Version: 0.102c

Date: 17th December 2013

Information Supplement:

Protecting Telephone-based Payment Card Data

TABLE OF CONTENTS

1 INTRODUCTION

1.1 BACKGROUND

This document has been produced to help make sure merchants and service providers are not exposing themselves and their customers to the risks of fraudulent activity when processing card payments over the telephone.

Recent fraud reduction initiatives such as Chip & Pin, Verified by Visa and MasterCard Secure code, have significantly reduced rates of fraud in the face to face and E-commerce sectors. There remains however a limited amount of solutions that can fight fraud in the Mail Order/ Telephone Order (MOTO) space, resulting in a shift of card fraud towards MOTO.

For merchants and service providers, appropriate measures are required to protect any systems that store, process and/or transmit cardholder data; since cardholder data can be present in telephone calls. Relevant systems include but are not limited to:

- telephony systems and infrastructure (PBX, auto-diallers, call & screen recording, IVRs etc.) that merchants and service providers use, for taking card not present payments;
- the people handling the calls;
- their physical environment;
- the systems used by those people to process the payments.

1.2 PURPOSE

This Information Supplement has been produced to provide payment security advice for merchants and service providers who accept and/or process card payments over the telephone. This document intends to highlight the key areas organisations with operations need to address in order to process card payment cards securely, and how best to protect their business and their customers from the risks of data compromise and fraud.

1.3 AUDIENCE

This information and guidance is aimed at Company Owners, Financial Directors, IT Directors and Call Centre Managers of businesses processing card payments over the telephone. The guidance is also aimed at Qualified Security Assessors (QSA) and Internal Security Assessors (ISA) to assist in the interpretation of the Payment Card Industry Data Security Standards (PCI DSS) as it relates to telephone payments.

1.4 DOCUMENT STRUCTURE

- Section 2 contains the Executive Summary – targeted at the busy reader, this section provides a high level summary of the main issues discussed and the recommendations.
- Section 3 describes the normal call flow for a telephone-based purchase using a payment card and how the Payment Card Industry Data Security Standards (PCI DSS) impact the process.
- Section 4 contains recommendations for merchants and services providers for delivering PCI DSS compliant services.
- Section 5 contains some frequently asked questions relevant to the subject matter.
- Section 6 contains a glossary of terms.
- Sections 7-12 contain annexes wherein specific technical issues are discussed in more detail.

2 EXECUTIVE SUMMARY

2.1 OVERVIEW

In order to understand how PCI DSS can be seen to relate to your phone system when receiving card payments over the phone it is important to be aware of the journey cardholder data takes when an individual divulges their card details. In order to demonstrate this journey we will be using the generic example of a customer making a telephone purchase through a call centre. In this case, when the customer provides their card details over the phone or enters their card details using the telephone keypad the call flow is in scope for PCI DSS.

This guidance attempts to describe where cardholder data is in scope for PCI DSS and therefore where PCI DSS controls are required. For the purposes of PCI DSS, the collection of systems, processes and people where cardholder data is processed, transmitted or stored, either by the merchant or service provider, is referred to as the Cardholder Data Environment (CDE) and it is this CDE which needs to be controlled and secured.

The assumption is made that cardholder details are provided by the customer during the call, either within the voice stream or via DTMF (Dual-Tone Multi-Frequency) tones by using the keypad. Where the customer uses the keypad and the DTMF stream is not audible to the call centre agent or interpretable by information technology systems, the call is out of scope for PCI DSS.

2.2 CONTEXT

During the course of a payment card transaction made over the telephone, cardholder data may be divulged either in spoken voice or in the DTMF tones used to signal key presses. As such a telephone call is a method of ***transmitting*** cardholder data. If the telephone call is recorded, as required by many financial service authorities, cardholder data is then present in the recordings and thus is ***stored***, probably in an accessible format. The implication is that systems involved in the transmission or recording of calls need to be protected as defined by the Payment Card Industry Data Security Standard (PCI DSS).

Increasingly VoIP technology is being used to make and receive calls via the Internet, an open public network. Since the merchant is in control of how their telephone system connects to the telephone network, it is important to understand how VoIP technology can be used securely.

2.3 IMPLICATIONS

Any sales process that involves taking card payments over the telephone will impose a requirement on you, the Merchant, to maintain compliance with the PCI DSS for the entire process. This responsibility rests with you whether you have direct operational control over all aspects of the process or use external service providers. Accountability, and with it financial liability, cannot be sub-contracted.

Whilst public fixed line telephone networks are assumed, by the PCI Security Standards Council, to be secure, the same cannot be said of Voice over Internet Protocol (VoIP) services. In this context, there are three main areas of concern when it comes to the security of payment card data when using VoIP services:

- Security of the connection between the purchaser and the Merchant;
- Security of payment card data within the Merchant's environment;
- Security of the payment processing mechanism.

Whether you take payments by asking your customer to speak the card details or use their telephone keypad, the most vulnerable element of the process to external interception is the connection between the customer and the Merchant. The obvious solution to this aspect of the process is to use encrypted VoIP services to reduce the risk of interception of sensitive card data.

Within the Merchant environment and the payment processing mechanism, the Merchant has two basic choices… do it yourself or sub-contract. If you handle the entire process yourself, the PCI DSS will require you to secure every aspect of the transaction, including the premises, the people, the processes, the systems and the networks where cardholder data is stored, processed or transmitted. If you choose to sub-contract, it is entirely possible to reduce or even eliminate the exposure of your business to the risks and consequent liabilities associated with cardholder data.

2.4 RECOMMENDATIONS

2.4.1 Understanding the location of your Cardholder Data

In order to comply with PCI DSS or when undertaking a risk based prioritised approach at reaching compliance, it is first important to understand where the cardholder data is on your network and to then make sure it is protected.

Remember that Cardholder data could be present in telephone calls. If it helps, draw a diagram showing the call flow on your network, asking your IT manager or PBX maintainer for assistance as required. Start from the customer calling in and work through the call flow until it is answered by the telephone operator. Don't forget to consider any 3rd party service providers, your phone systems, call recording systems and the telephone LAN if you have one. All devices which handle calls must be considered to be inside your cardholder data environment and must be protected.

2.4.2 Choosing Service Providers

The risks involved when using a Voice over IP Telephony Service provider, or cloud (hosted) telephony service provider need to be fully understood as the security of cardholder data is of paramount importance.

Service Providers are aggregators of Cardholder data and as such a possible target for criminals. When engaging with Service Providers you as a merchant are responsible for cardholder data security and should ensure that agreements specify precisely who is responsible for the security of cardholder data at each stage in the call flow. Service providers should also be asked to verify how they will ensure (and, as important, assure) that PCI DSS requirements continue to be met throughout the lifetime of the contract.

As the Merchant, whilst operational responsibility may be outsourced or sub-contracted, accountability cannot. Hence, it is essential that you ensure your service providers have proactive network monitoring in place on a 24x7 basis, that patching policies exist and are enforced, that services are independently assessed for PCI DSS compliance and that any changes to services that might impact your compliance status are discussed with you before they are implemented.

2.4.3 Managing your Cardholder Data Environment (CDE)

Eliminating cardholder data from your network, consolidating necessary cardholder data to known manageable network segments and isolating cardholder networks from non CDE networks will reduce the network components that require protection. Further to this

remember that PBX maintainers may have access to phone systems for maintenance reasons (and therefore be able to change behavour). It's very important to understand and document remote access networks, access procedures and their use (logging). Make sure you have a change management system setup with your maintainer.

3 GENERIC INCOMING CALL FLOW FOR A TELEPHONE PAYMENT

3.1 OVERVIEW

In order to understand how PCI DSS can be seen to relate to your phone system when receiving card payments over the phone it is important to be aware of the journey cardholder data takes when an individual divulges their card details. In order to demonstrate this journey we will be using the generic example of a customer making a telephone purchase through a call centre. In this case, when the customer provides their card details over the phone or enters their card details using the telephone keypad the call flow is in scope for PCI DSS.

This guidance attempts to describe where cardholder data is in scope for PCI DSS and therefore where PCI DSS controls are required. For the purposes of PCI DSS, the collection of systems, processes and people where cardholder data is processed, transmitted or stored, either by the merchant or service provider, is referred to as the Cardholder Data Environment (CDE) and it is this CDE which needs to be controlled and secured.

The assumption is made that cardholder details are provided by the customer during the call, either within the voice stream or via DTMF (Dual-Tone Multi-Frequency) tones by using the keypad. Where the customer uses the keypad and the DTMF stream is not audible to the call centre agent, the call is out of scope for PCI DSS.

Below is the call flow for our example call centre.

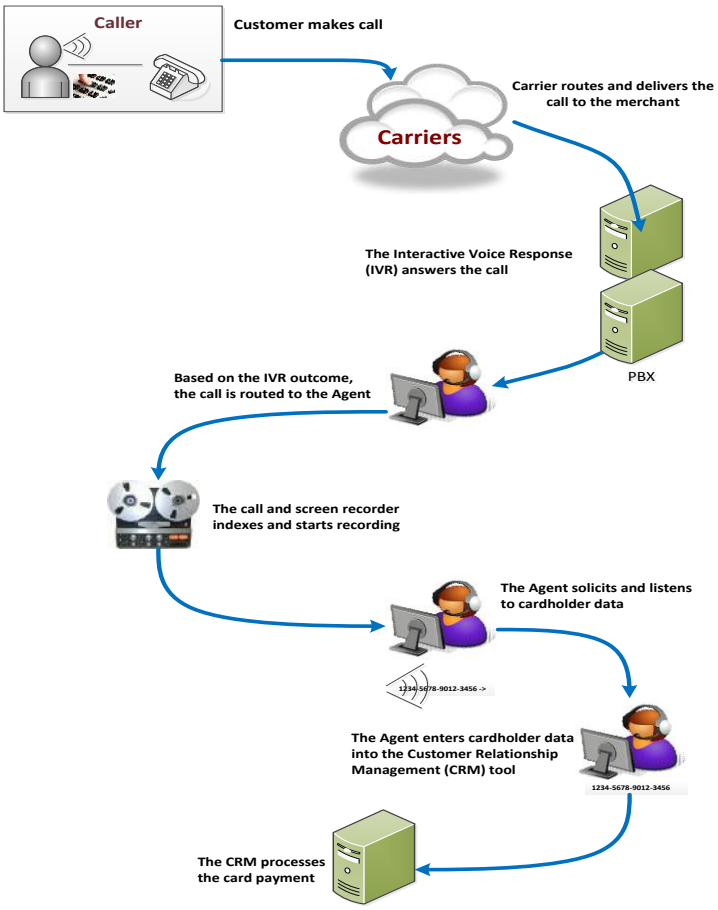


Figure 1: Cardholder data journey for a telephone order

3.2 How PCI DSS impacts the Call Flow

3.2.1 Summary

Having seen how cardholder data is transmitted through every component of the call flow, it is possible to now explore where in this journey you as a merchant are responsible for ensuring the security of the call in order to meet the requirements of PCI DSS. In what follows each component of the call flow will be explained in more detail and whether you, the merchant, will need to consider implementing action to protect it. If an aspect of this call flow is considered to be something that PCI DSS applies to, it is commonly said that it is in scope of PCI DSS.

