VERSADIAL®
recording made simple

Versadial PCI Compliance

Content

U.S. Toll Free: 1-877-723-4252
Email: sales@versadial.com
International Call: +1-949-457-0650
Fax: 1-949-457-0465
Mon. - Fri. 8am-6pm PST

Versadial Solutions
9940 Irvine Center Drive
Irvine, CA 92618
USA
www.versadial.com

ver. 5.16.12

Executive Summary

PCI Security Council's "Information Supplement: Protecting Telephone-based Payment Card Data" document recommends asking call center system vendors the following questions.

1. **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).

2. **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.

This document is provided for current or potential users and for resellers of the Versadial Call Recording Solution, as a response to the above questions. It also serves as a guide to making a call recording system and procedure compliant with PCI Data Security Standard. This document provides supplemental and relevant information as it pertains to the Versadial Call Recording Solution and does not replace or supersede PCI DSS requirements.

PCI DSS Requirements for Stored Cardholder Data

Per PCI Security Council's "Information Supplement: Protecting Telephone-based Payment Card 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	**Card Holder 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). For telephone operations, "sensitive authentication data" means the CAV2/CVC2/CVV2/CID and/or PIN values that may be taken during a telephone call.

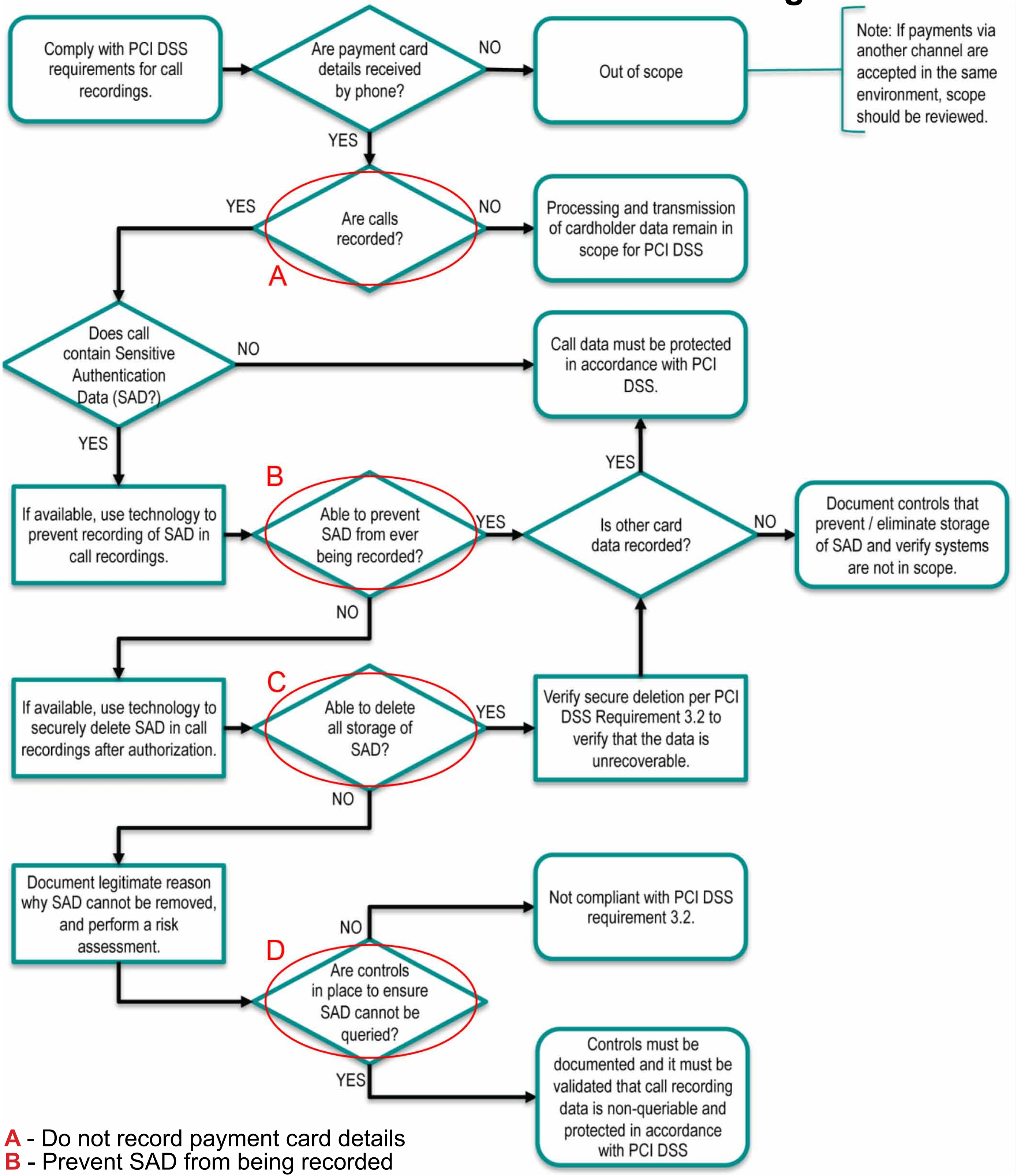
Even though Cardholder Data may be stored, the Primary Account Number (PAN) should be unreadable (inaudible from the call recording) per Requirement 3.4

From above we can conclude that in order to be PCI DSS compliant:

- The call recording system must not record/store Sensitive Authentication Data
- The call recording system should not store Cardholder Data in order to avoid some extra access control requirements

The following page shows how Versadial Solution's Call Recording technology features may be applied within the decision process for Voice Recording recommended by the PCI Security Council.

