAN data is rendered unreadable (for example, encrypted using strong cryptography) when stored.

This is part of PCI DSS Requirement 3.4 and includes ensuring PANs stored within the QA/recording and CRM solutions are encrypted using strong cryptography, or are otherwise rendered unreadable.

Call centers will need to ensure that transmission of cardholder data across public networks is encrypted.

This is part of PCI DSS Requirement 4 and includes:

- Using strong encryption protocols such as Secure Socket Layer and Transport Layer Security (SSL/TLS), Secure Shell (SSH), or Internet Protocol Security (IPsec) to secure transmission of any cardholder data over public networks, including:
  - Both wired and wireless networks used by at-home/remote agents and supervisors. For example, via a Virtual Private Network (VPN) with SSL/TLS. Please note that Wired Equivalent Privacy (WEP) protocol is no longer permissible as a security control for wireless networks.
  - Any public network segments used to carry or send screen or voice recordings.
  - Voice or data streams over Voice over IP (VoIP) telephone systems, whenever sent over an open or public network. Note that only those consumer or enterprise VoIP systems that provide strong cryptography should be used.
- Requiring agents to use analog telephone lines when a VoIP telephone system does not provide strong cryptography,
- Ensuring that payment card information is never sent over an unencrypted, end-user messaging medium such as chat, SMS (Simple Messaging System)/text or e-mail, or other non-encrypted communication channels.
- As a *best practice*, ensuring that stored recordings are not played back over a speakerphone if payment card information is included.

Call centers will need to ensure that proper user authentication is implemented for staff, agents, and administrators.

This is part of PCI DSS Requirements 7 and 8 and includes:

- Restricting access to QA/recording and CRM data containing payment card data based on the user's log-in account and corporate role; for example, providing screen recording play-back interfaces where the payment card information is displayed only to managers and compliance officers during legal discovery, and having it blacked out (masked) for all other supervisors and QA specialists
- Segmenting call-center operations so that the minimum required number of agents have access to payment card data; for example, payment card information can be entered by a sales agent, but a customer service representative may have access only to the masked PAN.
- Ensuring at-home/remote agents and supervisors use a two-factor authentication process.
- Ensuring that agents and supervisors do not share user IDs and passwords.

Call centers will need to ensure that they adhere to an information security policy.

This includes:

- Developing daily operational security procedures that are consistent with all PCI DSS requirements and clearly defining the responsibilities of all personnel.
- Developing usage policies for critical technologies to define proper use of these technologies for all personnel.
- Assigning an individual or team specific security responsibilities.
- Implementing a formal security awareness program so that all personnel are conscious of the importance of payment card security, and to make sure that all personnel are properly trained and knowledgeable about all security policies and procedures.
- Annually reviewing all security policies and procedures with all in-house and at-home/remote agents. As a *best practice*, require agents to acknowledge the security requirements as part of their daily sign-in process
- Screening of potential employees prior to hiring. In addition, as a *best practice*, monitoring of both at-home/remote agents and in-house agents. These practices help minimize the risk of attacks from internal sources. In any instance, call-center managers should ensure that controls are implemented to monitor policy compliance for on-site, remote and at-home users.
- Ensuring that at-home/remote agents are prohibited from unauthorized copying, moving, and storing of cardholder data onto local hard drives and removable electronic media when accessing cardholder data via remote-access technologies.

Call centers will need to ensure that any media used to record the information must be clearly labeled, inventoried and rendered unreadable following PCI DSS requirements.

- Pay particular attention to sensitive authentication data: **Storage is not permitted.**
- Physical and logical access to the media as well as logical access to the product used to record the calls should be restricted.
- All interaction with the recordings should be logged.
- Storage and backup/archiving of the recording solution must not become a backdoor to the solution.
- A destruction policy should be put in place such that recordings are not kept any longer than necessary.
- It is advisable to find a call-recording product allowing you to track logical and physical access to media containing data. It should also provide encryption features, strong authentication and detailed reporting and logging.

Finally, call centers will need to ensure that all PCI DSS requirements are implemented.

This includes:

- Strong authentication controls for all personnel with access to call recordings.
- Ensuring there are no direct connections between systems storing audio recordings and the Internet.
- Ensuring that systems are maintained to secure configuration standards and are regularly tested for vulnerabilities.
- Ensuring that at-home/remote agent and supervisor PCs have personal firewalls installed and operational.
- Ensure that at-home/remote agents and supervisor PCs have the latest version of the corporate virus protection software and definition files
- Ensure that at-home/remote agent and supervisor PCs have the latest approved security patches installed.
- Requiring agents and supervisors to use only company-approved systems.

What to Ask Your Call-Center Provider

How does the call-center system help my company comply with the PCI DSS requirements, and how does it automatically remove sensitive credit card information from recorded calls?

If you take credit card details over the phone, ask your supplier to prove that they are "PCI DSS compliant" and to explain how they remove sensitive authentication data from their recordings, automatically (with no manual intervention by your staff).

How will the call-center system comply with any future changes in legal regulations or codes of practice?

It is important that any call-recording system purchased now can adapt to future changes in the law, regulations and industry best practices. Organizations need to ensure that their recording system is as future-proof as it can be. Suppliers must be able to prove that regardless of any constraints or changes the government or other regulatory body may require for call recording solutions, their system is flexible enough to adapt.

About the PCI Security Standards Council

The mission of the PCI Security Standards Council is to enhance payment account security by driving education and awareness of the PCI Data Security Standard and other standards that increase payment data security.

The PCI Security Standards Council was formed by the major payment card brands American Express, Discover Financial Services, JCB International, MasterCard Worldwide, and Visa Inc. to provide a transparent forum in which all stakeholders can provide input into the ongoing development, enhancement, and dissemination of the PCI Data Security Standard (DSS), PIN Transaction Security (PTS) Requirements, and the Payment Application Data Security Standard (PA-DSS). Merchants, banks, processors, and point-of-sale vendors are encouraged to join as Participating Organizations.

ACKNOWLEDGEMENT

This Information Supplement contains material from a resource developed by PCI SSC Board of Advisor member Barclaycard. The Council thanks Barclaycard for making this content available to share with the wider PCI community.