To further assist in understanding exactly what is expected of you, in the blue boxes after each component discussion we have identified the PCIDSS requirements that apply to this component. These requirements can be viewed in more detail on the PCI DSS website.

3.2.2 Step 1 - Customer makes call by dialling a number

PCI DSS is concerned about protection of cardholder data by merchants and service providers and does not attempt to address the security of cardholder data for individuals. You therefore do not need to be concerned about ensuring the security of cardholder data at this point.

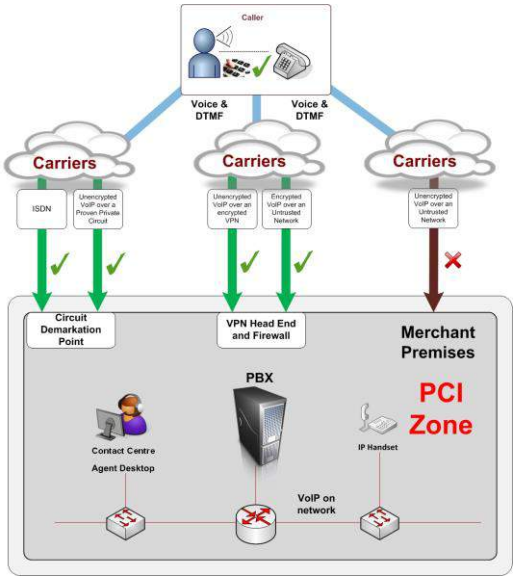
3.2.3 Step 2 - Telecommunications carrier routes and delivers the call to the merchant

As soon as the telecommunication carrier routes the call to you, under PCI DSS requirements, protection of cardholder data becomes your responsibility. In the case of you making an outbound call to the customer, again under PCI DSS requirements, protection of cardholder data becomes your responsibility.

As a merchant you are in control of the way in which you connect your phone systems to your chosen voice telecommunications carrier. This is where you or your phone system provider decides whether you want your calls to go through traditional phone lines or to use a VoIP service. Some of these links can be infiltrated by malicious individuals and as such PCI DSS will expect that you are ensuring the protection of calls transmitted over these links if you take card payments over the phone.

There are multiple ways you can connect to a voice telecommunications carrier but the three most common ways are:

1. Phone lines e.g. ISDN or analogue connection;
2. Internet connection and using Voice over Internet Protocol (VoIP) technology;
3. Private IP leased line and using VoIP technology.



You may not be aware how you connect to your voice telecommunications carrier. It is advisable to contact the company who provides your telephone system to confirm your connection type. The type of connection will dictate the security requirements you are expected to fulfil as part of PCI DSS.

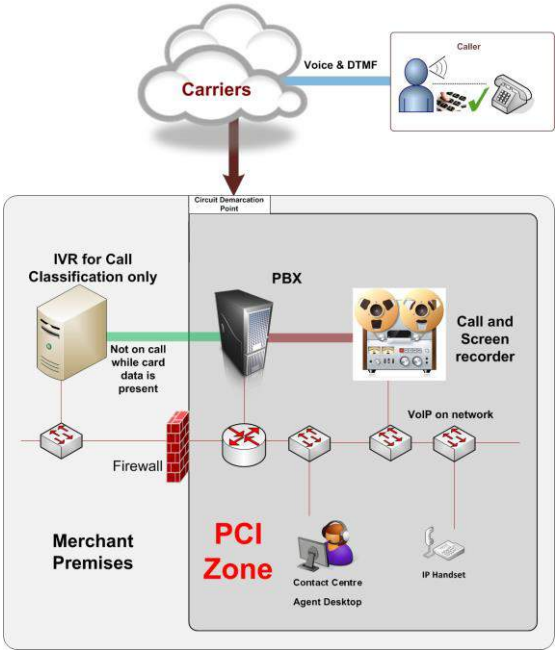
It is your responsibility to select a compliant connection type.

A more detailed examination of the implications of different carrier options is included in Annex A (Section 7).

3.2.4 Step 3 - The Interactive Voice Response (IVR) answers the call

If an IVR is used to answer the call or help route the call and could remain in the call path during the payment process then the device should be considered as part of the Cardholder Data Environment. As such since it could be used to solicit card data or eavesdrop during the payment part of the call. PCI DSS requirements apply to it and you should ensure that it is protected. Where it is not possible for the routing IVR to remain in the call path at the point of soliciting cardholder details then the IVR can be deemed out of scope. If the IVR could be reconfigured to be in the call path, then it is a connected device and you should ensure that it is protected.

IVRs in scope for PCI DSS will need to meet PCI Requirements 1, 2 and 4 through 12.



3.2.5 Step 4 - Based on the IVR choices, the is call sent to the appropriate Agent

The routing of the call to the most appropriate agent involves several different telephony components. As every aspect of the call after the routing by the telecommunications carrier is your responsibility you are required to consider how secure all the different telephony components are routing to the agent in relation to PCI DSS requirements.

The phone system, otherwise known as the Private Branch Exchange (PBX) or Private Automatic Branch eXchange (PABX) will always be within the call path and therefore will be transmitting cardholder data. This includes any accessory systems e.g. Automated Call Distribution systems and gateways. Therefore, the PBX system if compromised could be used to solicit cardholder data. For this reason PCI DSS requirements apply to it and you should ensure that you have implemented appropriate controls to protect it.

The PBX and telephony gateways should be protected under PCI DSS requirements 1, 2, 5 through 12

A more detailed examination of the different technologies involved in this step is included in Annex B (Section 8).

3.2.6 Step 5 - The call and screen recorders start recording

Call recorders are used to record and monitor the telephone call with the customer and the screen recorder records and monitors the agent's desktop screen session with the merchants computing systems, for the duration of the customer interaction. These activities are typically undertaken for quality, training and compliance reasons. When understanding how to apply to PCI DSS it is important to make a distinction between the recorder and its recordings.

Call and Screen Recorders and the recordings they make should comply with PCI Requirements 1 through 12.

A more detailed examination of call and screen recorders is included in Annex C (Section 9).

There are two recognised industry techniques for the prevention of capture of Primary Account Number (PAN) and Card Verification Value (CVV2) data on call recordings. These

are ‘pause and resume’ and DTMF tone masking. These are discussed in more detail in Annex D (Section 10).

3.2.7 Step 6 - The Agent asks for and listens to cardholder data

If the agent has access to cardholder data then PCI DSS requirements will also apply to them as it is possible for malicious individuals to infiltrate your company with the sole intension of obtaining cardholder data. It is also possible for otherwise honest staff to be coerced by organised criminal gangs in to compromising cardholder data. It is your responsibility as the merchant to ensure that appropriate PCI DSS controls are in place to prevent card data loss through staff.

To protect cardholder data within the physical contact centre the following controls should be in place:

1. Background checks on all contact centre staff (including previous employment history, criminal record, credit history and general reference checks) – Requirement 12.7 specifies that such checks are conducted for new employees, though if starting to take card payments in an existing call centre, it would be prudent to consider conducting such checks on existing staff;
2. Video monitoring or access controls as per FAQ 1156 – Requirement 9.1.1;
3. Card key in and card key out of all personnel with access to the contact centre with security at the perimeter of the contact centre – Requirement 9.1;
4. Clear identification of personnel and visitors (definitive) – Requirement 9.2;
5. If paper and pens are allowed within the call centre environment then the paper needs to be strictly controlled i.e. numbered and identifiable sheets of paper should allocated to named agents (Requirement 9.9) and the paper collected at the end of their shift to confirm all paper is collected and then ensuring all paper is destroyed as per Requirement 9.10. An alternative approach is for pen and paper to be replaced by fixed white boards and marker pens;
6. No personal items, including mobile telephones and tablets, on the contact centre floor (lockers provided for such outside of the contact centre;
7. Restricted email access to prevent potential leakage or loss of cardholder data - Requirements 7, 9.7 and 12.3;
8. No access to instant messaging to prevent potential broadcast of cardholder data – Requirements 7, 9.7 and 12.3;
9. No access to web or social media to prevent potential loss or leakage of cardholder data – Requirements 7, 9.7 and 12.3;
10. Detection of active mobile phones to prevent potential loss or leakage of cardholder data – Requirements 7, 9.7 and 12.3;
11. Wireless scanning to prevent the creation of a wireless network for the potential broadcast of cardholder data – Requirement 11.1;
12. Protection of USB ports and access to Bluetooth devices and other means of copying data off systems within the CDE;
13. Additional agent supervision to protect cardholder data to ensure adherence to policies and procedures.
14. Information security policy to protect cardholder data within the call centre environment – Requirement 12.6.2.

To be clear, it is the Merchant’s and/or the Service Provider’s responsibility to make cardholder data exposed within a physical call centre secure. If additional measures

beyond the above are indicated by the annual risk assessment (requirement 12.7.2 then the Merchant and/or Service Provider is obliged to implement such measures.

Given the controls which need to be in place for agents who come in to contact with cardholder data at your call centre, it is difficult to envisage any circumstances under which home / remote agents coming in to contact with card data can be considered as complying with PCI DSS requirements. Therefore you may find that in attempting to make these individuals compliant with the requirements very costly and in some cases not possible. See the controls in this section which outlines the PCI DSS requirements you are expected to meet to get a better understanding of why this is the case.

