# Guidance Notes

## PCI DSS Compliance as it relates to Call Recording

Published by
DMA Contact Centres & Telemarketing Council
First edition

# Contents

# Disclaimer

These notes have been compiled by the DMA's Contact Centre & Telemarketing Council to provide some guidance to operators of contact centres in the area of managing call recording compliance with the Payment Cards Industry Data Security Council (PCI) Data Security Standards (DSS) – they do not address any other area of compliance, with either the PCI DSS regulations or any other regulatory body (Financial Services Authority (FSA), Information Commissioner's Office (ICO) and others). They should be used as background guidance only and any queries should be addressed to the PCI or to a Qualified Security Assessor (QSA).

It should also be noted that for an outsourced contact centre, the requirement to PCI DSS compliance is the responsibility of the client, who would under normal circumstances be the company having the initial agreement with the payment card issuer. This would mean that unless there is a flow down within the supplier contract, PCI DSS compliance should be considered Best Practice and not a legal requirement. However, it would be best practice for outsourced contact centres to be able to advise their clients on the implications of the use of contact centre technology on PCI DSS compliance.

The DMA would like to thank Rufus Grig and the Contact Centres & Telemarketing Council for their contribution to this document.



# 1. Background

The Payment Cards Industry Data Security Council (commonly referred to as the PCI) is a body representing the major payment card (credit card, debit card etc) issuers set up to develop and promote security standards for account data protection. It produced the Data Security Standard (DSS) to assist merchants with protecting cardholder and accountholder information.

Achieving compliance with the PCI DSS has been a key business objective for many organisations and involves all aspects of data security including (but not limited to) data networks, web servers, database servers, line-of-business applications, card processing equipment, file servers, remote access systems and the management of which individuals have access to which systems. Achieving PCI DSS for most organisations requires considerable effort, but the principles of data security that it imposes are recognised by many organisations to be a positive benefit in the long term.

One area that has caused considerable confusion is the issue of the storage of cardholder information in call recording systems, commonly in place in contact centres for the purposes of compliance, quality and training purposes. This document outlines some of the requirements of the PCI DSS in relation to the storage of cardholder information in call recording systems and some potential solutions for contact centre operators.

It should be noted that PCI DSS impacts the contact centre in more areas than the call recording. For example, if IP Telephony is in use, then cardholder data is passed on the data network as data packs. Interactive Voice Response or Self-Service systems that process payment transactions handle and may store cardholder data, and scripting systems and the applications used in the contact centre to process payments will also be within the scope of the standard. This document does not address these areas.

# 2. The fundamental storage issues with cardholder data

The following table, reproduced from the PCI Data Security Standard, shows what cardholder data must be protected and must / must not be stored.

| | Data Element | Storage Permitted | Protection Required | PCI DSS Req. 3.4 |
|---|---|---|---|---|
| **Cardholder Data** | Primary Account Number (PAN) | Yes | Yes | Yes |
| | Cardholder Name [1] | Yes | Yes [1] | No |
| | Service Code [1] | Yes | Yes [1] | No |
| | Expiration Date [1] | Yes | Yes [1] | No |
| **Sensitive Authentication Data [2]** | Full Magnetic Stripe Data [3] | No | N/A | N/A |
| | CAV2/CVC2/CVV2/CID | No | N/A | N/A |
| | PIN/PIN Block | No | N/A | N/A |

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

As can be seen from the table, there are a number of different fields or parameters that have different rules depending on whether the data can be stored, and if so, is it a requirement that the data be protected.

A simple reading of the protection rules within the standard would lead to the following conclusions being drawn:

- That the call recording falls into the PCI DSS standard because it is digitally storing cardholder details, albeit not in a form that is easily machine readable
- That the PAN, cardholder name, service code and expiration date can all be stored, but that protection is required. In practice this protection includes controlling who can access the call recordings after they have been made which may also include encrypting the call recording to prevent unauthorised access
- That the CAV2/CVC2/VV2/CID (the code from the back of the code, sometimes referred to as the security code) must not be stored, even if the call recording is protected.

Manufacturers of call recording equipment have, for some time, had encryption and access control available and it would appear from a cursory reading of this standard that this encryption should be implemented if the call recording is going to include cardholder details. However, there is more than one type of encryption and the PCI DSS stipulate in much more detail the requirements of this encryption and access protection. Contact centre operators should check with their call recording vendors and their QSA that the encryption and access control provided is PCI DSS compliant.

