Security Standards Council®

Version: 3.0

Date: November 2018

Author: Protecting Telephone-Based Payments Special Interest Group

PCI Security Standards Council

Information Supplement:

Protecting Telephone-Based Payment Card Data

Document Changes

Date	Document Version	Description
March 2011	2.0	Initial release.
November 2018	3.0	Updated by PCI Special Interest Group.

Contents

1. Introduction

The Payment Card Industry Data Security Standard (PCI DSS) defines security controls to protect payment card data throughout the transaction lifecycle. PCI DSS requirements apply across all payment-acceptance channels, including mail order/telephone order (MOTO).

This document provides supplemental guidance, which does not add, extend, replace, or supersede PCI DSS requirements. The PCI Security Standards Council (PCI SSC) is not responsible for enforcing compliance or determining whether a particular implementation is compliant. Entities and third-party service providers should work with their acquirers and/or payment card brands to understand their compliance-validation and reporting responsibilities.

This document focuses exclusively on securing telephone-based payment card data including an entity's transition to voice-over-IP (VoIP) based communications. This is particularly relevant for entities in locations where established national carriers have announced transition plans to move away from Integrated Services Digital Networks (ISDN) and public switched telephone networks (PSTN) toward the exclusive provision of VoIP services. Where possible, the document uses simple language and diagrams to explain the risks and vulnerabilities associated with telephone-based payment environments and provides guidance on how to secure them irrespective of the size or capabilities of the telephony environment. This document does not provide guidance on the types of technology that should be used to meet an entity's business requirements.

A quick guide to navigating the document is provided in Appendix B, "Document Quick-reference Guide."

1.1 Objective

This Information Supplement provides guidance for today's telephone-payment environments—whether merchant, service provider, or vendor—to better manage the risk of fraudulent activity in this essential payment-service area. Written for a wide range of merchants, from small businesses to large contact centers, it allows the reader to understand the risks and security challenges associated to their telephone environment. This document also provides many hypothetical scenarios to help clarify how PCI DSS requirements can be applied to telephony technologies and to illustrate appropriate methods to address identified risks and challenges.

1.2 Audience

This document provides guidance for entities of all sizes and complexity that store, process, or transmit account data over the telephone. It is assumed that the reader has a basic knowledge of or experience in telephony and payment systems. A glossary of terms is provided in Section 1.4 for readers with limited knowledge or experience in these domains.

The intended audience includes, but is not limited to:

- Entities, such as merchants, that use telephony as a card-acceptance payment channel.
- Entities such as merchants, customer-service centers, call centers or contact centers that outsource or are considering outsourcing telephony payment acceptance to a third-party service provider.

- Service providers that accept payments over the telephone or manage transactions on behalf of merchants or other entities.
- Technology vendors providing, maintaining, and/or managing telephone payment systems.
- Providers of telephony services—e.g., interactive voice response (IVR) or Dual-Tone, Multi-Frequency (DTMF) masking/suppressing.
- Qualified Security Assessors (QSA) and Internal Security Assessors (ISA) that support these entities.
- Acquirers, payment service providers, and payment gateways that support relevant entities.
- Card issuers that support the secure distribution of payment cards to cardholders.

1.3 Using the document

This document covers the fundamental principles associated with applying PCI DSS requirements and other best practices for securing telephone-based payment card account data in a telephony environment. More specifically, this document:

- Considers why securing telephone-based account data is important.
- Provides clear statements on PCI DSS scope in both simple and complex telephony environments. This approach is intended to support the full range of environments, telephony systems, and supporting technologies that entities use to accept telephone-based payments.
- Provides guidance on documenting account data flows for a telephone-based cardholder data environment (CDE).
- Considers applicability of PCI DSS requirements to simple and complex telephone environments.
- Provides guidance on using third-party service providers for supporting telephone-based payments.
- Provides guidance on using methods that may help minimize the amount of account data in each type of telephone.

This document uses several Appendices:

Table 1 – Guidance appendices

Appendix	Description
A	Glossary to help the reader through the range of telephony-related terms and acronyms used in the document.
B	Quick Guide to using this guidance.
C	Process chart allowing the reader to identify their telephone environment and scope-reduction technologies they may want to consider.
D	High-level call-recording decision-making process.
E	Impact of VoIP on scope.
F	Further scoping considerations and how they should be assessed.
G	List of helpful and related reference materials published by the PCI SSC. Using these references alongside this document is strongly recommended.
H	The list of the organizations that contributed to this document.