3.2.8 Step 7 – The Agent enters cardholder data into the Payment Application (PA)

The agent enters cardholder data via their keyboard on the contact centre desktop into the merchant's PA. The agent desktop, the contact centre data network connected to this desktop and the PA are in scope for PCI DSS as a malicious individual could gain access to these and use a number of methods to extract cardholder data. For this reason you will need to use appropriate security controls to protect against this. For a more detailed understanding of general requirements and controls that need to be implemented, see box below.

If cardholder data is cached locally on the desktop then Requirement 3 of PCI will apply. PCI Requirements 1, 2 and 5 through 12 will apply to the agent desktop. PCI Requirements 1, 2 and 6 through 12 will apply to the data network. PCI Requirement 1, 2 and 5 through 12 will apply to the PA. Within the PA, PAN data should be masked to comply with PCI Requirement 3.3.

Alternatively the agent can enter cardholder data into a PIN Entry Device (PED) to process the payment. This technique removes the agent desktop and CRM from PCI scope. If the call is delivered over an analogue line and the merchant only processes card payments through PEDs, then the merchant may be eligible for Self-Assessment Questionnaire-B (SAQ-B). If such telephone payments operate over VoIP, then only SAQ-D or a ROC will be applicable.

If a terminal emulator such as Citrix is used to access the merchant CRM and cardholder data is entered into the terminal emulator client then the agent desktop, the agent desktop network and terminal emulator server(s) and the network for the terminal emulator server(s) are in scope for PCI DSS.

3.2.9 Step 8 – The PA processes the card payment

If you are receiving calls containing cardholder details and your staff enters these details into a payment application, then this application will be in scope of PCI DSS requirements as if it was to be maliciously attacked cardholder data can be drawn from it. However, the PCI DSS requirements you are expected to undertake to protect such vary depending on what your application is being used to do.

If it is storing the cardholder data then you will have to be applying security controls in line with PCI DSS requirement 3. If it is being used to process cardholder data it needs to meet PCI Requirements 1, 2 and 5 through 12. If the application transmits cardholder data over an open or public network it needs to meet PCI Requirement 4. If your application is doing

all three aspects then you will have to ensure that you have met all the previously stated requirements.

Merchants using hosted PAs or payment pages should be aware that if such a system processes, transmits or stores cardholder data then the service provider needs to be managed according to requirement 12.8.

If a merchant's systems use a hosted payment page from a PCI Certified (preferably Level 1) Payment Services Provider (PSP) into which an agent enters cardholder data then the agent desktop is in scope for PCI DSS. However, the merchant's systems and the data network connected to the agent desktops are taken out of scope of PCI DSS by the hosted payment page as cardholder data is transmitted securely directly from the desktop to the PSP.

A more detailed discussion of the implications for multi-site organisations is included in Annex E (Section 11).

3.3 Alternate Call Flows

There are a variety of ways in which the generic example of a call flow can vary. It may be the case that rather than owning and running all these telephony components, you have instead outsourced some or all of them to third parties to manage.

It is important when considering PCI DSS compliance to consider the full payment call flow, identify what components process, transmit or store cardholder data, determine the ownership of the components and ensure all components are secured. Where components are hosted by Service Providers then either the Service Providers must be certified PCI compliant or you must include the services as part of your own compliance assessment. In either event it remains your responsibility to ensure that such services are provided in a compliant manner.

All Payment Applications, hosted within Service Providers or on premise at Merchants must be Payment Application Data Security Standard (PA DSS) certified as per the Visa and MasterCard directives below:

- http://www.mastercard.com/us/company/en/docs/MasterCard_PA_DSS_Mandate.pdf
- http://usa.visa.com/download/merchants/payment_application_security_mandates_regions.pdf).

A more detailed examination of some implementation options is included in Annex F (Section 12).

4 RECOMMENDATIONS

4.1 UNDERSTANDING THE LOCATION OF YOUR CARDHOLDER DATA

In order to comply with PCI DSS or when undertaking a risk based prioritised approach to reach compliance, it is first important to understand where the cardholder data is on your network and to then make sure it is protected.

Remember that Cardholder data could be present in telephone calls. If it helps, draw a diagram showing the call flow on your network, asking your IT manager or PBX maintainer for assistance as required. Start from the customer calling in and work through the call flow until it is answered by the telephone operator. Don't forget to consider any 3rd party service providers, your phone systems, call recording systems and the telephone LAN if you have one. Devices which handle calls must be considered to be inside your cardholder data environment and must be protected.

4.2 CHOOSING SERVICE PROVIDERS

The risks involved when using a Voice over IP Telephony Service provider, or cloud (hosted) telephony service provider need to be fully understood as the security of cardholder data is of paramount importance.

Service Providers are aggregators of Cardholder data and as such a possible target for criminals. You should consider the following 'best practices' in order to keep your cardholder data safe:

- Speak to multiple service providers to compare and contrast their service offerings. This will help you understand more clearly their service offerings and help you make an informed choice.
- Ask the service provider about the security systems on their network and make it clear you need to comply with PCI DSS. A reputable service provider should understand what this means and be able to describe their security capabilities in clear, non-technical terms and offer security as part of their basic service.
- If a service provider is a PCI DSS Level-1 service provider and, as part of their secure services, offer a solution that you can use, then this is a strong indicator that you should consider using them. A PCI DSS Level-1 Service Provider has demonstrated that they clearly understand the importance of call security and have made a business decision to run a compliant service.
- Buy telephony service from a Service Provider who can demonstrate use by other merchants. Handling cardholder data requires experience.

When engaging with Service Providers you as a merchant are responsible for cardholder data security and should ensure that agreements contain the following:

- Specifies the responsibility for Cardholder data and any demarcation points.
- Indicated how they meet applicable PCI DSS requirements, how they will verify compliance and how they will maintain compliance.
- Identifies whether the Service Provider has its own PCI DSS compliance validation process or if not, that they will support you as the merchant in your own PCI DSS assessment each year for the services they provide to you.

You, as the merchant, should also check as part of the service agreement:

- That the Service Provider is actively monitoring their network 24/7 for security breaches and for maintaining service guarantees, and has a security patch procedure in place.

- If the Service Provider's network infrastructure and processes have NOT been independently assessed for PCI DSS compliance, the service provider may find it difficult and costly to remedy identified security issues. When outsourcing services to a third party service provider agree which company will pay to remediate security issues before signing up for service.
- If the Service Provider is a PCI DSS Level-1 Service provider ask to see the Service Provider's Attestations of Compliance (AOC) to make sure the service you take from them is included and the compliance is valid. If the service provider includes the network links from their service to your PBX, then this reduces the size of your cardholder environment and makes the job of ensuring compliance much easier. Service providers like you, the merchant, should be updating their PCI DSS compliance annually.

4.3 Managing your Cardholder Data Environment (CDE)

Eliminating cardholder data from your network, consolidating necessary cardholder data to known manageable network segments and isolating cardholder networks from non CDE networks will reduce the network components that require protection. Further to this remember that PBX maintainers may have access to phone systems for maintenance reasons. It's very important to understand and document remote access networks, access procedures and their use (logging). Make sure you have a documented and agreed change management system setup with your maintainer.

5 Frequently Asked Questions

5.1 Questions for Hosted Service Providers

5.1.1 Is the service you are providing me PCI DSS Compliant as a Level 1 PCI DSS Service Provider?

If a Service Provider is Level 1 PCI DSS compliant they are able to offer a service that has been independently audited and has been found to be effectively protecting cardholder data. For this reason, where possible when outsourcing, you should use a Level-1 PCI DSS Service Provider. You should ask to see the Service Provider's Attestation of compliance to ensure they're officially acknowledged as PCI compliant.

Even if the service provider is PCI DSS compliant you should ensure that you use the service in a PCI DSS compliant manner, that you maintain compliance for the parts of the service/telephony solutions that it is your responsibility to maintain. Refer to the Cloud Guidelines as it explains this split of responsibilities and implications of service provider compliance for the client and vice versa well (section 5.1 in particular).

When you do this, you should check that their attestation covers every aspect of the service they are providing you. If the Service Provider is not certified as Level-1 or self-certified, you as a merchant will need to ensure that you implement internal actions and procedures to your business which ensure the services being provided to you meet all the requirements expected of you under PCI DSS.

5.1.2 Am I using the public internet to access your servers and if so, are communications encrypted?

If they answer that they are using the public internet then the most appropriate response to the follow up question of 'is the communication encrypted' is Yes.

Any network traffic containing cardholder data needs to be strongly encrypted if open or public networks are used as these are especially susceptible to malicious attack. In order to be PCI compliant it is strongly suggested that you do not use a service that uses a public network without encryption services.

If they answer that they are providing a service over a "private" MPLS or other type of leased line[1], then the service should not automatically be assumed to be secure. For cardholder data to traverse a private link unencrypted, the underlying service provider should offer the service as part of their Level 1 PCI DSS Service. If the security of the private link cannot be determined, then you the merchant should treat this link as an open or public connection and secure using encryption[2].

5.1.3 Am I using a proven private circuit to access your Servers?

A proven private circuit is a leased line or other type of IP circuit using private IP address space where the underlying carrier has provided assurance that the circuit is built Carrier to Premise using managed and controlled network appliances to secure the circuit and that the public internet has not been used as a component of the transmission circuit without use of strong encryption. If such a circuit is used this is out of scope for PCI DSS.

[1] Reference FAQs 1045, 1043, 1068
[2] Reference FAQ 8705

5.1.4 Are you call recording in any way?

If the Service Provider is recording (storing) calls then you must ensure with them that sensitive authentication data is not stored after authorisation as per PCI DSS requirement 3.2. If the Service Provider is pausing the call recorder to prevent cardholder data being stored and the call recorder remains in the call path at the time of cardholder capture then the Service Provider will have to be certified as being PCI DSS compliant.

5.2 Questions for PBX Vendors

5.2.1 Are you aware that the phone system you are providing to us is part of our cardholder data environment and therefore has to meet PCI DSS requirements?

The phone system is part of the Cardholder Data Environment and subject to PCI DSS controls. As such you should ensure your PBX maintainer understands that the phone systems are part of your CDE and that they are aware of the actions you require from them in order to help you ensure that you comply with PCI DSS.

5.2.2 Can you reassure me that your company policy with regards to device access and password control is in-line with PCI DSS requirements?