# 3. The CVC2 or security code

Where the most controversy and confusion has arisen is in the storage of the CVC2 number in call recordings. Upon initial reading of the specification it would appear clear that this information cannot be stored in a call recording. This has been the subject of much debate with different QSAs and call recording vendors making different interpretations – with one of the common contentious issues being whether it would be sufficient to encrypt a recording containing the CVC2 number in order to obtain compliance.

The PCI has itself issued different advice at different times on this subject, but the most recent advice in the form of a "Frequently Asked Question" (FAQ) Are audio/voice recordings containing cardholder data and/or sensitive authorisation data included in the scope of the PCI DSS, published in February 2010, is published verbatim below[1]:

**Question:** 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.

1 http://selfservice.talisma.com/display/2/index.aspx?c=58&cpc=MSdA03B2IfY15uvLEKtr40R5a5pV2lnCUb4i1Qj2q2g&cid=81&cat=&catURL=&r=0.443991661071777

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.

The penultimate paragraph suggests that if the recordings cannot be data mined, then they can be stored as long as the data is protected. Data mining could include the use of speech analytical tools that mine call recording for information and might enable the payment sections of calls from being retrieved and converted into data.

A face-value reading of the February 2010 FAQ as a whole might be summarised as:

- If the technology exists to prevent the CVC2 details being capture in the call recording then it should be used
- If the technology is not present, then the CVC2 details can be stored in the call recording, provided that it meets the encryption and access control criteria set out in the PCI DSS
- That if speech analytics is used, then the CVC2 details should not be stored in the call recording

# 4. Strategies for achieving PCI DSS compliance with call recordings

This section provides an overview of various strategies and technology solutions that can be used to help a contact centre obtain PCI DSS compliance.

## Pausing recording during the payment section of the call

This solution makes use of the functionality provided by some call recording equipment vendors to pause call recording and then resume it at a later stage within the call. This has the effect of removing any cardholder data from the call recording and therefore achieving PCI DSS compliance.

The primary problem to solve when implementing this approach is "how to know when to pause / resume the recording". There are three common approaches, summarised below.

1. **Provide the agent with a pause / resume button on their screen**

This is usually the simplest way to achieve this functionality with most call recording vendors having a small application that will run on the agent's PC. The agent will be required to hit the pause button on entering the payment processing section of the call, and then to hit the resume button afterwards.

The advantage of this method is its cost and ease of integration (i.e. no integration is required) but has a major disadvantage in that it relies on the agent to remember both to pause the call recording and then resume it again at the appropriate times. The agent forgetting to pause the call recording may put the PCI DSS compliance in jeopardy, and forgetting to resume it afterwards may cause problems both for regulatory compliance (for example, FSA compliance) and quality monitoring purposes.

2. **Integrate the agent's application with the call recording system using an Application Programming Interface (API)**

With this method, modifications are made to the application the agent uses to process payments – for example, a scripting application. When the script moves on to the payment processing "page" or screen, the script sends a message via the Application Programming Interface provided by the call recording vendor, instructing the call recording to stop. When the script or application moves out of the payment processing phase, another message is sent to instruct the recorder to resume recording.

The advantage of this approach is that the agent cannot forget to invoke the pause / resume function because it is built into the script. However, this approach does present some technical challenges and requires bespoke development work to be carried out on the applications used by the agents. In some cases, agents may process cardholder payments using a number of different applications which increases the amount of integration work required, and it is not always possible to modify applications.

3. **Use Desktop Integration Technology to pause / resume the recordings**

This approach uses technology which "watches" the agent's activity and can be configured to invoke the call recording systems' pause and resume APIs when the agent performs certain functions. Some leading call recording vendors provide such tools, primarily for integrating business data with the call recording, but the same technology can be used to pause and resume recordings. For example, if all payments are processed using a separate Payment Processing Application, the technology can be configured to issue the pause command when that application receives focus (i.e. when the agent switches to it) and to resume the recording when it loses focus (i.e. when the agent goes back to another application, moving the payment processing application into background.)

This solution has its advantages when integration with the agent's applications is not possible, but is not available on all call recording platforms and still requires skilled configuration work.