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
YES
Are calls recorded?
NO
Processing and transmission of cardholder data remain in scope for PCI DSS
A
Does call contain Sensitive Authentication Data (SAD?)
NO
Call data must be protected in accordance with PCI DSS.
YES
YES
B
If available, use technology to prevent recording of SAD in call recordings.
Able to prevent SAD from ever being recorded?
YES
Is other card data recorded?
NO
Document controls that prevent / eliminate storage of SAD and verify systems are not in scope.
NO
C
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.
D
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

A - Do not record payment card details
B - Prevent SAD from being recorded
C - Delete SAD from recording storage
D - Provide controls to ensure SAD cannot be queried

How to Comply

	Versadial Notes
A - Do not record calls with SAD	If your call recorder does not record any Payment card detail or sensitive authentication data (SAD). Your call recorder is compliant – period.
B - Prevent SAD from being recorded	Preventing SAD from being recorded by using only technology features is very challenging. All methods currently available from different vendors are not 100% effective. Speech recognition, Desktop analytics and other methods are error-prone unless used in conjunction with a strongly enforced process policy, which isolates time segment during which payment card details are uttered by the cardholder. Otherwise your company will not be PCI DSS compliant, even if your vendor claimed “compliant call recording system”. **Examples? :** • Agent collects payment info without opening screen or program, or other action, which is supposed to trigger recording pause. • Agent collects payment info before or after triggering event • Agent collects payment info from the phone/ channel with no triggering events
C - Delete SAD from the recording storage	Detecting if SAD has been recorded by using only technology features is also very challenging. (See notes from section B above). However, it can be more effective to detect recordings which potentially contain SAD and to flag them as such. So technology should allow for deletion of all recordings marked as containing SAD, or such recordings should be protected according PCI DSS (ensure Sensitive Authentication Data cannot be queried, see section D) Also,if you use B level recording prevention (see above) you still need to have a procedure in place to audit consistent execution of payment information collection procedure, and an option to fix the situation when a recording still slipped through. So technology should allow for removal of SAD from the recording, or at least deletion of the whole recording.
D - Provide controls to ensure SAD cannot be queried	Per PCI DSS guidelines “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 fulfill PCI DSS requirements without contravening government laws and regulations, these technologies should be used.” ***Note: “****Encrypting sensitive authentication data is not by itself sufficient to render the data non-queriable*” **Also :** “*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.*” Considering all of the above, Versadial has selected to concentrate on Level A, B and C technology features as part of our call recording packages. The Level D archiving package will be offered to interested parties as a separate, add-on product.

Making Your Call Recorder
PCI DSS Compliant with VSLogger Unlimited

Option 1 (internal policy and procedure)		
	Internal Procedures	**Recorder configuration**
A	Have a dedicated line for collection of payment card details.	• Do not record trunk lines • Do not record payment collection line(s)

Option 2 (with staff intervention)		
	Internal Procedures	**Recorder configuration**
B	Put a procedure in place that requires agents to stop recording, before collecting payment card details	• Do not record trunk lines • Install Versadial Desktop Assistant on the agent's PC • Configure ADA to allow Pause/Silence recording • Give agents permission to pause/silence recordings for their phone channel
C	For cases when an agent fails/forgets to stop recording in section B: • Put a procedure in place that requires agents to erase sensitive information from the recording after the call. • Put a procedure in place that requires agents to add a note e.g. "DELETE -CC" to the call. • Put a procedure in place that requires the recorder administrator to delete all recordings with the above note daily.	• Give agents permission to edit(replace sensitive info with silence) recordings for their phone channel (Allowed access to VSLogger UI) • Give agent ability to "Make a Note" • Enable the "Delete Recording" Administrative feature

Option 3 (automatic)		
	Internal Procedures	**Configuration**
C	Put a procedure in place that requires agents to collect payment card details only through the Interface with Recording Control Events. (See. Appendix 1. "Creating Sensitive Information Collection Interface with Recording Control Events.")	• Do not record trunk lines • Enable VSLogger API interface • Configure "Sensitive information collection interface with Recording Control Events" which sends a "Stop" , "Mute or "Pause" commands to VSLogger recorder whenever an agent collects payment card details.

Appendix 1.
Creating Sensitive Information Collection Interface with Recording Control Events

It is simple enough to establish a process to prevent recording sensitive information with call center staff intervention (manual Stop/Pause recording commands before collecting sensitive information). A step further would be to generate Stop/Pause commands automatically. There are different ways of doing this using Versadial VSLogger API.

Internal Custom Software

Only customers know their internal processes from top to bottom. Internal (often custom software) controls general workflow. If sensitive information collection process is controlled by such a program, the same program can send the recorder Stop/Pause or Mute commands as needed.

Call Center Data Collection Software Capable of Triggering an Event

Many Call center software packages that provide a Call Center Representative with popup screens are also capable of generating events or executing custom commands/scripts during transitions from one form to another. Such a feature can be used to send recorder Stop/Pause or Mute commands when a Call Center Representative opens a payment card collection form.

3rd Party Desktop Analytics (Automation) Software

There are 3rd party applications capable of detecting the moment when a specific form or window is open or focused. These applications may be used to send recorder Stop/Pause commands when a Call Center Representative opens a payment card collection form/application.

VERSADIAL®
recording made simple

U.S. Toll Free: 1-877-723-4252
Email: sales@versadial.com
International Call: +1-949-457-0650
Fax: 1-949-457-0465
Mon. - Fri. 8am-6pm PST

Versadial Solutions
9940 Irvine Center Drive
Irvine, CA 92618
USA
www.versadial.com