The most appropriate answer here would be 'Yes and this is auditable'.

Access to devices within the CDE is auditable. Default passwords should not be used and there are often several levels of default passwords for PBXs used for manufacturer support. These passwords are commonly found in documentation and on the internet and should be changed. Insecure services should be disabled e.g. insecure use of Simple Network Management Protocol (SNMP). Devices must be managed under your change control process. Make sure your PBX maintainer always follows your change control process.

In these circumstances, the term "Change Control Process" is used to refer to the management process that ensures that no changes are made to the CDE without being documented, auditable and reversible.

5.2.3 How are IP handsets connected to the phone system?

The IP handset is a connected system component and as such should comply with PCI DSS including device configuration standards, access controls, user identification, etc.

The ideal answer to this question would be that they are connected via a protected network and their documentation clearly shows how.

The telephone network is part of your Cardholder Data Environment (CDE) and is therefore auditable and network documentation needs to include telephones. As such if they are not aware of how their IP handsets connect to your phone system you will have to discover and document this yourself. You also need to make your PBX maintainer aware of your change control process (this is where you document any changes you make which will affect your CDE) and ensure that they follow this procedure whenever looking to make changes to the service they are providing you. The reason you need to know how your phones are connected to your network is so that you can ensure perfect configuration and thus minimise the risk of cardholder data loss by exposing this data inadvertently to outside of the cardholder data environment.

5.2.4 Have remote VoIP phones been configured and if so is the network protected?

If Remote phones or gateways exist, is this via a strong encryption VPN or otherwise protected network?

If remote VoIP phones have been connected then any VoIP traffic traversing open public networks needs to be encrypted. The remote network as part of the CDE is auditable and network documentation needs to include telephones. Make sure your PBX maintainer is aware of your change control process and all work is fully documented in an auditable fashion. The reason you need to know how your phones are connected to your network is so that you can ensure perfect configuration and thus minimise the risk of cardholder data loss by exposing data inadvertently to outside the cardholder data environment.

5.2.5 If remote access to the PBX is in place for support is that access secure, monitored and auditable?

Here you will be looking for the answer 'Yes, a secure connection is used for remote support and the identity and actions of anyone accessing the PBX remotely are monitored and logs are maintained of their actions'. If they do not answer yes to this you will be required to ensure that you have produced the documentation which records this for your phones.

All external access to the CDE under PCI DSS is to be secure and monitored. Unauthorized access to the PBX could result in the loss of cardholder data via a number of scenarios. Unsecured methods of access such as modems should be changed in favour of VPNs and similar secure access methods.

Reference PCI DSS requirements 8.3, 8.5.6, 12.3.8, 12.3.9, 12.3.10.

5.2.6 Are the servers and operating systems used for the PBX and associated applications suitably hardened against attack and are maintenance patches installed when available?

The most appropriate answer here would be 'Yes. The operating systems used for the PBX, management applications and all other associated systems have been hardened to remove any security risks. An auditable process is in place to install all maintenance patches released by the manufacturer as soon as they become available'.

PBXs, like any other application, can be attacked via the operating system they run on. Many manufacturers harden their preferred operating systems in order to address this and that needs to be confirmed. As manufacturers become aware of any security risks they will often address them in maintenance patches and service packs which need to be installed in a timely fashion in the same way anti-virus software needs to be kept current. If the service provider doesn't answer yes to this question then again this is something you will have to find a way of ensuring it is done.

Reference PCI DSS requirements 2 and 6.

5.3 Questions for VoIP Service Providers

5.3.1 Is the network link to the VoIP call servers encrypted by VPN or is secure VoIP used (e.g. SIP over TLS/SRTP)?

SIP = Session Initiation Protocol. A network protocol used to setup calls

TLS = Transport Layer Security.

SRTP = Secure Real-time Transport Protocol.

You would want here for your service provider to answer YES by VPN or Yes by Encrypted SIP.

A VPN (Virtual Private Network) is a logical link built between two or more network devices. A VPN is typically configured on a firewall and must use strong encryption.

SIP is the common VoIP call signalling system used to setup phone calls. If SIP runs over an open or public link unencrypted it is very simple to capture the traffic and record calls. However if SIP runs over an open or public network and is configured to use a special network transport called TLS, then TLS provides the VPN function and calls can be protected by using encrypted media streams called SRTP. Suitable strong cyphers must be used for both TLS and SRTP.

A call encryption scheme for SIP called ZRTP must not be used to protect cardholder data, since the call signalling end to end might not protected. Call signalling can contain cardholder data.

Network infrastructure (firewalls) or SBC (Session Border Controllers – VoIP voice routers) providing the network protection are within the scope of PCI DSS Audit.

5.3.2 Do you use TLS/SRTP? If so have you disabled non-secure services (i.e. UDP/TCP/RTP)?

Again you will be looking for the service provider to answer yes to both of these questions.

When configuring communications devices, a significant risk exists that the engineer performing the configuration makes mistakes and leaves insecure or unnecessary services active. Your agreement with your service provider (or in house team) should ensure that regular checks are made of network device configurations against PCI DSS and business requirements to ensure that only those services that are required and compliant are active.

Therefore when talking to your service provider it is important to make sure they have disabled insecure services. For example if a SIP telephone call is setup using TLS, then it is equally important to ensure that SRTP is always used (SRTP is the secured version of Real time Transport Protocol or RTP) and communication using RTP is not available.

No changes should be made to network devices without going through the formal change control process.

5.3.3 Have you created and enforced the use of strong usernames and password for my phones?

You will want them to answer yes here as to ensure full security your service provider should have setup complex usernames and password for all your IP telephones. This also applies to provisioning interfaces and as such if they are not providing this, you should ensure that they begin to.

5.3.4 Are the usernames and passwords you have supplied unique to my installation and not available elsewhere?

You will want them to answer YES to this question as if IP telephones usernames / password become known, they may be duplicated and used maliciously elsewhere on the internet.

Where default usernames and passwords are supplied, these should be replaced with auditable usernames assigned to individuals with unique strong passwords known only to those individuals. Default usernames should then be deactivated or preferably removed.

5.3.5 Who has access to my user web portal?

The answer you should expect to get is that only authorised personnel have access to this and that there are strong authentication methods used. If the service provider has a web portal that lists sensitive information such as SIP usernames and passwords or has network

configuration applications, then access to this portal should be strongly protected. Unauthorised use of the portal could for example allow calls to be diverted to non-intended personnel.

5.3.6 I use an Analogue telephone adapter for fax and my faxes may have cardholder data present. Is the Analogue telephone adapter protected in the same fashion as my IP telephone?

You want for them to answer yes to this question. A Fax encoded in a VoIP network should be treated the same as if it were a voice call and be subject to the same controls. You need to ensure your Service Provider treats the FAX systems in the same way as a voice device.

6 GLOSSARY

Term	Definition
Access control	Mechanisms that limit availability of information or information-processing resources only to authorised persons or applications.
Access Circuits (VOIP)	An ISDN replacement service consisting of an IP network connection. The intended use is for the connection of a customer site to a VoIP Service provider.
Account Data	Account data consists of cardholder data plus sensitive authentication data.
Acquirer	Also referred to as "acquiring bank" or "acquiring financial institution," it is an entity that initiates and maintains relationships with merchants for the acceptance of payment cards.
AES	Abbreviation for "Advanced Encryption Standard." Block cypher used in symmetric key cryptography adopted by NIST in November 2001 as U.S. FIPS PUB 197 (or "FIPS 197"). See Strong Cryptography.
Authentication Credentials	Combination of the user ID or account ID plus the authentication factor(s) used to authenticate an individual, device, or process.
Authorisation	The granting of access or other rights to a user, program, or process. For a network, authorisation defines what an individual or program can do after successful authentication. For the purposes of a payment card transaction authorisation occurs when a merchant receives transaction approval after the acquirer validates the transaction with the issuer/processor.
Caller ID, Caller identification, (CID), Caller Line Identity (CLI), calling line identification presentation (CLIP)	Is a telephone service that transmits a caller's number to the called party's telephone equipment during the ringing signal, or when the call is being set up but before the call is answered? Where available, caller ID can also provide a name associated with the calling telephone number. The information made available to the called party may be displayed on a telephone's display, on a separately attached device, or be processed by an attached computer with appropriate interface hardware.
Cardholder Data	At a minimum, cardholder data consists of the full PAN. Cardholder data may also appear in the form of the full PAN plus any of the following: cardholder name, expiration date and/or service code. See Sensitive Authentication Data for additional data elements that may be transmitted or processed (but not stored) as part of a payment transaction.
Cardholder Data Environment (CDE)	The people, processes and technology that store, process or transmit cardholder data or sensitive authentication data, including any connected system components.

Term	Definition
Card Verification Code (CVC) or Value (CVV) (CVV2)	Also known as Card Validation Code or Value, or Card Security Code. Refers to either: (1) magnetic-stripe data, or (2) printed security features. 1. Data element on a card's magnetic stripe that uses secure cryptographic process to protect data integrity on the stripe, and reveals any alteration or counterfeiting. Referred to as CAV, CVC, CVV, or CSC depending on payment card brand. The following list provides the terms for each card brand: • CAV - Card Authentication Value (JCB payment cards) • CVC - Card Authentication Value (JCB payment cards) • CVV - Card Validation Code (MasterCard payment cards) • CSC - Card Security Code (American Express) 2. For Discover, JCB, MasterCard, and Visa payment cards, the second type of card verification value or code is the rightmost three-digit value printed in the signature panel area on the back of the card. For American Express payment cards, the code is a four-digit unembossed number printed above the PAN on the face of the payment cards. The code is uniquely associated with each individual piece of plastic and ties the PAN to the plastic. The following list provides the terms for each card brand: • CID - Card Identification Number (American Express and Discover payment cards) • CAV2 - Card Authentication Value 2 (JCB payment cards) • CVC2 - Card Validation Code 2 (MasterCard payment cards) • CVV2 - Card Verification Value 2 (Visa payment cards)
Change Control	The collection of management processes that ensures that any proposed change to an environment is subjected to impact assessment before being made, is authorized, documented, auditable and reversible.
Cryptography	Discipline of mathematics and computer science concerned with information security, particularly encryption and authentication. In applications and network security, it is a tool for access control, information confidentiality, and integrity.
Default Accounts	Password on system administration, user, or service accounts predefined in a system, application, or device; usually associated with default account. Default accounts and passwords are published and well known, and therefore easily guessed.
Default Password	Password on system administration, user, or service accounts predefined in a system, application, or device; usually associated with default account. Default accounts and passwords are published and well known, and therefore easily guessed.
DDI, DID	Acronym for Direct Dial in or Direct Inward Dialling. An external telephone number allocated to a particular telephone within an organisation.
DNS	Acronym for "Domain Name System" or "domain name server." System that stores information associated with domain names in a distributed database on networks such as the Internet.