## Encrypt and control access to the call recordings

As already covered earlier in this document, many call recording vendors offer encryption and access control functionality. Care should be taken to ensure that the methods used comply with the PCI DSS standards, and there are a number of issues contact centres adopting this approach should be aware of:

- Ensure that all applications in the call recording vendor's application suite comply with the rules – for example, the quality management, performance management and training modules that may use call recordings as source material
- If speech analytics is to be used, discuss with a QSA or the PCI itself if its use constitutes "data mining" as outlined in the February 2010 FAQ (see The CVC2 or Security Code above)
- If any recordings are to be passed to a third party – as often happens when an outsourced service provider sends copies of call recordings to their clients – then the relevant sections of the call should be masked or deleted prior to being sent to the client. Many call recording systems provide this function to edit a recording or to place silence over certain sections of it.

## Prevent the cardholder details from being recorded

There is some technology available that intercepts calls between the network provider's telephone lines and the call recording system that enables the cardholder data to be removed from the call. The agent asks the caller to enter their cardholder data using their telephone keypads, and the system prevents the tones received from being passed on to the agent. This technology requires integration both with payment gateways and with the agent's business application, but has the advantage of completely removing cardholder data from the call recording. In addition, it also keeps cardholder data away from the agents, removing the possibility of accusations of fraud from within the contact centre.

This technology requires additional investment and the costs could be material when implemented over a large number of inbound or outbound telephone lines. These solutions have the advantage of "de-scoping" the contact centre completely from PCI-DSS requirements – if no card details ever reach the contact centre systems, then those systems do not need to conform to the requirements of the PCI-DSS.

## Transfer the call to a self service application to collect cardholder data

In this solution, when the agent gets to the part of the call where sensitive cardholder details are to be collected, the agent transfers the call to an IVR self-service application to collect the details using either speech recognition or tones from the telephone keypad. It may be that the whole payment section is handled by the IVR, or it could simply be the collection of the CVC2 number. The advantages of this approach are that the details can be removed completely from the agent, but there are a number of disadvantages.

Firstly, the agent loses control of the call and the experience for the customer can be unsettling. Secondly, integration is required between the Self-Service application and agent's business application and between the self-service application and the payment processing system. Thirdly, the IVR system itself must also be PCI DSS compliant and finally, if trunk-side call recording is deployed then there may need to be integration between the call recording system and the self-service application to ensure that the recording is paused to avoid recording the self-service leg of the call.

## Processes & compensating controls

Achieving PCI DSS compliance is a complex topic for any organisation and this document is intended to provide an overview of some of the technology solutions which are available to aid with the call recording element. In many cases, it may not be possible to solve the problem with the use of technology alone. In assessing an organisation's compliance with the PCI DSS the concept of "compensating controls" can be used – if an organisation cannot achieve the letter of the standard, then it may, in some circumstances, implement a compensating control. In the examples given above, for example, if the call recordings contain the CVC2 number but are encrypted, a compensating control may be to ensure most call recordings are kept "off-line" i.e. not accessible over the network, and the storage media protected with appropriate physical security.

# Further reading

The PCI web site provides for full detail of the PCI DSS, and its revision published in November 2010. In addition, the acquiring banks will be able to provide guidance on individual aspects of compliance. Organisations subject to regulation by the Financial Services Authority (FSA) should also consider their FSA compliance obligations regarding the recording of telephone calls alongside the requirements of PCI DSS.

**Links to:**

PCI Website
https://www.pcisecuritystandards.org/

FSA Website
http://www.fsa.gov.uk/

Barclaycard white paper
http://www.barclaycard.co.uk/business/documents/pdfs/processing_telephone_payments.pdf

# Glossary of terms

| | |
|---|---|
| **PCI** | Payment Cards Industry – The body representing card issuers |
| **PCI DSS** | The Payment Cards Industry Data Security Standard |
| **PAN** | Primary Account Number. The long number on a payment or credit card – sometimes referred to as the card number. |
| **Service Number** | Sometimes referred to as the card's "Issue Number" |
| **QSA** | Qualified Security Assessor |
| **CAV2/CVC2/VV2/CID** | These acronyms all refer to the security code on the signature strip of a payment or credit card. |
| **IVR** | Interactive Voice Response |