Term	Definition
DSS	Acronym for "Data Security Standard" and also referred to as "PCI DSS"
DTMF	Acronym for Dual Tone Multi Frequency signalling. Used to signal key-presses within a telephone network. Various methods of DTMF transmission exist for VoIP networks. The tones may be carried by the call signalling channel or the media channel. DTMF key-presses are often used to allow a user to key in credit card data or PIN information and as such the security of DTMF tones and VoIP calls is of paramount importance.
Encryption	Process of converting information into an unintelligible form except to holders of a specific cryptographic key. Use of encryption protects information between the encryption process and the decryption process (the inverse of encryption) against unauthorized disclosure.
Encryption Algorithm	A sequence of mathematical instructions used for transforming unencrypted text or data to encrypted text or data, and back again. See Strong Cryptography.
Entity	Term used to represent the corporation, organization or business which is undergoing a PCI DSS review.
Firewall	Hardware and/or software technology that protects network resources from unauthorised access. A firewall permits or denies computer traffic between networks with different security levels based upon a set of rules and other criteria.
H323	A ITU standards based media signalling protocol typically used to setup VoIP or Multimedia calls.
HOSTED VoIP	A VoIP service with IP PBX functions provided by a service provider without the need for a physical PBX to be installed at a customer site.
IETF	Acronym for "Internet Engineering Task Force." Large, open international community of network designers, operators, vendors, and researchers concerned with evolution of Internet architecture and smooth operation of the Internet. The IETF has no formal membership and is open to any interested individual.
IP	Acronym for "internet protocol." Network-layer protocol containing address information and some control information that enables packets to be routed. IP is the primary network-layer protocol in the Internet protocol suite.
IP Address	Also referred to as "internet protocol address." Numeric code that uniquely identifies a particular computer on the Internet.
IPSEC	Abbreviation for "Internet Protocol Security." Standard for securing IP communications by encrypting and/or authenticating all IP packets. IPSEC provides security at the network layer.
ISO	Better known as "International Organisation for Standardisation." Non-governmental organization consisting of a network of the national standards institutes of over 150 countries, with one member per country and a central secretariat in Geneva, Switzerland, that coordinates the system.

Term	Definition
Issuer	Entity that issues payment cards or performs, facilitates, or supports issuing services including but not limited to issuing banks and issuing processors. Also referred to as "issuing bank" or "issuing financial institution."
LAN	Acronym for "local area network." A group of computers and/or other devices that share a common communications line, often in a building or group of buildings.
Leased Lines	A highly available network connection provided to customers by telecommunication service providers.
MAC	Acronym for "message authentication code." In cryptography, it is a small piece of information used to authenticate a message. See Strong Cryptography.
MAC Address	Unique identifier assigned to network interfaces for communications on the physical network segment (physical device such as a desktop computer).
Magnetic-Stripe Data	Also referred to as "track data." Data encoded in the magnetic stripe or chip used for authentication and/or authorization during payment transactions. Can be the magnetic stripe image on a chip or the data on the track 1 and/or track 2 portion of the magnetic stripe.
Malicious Software / Malware	Software designed to infiltrate or damage a computer system without the owner's knowledge or consent. Such software typically enters a network during many business-approved activities, which results in the exploitation of system vulnerabilities. Examples include viruses, worms, Trojans (or Trojan horses), spyware, adware, and rootkits.
Masking	In the context of PCI DSS, it is a method of concealing a segment of data when displayed or printed. Masking is used when there is no business requirement to view the entire PAN. Masking relates to protection of PAN when displayed or printed. See Truncation for protection of PAN when stored in files, databases, etc.
Merchant	For the purposes of the PCI DSS, a merchant is defined as any entity that accepts payment cards bearing the logos of any of the five members of PCI SSC (American Express, Discover, JCB, MasterCard or Visa) as payment for goods and/or services. Note that a merchant that accepts payment cards as payment for goods and/or services can also be a service provider, if the services sold result in storing, processing, or transmitting cardholder data on behalf of other merchants or service providers. For example, an ISP is a merchant that accepts payment cards for monthly billing, but also is a service provider if it hosts merchants as customers
MPLS	Acronym for "multi protocol label switching." Network or telecommunications mechanism designed for connecting a group of packet-switched networks. MPLS is often used to provide logical point to point connections over shared underlying IP networks. MPLS does not provide encryption services.

Term	Definition
NAT	Acronym for "network address translation." Known as network masquerading or IP masquerading. Change of an IP address used within one network to a different IP address known within another network.
Network	Two or more computers connected together via physical or wireless means.
Network Administrator	Personnel responsible for managing the network within an entity. Responsibilities typically include but are not limited to network security, installations, upgrades, maintenance and activity monitoring.
Network Components	Include, but are not limited to firewalls, switches, routers, wireless access points, network appliances, and other security appliances.
Network Segmentation	Network segmentation isolates system components that store, process, or transmit cardholder data from systems that do not. Adequate network segmentation may reduce the scope of the cardholder data environment and thus reduce the scope of the PCI DSS assessment. See the Network Segmentation section in the PCI DSS Requirements and Security Assessment Procedures for guidance on using network segmentation. Network segmentation is not a PCI DSS requirement.
Non-Consumer Users	Individuals, excluding cardholders, who access system components, including but not limited to employees, administrators, and third parties.
NTP	Acronym for "Network Time Protocol." Protocol for synchronising the clocks of computer systems, network devices and other system components.
PA-QSA	Acronym for "Payment Application Qualified Security Assessor," company approved by the PCI SSC to conduct assessments on payment applications against the PA-DSS.
PAN	Acronym for "primary account number" and also referred to as "account number." Unique payment card number (typically for credit or debit cards) that identifies the issuer and the particular cardholder account.
PAT	Acronym for "port address translation" and also referred to as "network address port translation." Type of NAT that also translates the port numbers.
Payment Application	Any application that stores, processes, or transmits cardholder data as part of authorisation or settlement.
Payment Cards	For purposes of PCI DSS, any payment card/device that bears the logo of the founding members of PCI SSC, which are American Express, Discover Financial Services, JCB International, MasterCard Worldwide, or Visa Inc.
PBX	Acronym for Private Branch Exchange. A Private telephone system typically deployed within an organisation providing private numbering and routing for internal calls.
PCI	Acronym for "Payment Card Industry."
POS	Acronym for "point of sale." Hardware and/or software used to process payment card transactions at merchant locations.

Term	Definition
Private Network	Network established by an organization that uses private IP address space. Private networks are commonly designed as local area networks. Private network access from public networks should be properly protected with the use of firewalls and routers.
Protocol	Agreed-upon method of communication used within networks. Specification describing rules and procedures that computer products should follow to perform activities on a network.
PSTN	Acronym for Public Switched Telephone Network. A meshed global telephone network carrying predominately voice calls.
Public Network	Network established and operated by a telecommunications provider, for specific purpose of providing data transmission services for the public. Data over public networks can be intercepted, modified, and/or diverted while in transit. Examples of public networks in scope of the PCI DSS include, but are not limited to, the Internet, wireless, and mobile technologies.
QSA	Acronym for "Qualified Security Assessor," company approved by the PCI SSC to conduct PCI DSS on-site assessments.
Remote Access	Access to computer networks from a remote location, typically originating from outside the network. An example of technology for remote access is VPN.
Reseller / Integrator	An entity that sells and/or integrates payment applications but does not develop them.
RFC 1918	The standard identified by the Internet Engineering Task Force (IETF) that defines the usage and appropriate address ranges for private (non-internet routable) networks.
Router	Hardware or software that connects two or more networks. Functions as sorter and interpreter by looking at addresses and passing bits of information to proper destinations. Software routers are sometimes referred to as gateways.
RSA	Algorithm for public-key encryption described in 1977 by Ron Rivest, Adi Shamir, and Len Adleman at Massachusetts Institute of Technology (MIT); letters RSA are the initials of their surnames.
RTP	Acronym for Real time Transport Protocol. Part of the IP protocol suite RTP provides timestamps, sequence numbers and is typically used in a media streaming environment such as a VoIP call.
SAQ	An acronym for Self Assessment Questionnaire. Level 2 to 4 Merchants and Level 2 Service Providers can self-certify their PCI DSS compliance through the completion of a SAQ.
SBC	Acronym for Session Border Controller. A device regularly deployed in VoIP networks to exert control over the signalling and sometimes media streams. An SBC may be able to encrypt / decrypt voice calls but the capabilities and configuration of a particular device should be ratified as required.
Security Policy	Set of laws, rules, and practices that regulate how an organization manages, protects, and distributes sensitive information.

Term	Definition
Security Protocols	Network communications protocols designed to secure the transmission of data. Examples of security protocols include, but are not limited to SSL/TLS, IPSEC, SSH, etc.
Sensitive Area	Any data center, server room or any area that houses systems that stores, processes, or transmits cardholder data. This excludes the areas where only point-of-sale terminals are present such as the cashier areas in a retail store.
Server	Computer that provides a service to other computers, such as processing communications, file storage, or accessing a printing facility. Servers include, but are not limited to IP-PBX, web, database, application, authentication, DNS, mail, proxy, and NTP.
Service Provider	Business entity that is not a payment brand, directly involved in the processing, storage, or transmission of cardholder data. This also includes companies that provide services that control or could impact the security of cardholder data. Examples include managed service providers that provide managed firewalls, IDS and other services as well as hosting providers and other entities. Entities such as telecommunications companies that only provide communication links without access to the application layer of the communication link are excluded.
SHA-1/SHA-2	Acronym for "Secure Hash Algorithm." A family or set of related cryptographic hash functions including SHA-1 and SHA-2. See Strong Cryptography.
SIP	Acronym for Session Initiation Protocol. SIP is an IETF-defined signalling protocol widely used for controlling communication sessions such as voice and video calls over Internet Protocol (IP) e.g. VoIP.
SIP TRUNKING	A Multi-call logical signalling link between two SIP Endpoints. Typically used to describe the SIP link between the IP PBX and the VoIP Service Provider.
SRTP	Acronym for Secure Real time Transport Protocol. An encrypted form for RTP.
SSH	Abbreviation for "Secure Shell." Protocol suite providing encryption for network services like remote login or remote file transfer.
SSL	Acronym for "Secure Sockets Layer." Established industry standard that encrypts the channel between a web browser and web server to ensure the privacy and reliability of data transmitted over this channel.

Term	Definition
Strong Cryptography	Cryptography based on industry-tested and accepted algorithms, along with strong key lengths and proper key-management practices. Cryptography is a method to protect data and includes both encryption (which is reversible) and hashing (which is not reversible, or "one way"). Examples of industry-tested and accepted standards and algorithms for encryption include AES (128 bits and higher), TDES (minimum double-length keys), RSA (1024 bits and higher), ECC (160 bits and higher), and ElGamal (1024 bits and higher). See NIST Special Publication 800-57 (www.csrc.nist.gov/publications/) for more information.
TCP	Acronym for Transmission Control Protocol. Provides a reliable connection between IP stations.
TLS	Acronym for "Transport Layer Security." Designed with goal of providing data secrecy and data integrity between two communicating applications. TLS is successor of SSL.
Transaction Data	Data related to electronic payment card transaction.
Trojan	Also referred to as "Trojan horse." A type of malicious software that when installed, allows a user to perform a normal function while the Trojan performs malicious functions to the computer system without the user's knowledge.
Trusted Network	Network of an organisation that is within the organisation's ability to control or manage.
UDP	Acronym for User Datagram Protocol. Part of the TCP/IP protocol set the UDP protocol provides a 'non reliable' method of transmitting data between IP stations. Streaming real time media applications such as a VoIP call typically use UDP as the transmission protocol.
Untrusted Network	Network that is external to the networks belonging to an organisation and which is out of the organisation's ability to control or manage.
VLAN	Abbreviation for "virtual LAN" or "virtual local area network." Logical local area network that extends beyond a single traditional physical local area network.
VoIP	Acronym for Voice Over Internet Protocol. The framework for using an IP network for the transmission of voice and video data.
VPN	Acronym for "virtual private network." A computer network in which some connections are virtual circuits within some larger network, such as the Internet, instead of direct connections by physical wires. The end points of the virtual network are said to be tunneled through the larger network when this is the case. While a common application consists of secure communications through the public Internet, a VPN may or may not have strong security features such as authentication or content encryption. A VPN may be used with a token, smart card, etc., to provide two-factor authentication.
WAN	Acronym for "wide area network." Computer network covering a large area, often a regional or company wide computer system.

Term	Definition
Web Application	An application that is generally accessed via a web browser or through web services. Web applications may be available via the Internet or a private, internal network.
Web Server	Computer that contains a program that accepts HTTP requests from web clients and serves the HTTP responses (usually web pages).

7 Annex A – Carrier Options and their Implications

7.1 ISDN and POTS (Analogue)

The PCI Security Standards Council have clearly indicated for some time that ISDN/POTS lines can be assumed to be PCI DSS Compliant

Traditional phone lines usually connect directly to the voice telecommunications carrier and are therefore considered private as no-one else can access them. As a result PCI considers these to be secure and you will not need to protect the calls further. Private lines are not subject to control under requirement 4.1 of PCI DSS.

Are digital leased lines considered public or private? (FAQ 1068)

For PCI DSS requirement 4.1, digital leased lines are considered to be private since they are dedicated to the individual customer's traffic.

7.2 VoIP over an Untrusted Network

Unencrypted VoIP (or not strongly encrypted VoIP) over an Untrusted Network is NOT PCI DSS Compliant.

This type of connection exposes unprotected VoIP traffic to an untrusted network. As calls are not protected by encryption or other means, these calls can be unilaterally intercepted. These make them vulnerable to eavesdropping and data theft.

This type of connection is not suitable for use if cardholder data is present and must not be used.

7.3 VoIP over a Proven Private Network

VoIP over a ***Proven Private Network*** is considered PCI DSS Compliant.

If you have this type of link you have leased a private line (i.e. dedicated for your own use) between your premises and the premises of your voice telecommunications provider. It may be the case that this line has some insecure aspects. Because of this you **must gain assurance** from the company you lease this line from that it is secure. If you gain this assurance you are not required to take any further action as you have a Proven Private Network, which is where a service provider **has given guarantees** that the underlying transmission circuit is secure.

For this reason security is ensured and the connection is not considered subject to PCI DSS Requirement 4.1. If the service provider cannot give this guarantee then the connection should be considered open and unprotected.

7.4 Encrypted VoIP over an Untrusted Network

Encrypted VoIP over an Untrusted Network can be PCI compliant if appropriately configured.

All VoIP calls are made up of two components, namely the call signalling, to set up and control the call, and the call media (voice) stream.

A VoIP call can be made using a carrier service which encrypts the signalling and media streams created by the telephony infrastructure. This is an encrypted VoIP call.

In technical terms an example of this is the VoIP signalling protocol SIP, running over a TLS connection with SRTP media. Both TLS and SRTP need to provide the protection levels stipulated by PCI DSS Requirement 4.1.

In order to perform this type of encrypted VoIP call, as an entity you must ensure that your IP-PBX (phone system) supports SIP/TLS with SRTP. If this method is not supported by the IP-PBX there are voice gateway devices called Session Border Controllers (SBCs) available to carry out this function. Your PCIDSS Level-1 Service provider may provide SBCs for this purpose as part of their PCIDSS Level-1 service.

Check with your IT department or phone system maintainer that an appropriately strong level of encryption is being used.

Before entering into any contract with a service provider, it is essential to assure yourself that the service is compliant with requirements 1, 2 and 5 through 12. It is your responsibility to ensure that your equipment, systems and processes are compliant with requirement 4.1.

7.5 VoIP over a VPN

VoIP over a VPN can be PCI Compliant if the VPN is appropriately configured.

Any VoIP service that uses the internet or other open public networks to connect you to your voice telecommunications provider will be susceptible to malicious attack. For this reason if you are using this type of service, you must ensure that you protect your calls using encryption.

This type of connection takes the VoIP call traffic between the telecommunications carrier and your telephone infrastructure and protects its transmission over the link by using a classic network level virtual private network (VPN). Classic network level VPN is a virtual wide area network (WAN) link created by firewalls establishing an encrypted connection between them. You must ensure that the VPN provides a strong encryption level adhering to PCIDSS standards and the infrastructure providing the VPN must be protected.

The level of protection stipulated by PCI DSS Requirement 4.1 and the infrastructure providing the VPN service will need to meet PCI Requirements 1, 2 and 4 through 12.

8 ANNEX B – TELEPHONY TECHNOLOGIES AND THEIR IMPLICATIONS

8.1 NETWORK SEGMENTATION AND THE LOCAL AREA NETWORK

VoIP bearing networks with cardholder data must be segregated from other non CDE networks. This segregation can be made using separate physical network components, or by use of network firewalls. Network firewalls must be themselves protected with controls.

8.2 LAN SWITCH

A Local Area Network (LAN) switch is a device used to connect computer devices together using cables to form a network. In telephony the LAN switch is used to connect telephone system components such as the PBX, IVR and (VoIP) telephone handsets[3] and enables them to communicate between each other. When receiving cardholder details via the phone the LAN switch which connects these components together will be transmitting cardholder data. For this reason it comes under the scope of PCI DSS and requires you to ensure that it is secured from malicious attack. For guidance on securing your LAN switch see recommended PCI DSS requirements below.

LAN Switches should be protected under PCI DSS requirements 1, 2, 5 through 12

8.3 HANDSETS

8.3.1 IP Handsets

Where calls are delivered to a VoIP handset and the call contains cardholder data then the VoIP handset is in scope for PCI as again it could be maliciously attacked. For guidance on securing your IP handset see recommended PCI DSS requirements below.

IP Handsets should meet PCI Requirements 2, 5, 7 and 8. If bespoke development is carried out on the handsets Requirement 6 would also apply.

8.3.2 Softphones

Rather than using IP handsets your company may use softphones whereby staff have headsets connected to their workstations in order to answer phone calls. Because the workstation is processing cardholder data via the phone call, the workstation for the same reason as the IP handset becomes in scope of PCI DSS. You are therefore required to implement controls to ensure its protection again malicious attack. See box below for guidance.

User access control and privilege restrictions should prevent users from installing and configuring unauthorised IP softphones and tools including Skype, IM voice calling on their workstations. Unauthorised softphone software may allow attackers to enable the local PC microphone and listen in to the user's conversations. Make sure your Acceptable Use Policies restricts use of these tools and limit voice calling to your centrally managed corporate VoIP solution.

Workstations on which softphones operate should be protected under PCI DSS requirements 1, 2, 5 through 12

[3] a telephone handset designed to operate on an Internet Protocol based Local Area Network

9 ANNEX C – CALL AND SCREEN RECORDERS AND THEIR IMPLICATIONS

9.1 SCREEN AND CALL RECORDERS

Beyond the call recordings it is also important to consider the call recorder. Most trunk side and agent side call recorders are within the call path for the totality of the call. If the call recorder is exposed to cardholder data, even if the call recorder at that time is not call recording, the call recorder is in scope for PCI.

Again for screen recordings storage of cardholder data must comply with PCI Requirement 3. If screen images are not broadcast to the screen recorder at the time of the agent entering cardholder data then the screen recorder will be out of scope of PCI.

As described within the cardholder data journey for a Telephone Order it is necessary to consider both the call recorder and the call recordings when considering PCI Compliance. With this said it is important to comply with PCI Requirement 3 for call recordings. The following will recap what was published in December 2010 in the Information Supplement 'Protecting Telephone-based Payment Card Data'. Since the publication numerous tools and techniques have become available to ensure that merchants do not need to store SAD data on call recordings.

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 authorisation even if encrypted.

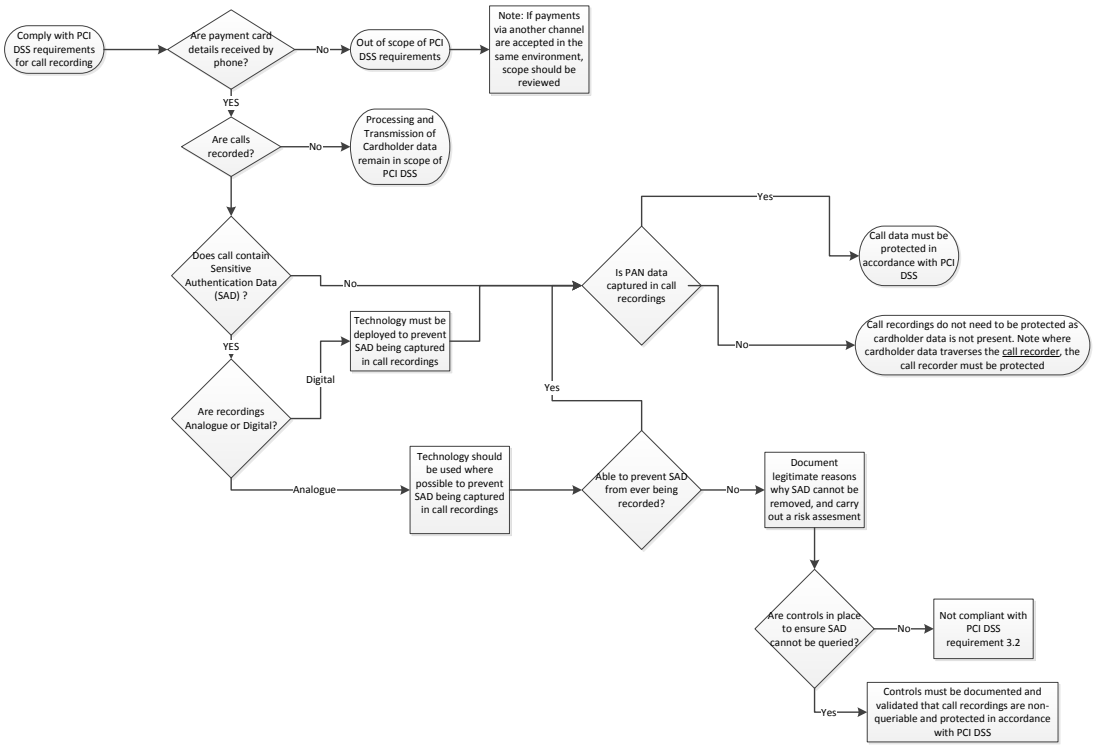
It is therefore prohibited to use any form of digital audio recording (using formats such as WAV, MP3, etc.) for storing CAV2, CVC2, CVV2 or CID codes after authorisation if that data can be queried; recognising that multiple tools exist that potentially could query a variety of digital recordings.

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 authorisation 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 flow chart below shows the process a merchant should follow when assessing the risk for their call centre operations and aims to clarify the FAQ above.


Comply with PCI DSS requirements for call recording
Are payment card details received by phone?
No
Out of scope of PCI DSS requirements
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 of PCI DSS
Does call contain Sensitive Authentication Data (SAD) ?
No
Is PAN data captured in call recordings
Yes
Call data must be protected in accordance with PCI DSS
No
Call recordings do not need to be protected as cardholder data is not present. Note where cardholder data traverses the call recorder, the call recorder must be protected
YES
Are recordings Analogue or Digital?
Digital
Technology must be deployed to prevent SAD being captured in call recordings
Yes
Analogue
Technology should be used where possible to prevent SAD being captured in call recordings
Able to prevent SAD from ever being recorded?
No
Document legitimate reasons why SAD cannot be removed, and carry out a risk assesment
Are controls in place to ensure SAD cannot be queried?
No
Not compliant with PCI DSS requirement 3.2
Yes
Controls must be documented and validated that call recordings are non-queriable and protected in accordance with PCI DSS

* Flowchart Notes

Sensitive Authentication Data must not be able to be queried. Note all voice and video CODEC formats are deemed to be able to be queried. Data that is able to be queried 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 data is not sufficient to render the data as not being able to be queried.*

For data to be considered "*not being able to be queried*" it must not be feasible for users of the system or malicious users that gain access to the system to retrieve or access the data or for malicious users having gained access to use commonly available tools for data mining purposes. Access to the types of functions listed above must be extremely limited, documented, and actively monitored. Additionally, controls must be in place to prevent unauthorized access to these functions.

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.

10 Annex D – Methods of Masking Cardholder Data

10.1 Pause And Resume

Call recorders can be paused during the communication of cardholder data from the caller to the agent and call recording resume thereafter. This can be achieved by the agent manually pausing the call recording or automatically through Computer Telephony Integration (CTI) triggers.

10.1.1 Manual Pause And Resume

Careful consideration is required when using this technique. There is a high risk that the process to pause and resume a call recording is not rigorously followed by the agent. Where manual pause and resume is implemented, it is essential to periodically audit call recordings to confirm that PAN and CVV2 data is not being captured. Note Call recordings with only PAN data (i.e. no CVV2) can be protected through encryption as defined within PCI DSS. If CVV2 data is discovered through the audit process an alternate method for not recording CVV2 data should be deployed.

Manual pause and resume has further complications from a business perspective in that agents are at liberty to cease call recording at will and therefore can abuse this system. Furthermore legal regulations in certain industries would preclude such capabilities. Finally when submitting call recordings in a court of law, where such pause and resume capabilities are available, may impact the validity of the evidence.

10.1.2 Automatic Pause and Resume

Triggers can be added within Agent applications to both pause and resume call recordings when entering and exiting payment screens / payment fields. Call recordings should be periodically audited to confirm that PAN and CVV2 data is not being captured. Note that following agent application changes, triggers should be tested to confirm that they are still active and in place.

10.2 DTMF Tone Masking

This method separates the keypad tone signals from the voice stream allowing the tones to be processed automatically while the call centre agent continues the discussion with the customer. There are a number of service providers offering different ways of achieving this result, which removes the call centre from the scope of PCI DSS as no cardholder data.

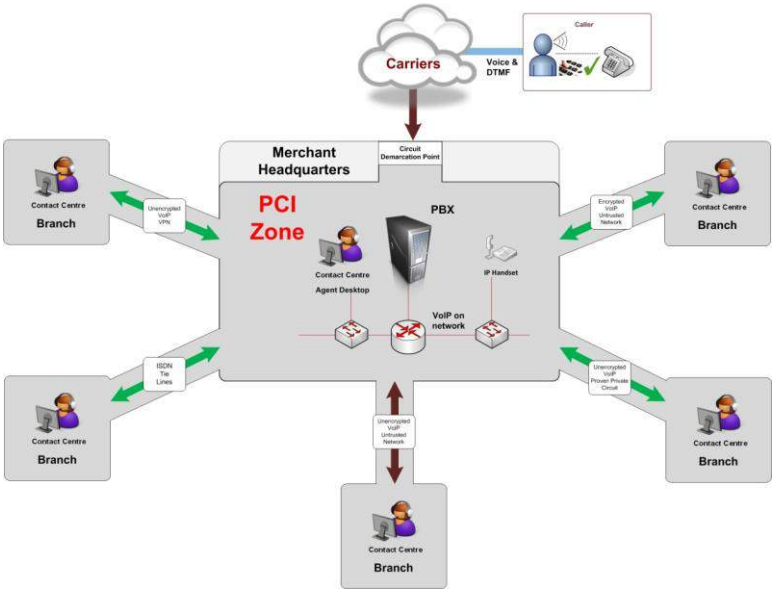
You must make sure that DTMF screening services cover both received calls and placed calls to customers. In the case where inbound calls are screened for DTMF and DTMF is masked, then this removes the call centre from the scope of PCI DSS as no cardholder data. However in the case where outbound calls are also placed to customers, you must make sure that your screening service is also active, otherwise the call center is in scope of PCI DSS as calls can contain cardholder data and the site must be protected.

11 ANNEX E – IMPLICATIONS FOR MULTI-SITE ORGANIZATIONS

11.1 OVERVIEW

If you forward telephone calls between sites and if you have a business practice of accepting card payments over the phone then the links between your offices are in scope of PCI DSS. Since you have control of how these sites are connected together and since the links transmit cardholder data you must select a method that is PCI DSS compliant.

The following diagram depicts various ways you could forward calls between sites.



11.2 CALL FORWARDING VIA THE PSTN

Call forwarding via the PSTN is in scope for PCI DSS

If you divert an incoming phone call to another office by forwarding back via the PSTN then the PSTN connection should be considered in scope of PCI DSS as discussed in section 2.2.1.1.

11.3 ISDN TIE LINES

ISDN Tie lines can be considered PCI Compliant

An ISDN Tie line is a telecommunication link between internal phone systems and is considered private. Private lines do not require you to take any further action to ensure their security.

11.4 VOIP OVER VPN

VoIP over a VPN can be PCI Compliant if the VPN is appropriately configured.

Treated the same as 7.5.

11.5 ENCRYPTED VOIP OVER AN UNTRUSTED NETWORK

Encrypted VoIP over an Untrusted Network can be PCI compliant if appropriately configured.

Treated the same as 2.2.1.4.

11.6 VoIP over a Proven Private Network

VoIP over a Proven Private Network can be PCI DSS compliant.

Same as 7.3.

11.7 VoIP over an Untrusted Network

VoIP over an Untrusted Network is NOT PCI DSS Compliant.

Treated the same as 7.2.

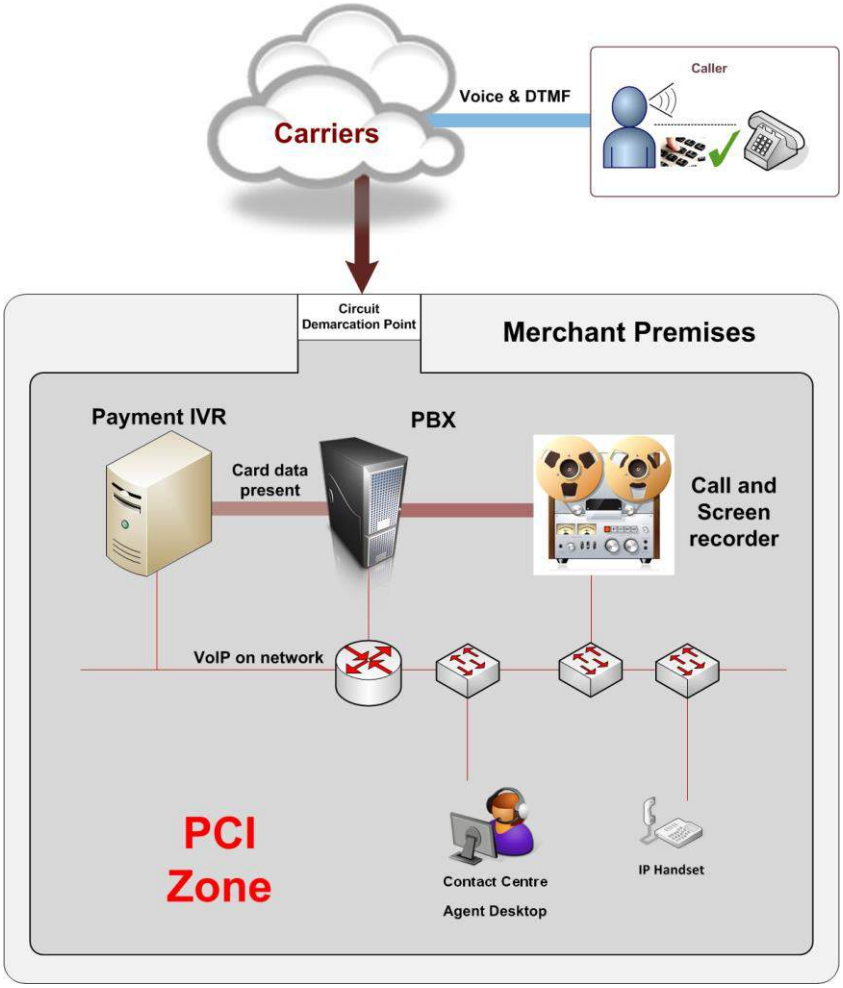
This type of connection is not suitable for use if cardholder data is present and should not be used.

12 ANNEX F – EXAMPLE IMPLEMENTATION SCENARIOS

12.1 PAYMENT IVR

If a merchant uses an automated payment IVR collecting cardholder data either by voice or through DTMF tones then the automated payment IVR is in scope for PCI.

Sensitive Authentication Data (SAD) as in the CVV2/CVC2/CID/CAV2 must not be included in any logs as per Requirement 3.2. PAN data is only allowed in such logs if all logs are encrypted and meet PCI Requirement 3. A merchant's automated payment IVR in scope for PCI should satisfy PCI Requirements 1, 2 and 5 through 12.



Where an IVR is being used to allow for self-service payment transactions the cardholder will be sharing their details with the IVR either via voice recognition software, or by using their telephone keypad transmitting the digits as DTMF tones. In either case the IVR is receiving and processing cardholder details and so is in scope of PCI DSS.

If the IVR is on your premises then the network that is routing the cardholder data to the IVR also needs to be considered for PCI compliance as it is carrying cardholder data.

Automated Payment IVRs should comply with PCI Requirements 1 through 12.

Some organisations capture cardholder data as part of their ID&V process, for example a bank soliciting debit card number for identification of an account holder. Any systems

involved in the transmission, processing or storage of any cardholder data is in scope for PCI. This includes IVRs (both DTMF tone and speech recognition) and Computer Telephony Integration (CTI) where the latter passes cardholder data as attached data to an agent desktop or CRM client session.

12.2 Assisted Outbound Dialling

An outbound call may contain cardholder data and as such remains in scope for PCI DSS.

Outbound calling may be assisted by an Autodialler. An Autodialler integrates into the telephone and CRM environment connecting customers with Agents in an efficient manner.

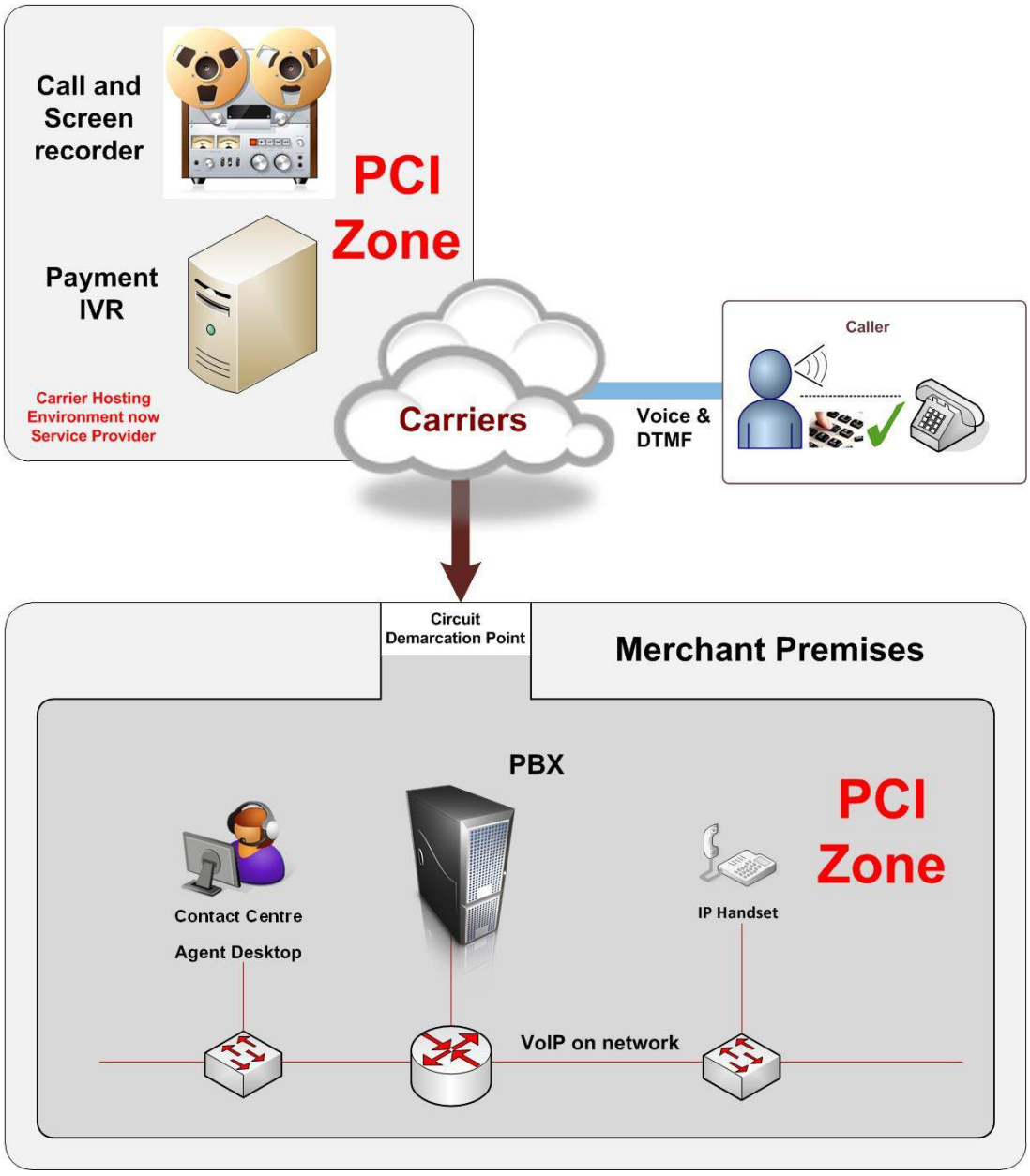
If the dialler is only involved in the call setup and is never involved in the call while cardholder data is shared then, depending upon the network segmentation, it may be out of scope for PCI DSS and you will not need to apply any security controls to it.

If the Autodialler does not come in to contact with Cardholder data and cannot via re-configuration come in to contact with cardholder data, then it is out of scope of PCI DSS.

If the Autodialler comes in to contact with cardholder data, for example, call signalling or unencrypted call media flows through it - when card data is transmitted, then it is in scope with PCI DSS and subject to controls and protection.

Outbound diallers in scope for PCI DSS should comply with PCI Requirements 1,2 and 5 through 12.

12.3 HOSTED SERVICES & SERVICE PROVIDERS



Service providers must be managed in accordance with Requirement 12.8.

PCI DSS applies directly to service providers that store, process, transmit cardholder data in the provision of services to merchants due to the nature of their business: "PCI DSS applies to all entities that store, process or transmit cardholder data". Where merchants are using these service providers, the service provider has an independent responsibility to be compliant. Until they become compliant, those services must be considered part of the merchant's PCI DSS scope.

If a merchant uses hosted telephony services including but not limited to IVR, Automated Payment IVR, ACD, PBX, Auto-dialling, call recording and screen recording and as defined within this guideline these devices are in scope for PCI DSS then the hosted provider is defined within PCI DSS as a Service Provider. As such, if the Service Provider is transmitting, processing or storing in excess of 300,000 transactions (or a component of

such a transaction i.e. any process which uses cardholder data) for Visa or MasterCard then the Service Provider will be classified as a Level 1 Service Provider.

As a Level 1 Service Provider it will need to obtain a QSA certified Report of Compliance (RoC) and provide the merchant with an Attestation of Compliance (AoC) which includes within the section 2a "Services Provided that were included in the Scope of the PCI DSS Assessment". Merchants have the obligation to ensure that the services covered by the RoC include all in scope PCI elements provided by the Service Provider. Furthermore, the merchant has the obligation to confirm annually that the Service Provider is up to date with its PCI certification and that the scope of the RoC covers all PCI aspects of their service. Service Providers processing less than 300,000 transactions annually with Visa or MasterCard can self-certify (through a Self-Assessment Questionnaire SAQ). A merchant must use a PCI DSS compliant service provider. A merchant must check that any service providers they use are listed on Visa-Europe's Merchant agent website.

Merchants have the obligation to ensure that the services provided to them are included in the service providers own PCI DSS assessment and to understand the PCI DSS responsibilities they retain as the result of outsourcing services to a service provider. Use of a PCI DSS compliant service provider does not result in PCI DSS compliance for the service provider's clients (the merchant).