1.4 Terminology

A number of terms used in this document are defined in the Payment Card Industry (PCI) Data Security Standard Glossary, Abbreviations and Acronyms https://www.pcisecuritystandards.org/pci_security/glossary). Telephony-specific terms are available in the document's glossary (Appendix A).

In addition to the telephony-related terms and acronyms detailed in Appendix A, the following PCI DSS terms and acronyms are used throughout this document:

Table 2 – Payment card data

Account Data	
Cardholder Data (CHD) includes:	**Sensitive Authentication Data (SAD) includes:**
▪ Primary Account Number (PAN) ▪ Cardholder Name ▪ Expiration Date ▪ Service Code	▪ Full track data (magnetic-stripe data or equivalent on a chip) ▪ Card verification code: CAV2/CVC2/CVV2/CID ▪ PINs/PIN blocks

2 Setting the Stage

2.1 The Risk of Fraud

For card-not-present (CNP) fraud, a criminal only needs to obtain the PAN, cardholder name, expiry date and, sometimes, the card verification code as defined in Section 1.4. All of these data elements, as well as additional personally identifiable information such as, but not limited to, postal code and shipping address are data elements provided by the cardholder during a telephone transaction. The PIN or full track data are not used in the context of CNP.

The working environment in which telephone-based transactions are received provides numerous opportunities for compromising payment card data both externally by criminals gaining access to systems and software and internally via personnel with malicious intent handling the calls. Personnel receiving account data through a telephone handset or via a computer screen could use a variety of techniques to acquire and record this data, from simply writing the details into a book or mobile device to utilizing key-logging or recording equipment. In addition, audio signaling can be captured in transit, and it is trivial for an attacker to convert audio into queryable data.

Risk-mitigation technologies such as EMV chip cards have helped to significantly reduce card-present fraud rates. As a result, criminals are increasingly looking to exploit CNP channels such as mail order/telephone order and e-commerce. Telephone-based payments represent an area of opportunity for fraud—as this method of payment exposes account data in the clear—and must be given full consideration in any security strategy and PCI DSS compliance program.

2.2 People, Process, and Technology

This document rests on three pillars: people, process and technology. As we will see in the subsequent chapters, after identifying the type of telephone-based payment one is operating, it is important to recognize the risks associated with people in such an environment, the impact they can have on the overall security of payment card data, and how to prevent or reduce these risks. The processes related to people, whether to manage them or their activities, need to be adapted to the environment and the role performed by each group of staff members. The technology needs to support the processes and the people in preventing or reducing the risks to payment card data.

2.3 PCI DSS Applicability to Telephony Environments

PCI DSS applies to all system components included in or connected to the cardholder data environment (CDE). The CDE is comprised of people, processes, and technologies that store, process, or transmit cardholder data or sensitive authentication data.[1]

Accepting spoken account data over the telephone puts personnel, the technology used, and the infrastructure to which that technology is connected into scope of PCI DSS.

[1] Refer to the section “Scope of PCI DSS Requirements” in PCI DSS.

Telephone environments can vary enormously in size and complexity from a small merchant in a simple telephone environment or reception desk where payments are taken over a single telephone line, to a large, complex, multi-site environment or call center operation able to process hundreds of card payment transactions simultaneously. The following sections describe the applicability of PCI DSS requirements to both simple and complex telephony environments.

2.3.1 Simple Telephone Environments

For the purposes of this document, a simple telephone environment is an environment where an entity (e.g., a merchant) receives account data via a single or limited number of telephone lines. Payment processing in simple telephone environments often occurs using payment channels such as a dial-up payment terminal or a virtual terminal. Entities processing telephone payments in this way should consider how customer account data is secured.

Scenario 1 – Traditional telephone line

Generally speaking, entities are not considered responsible for the transmission of card data over an external traditional telephone line (also described as “plain old telephone service,” or POTS), as the risk of man-in-the middle attacks on data transmissions over these lines is considered low.

Diagram 1 below shows a simple telephone environment where account data is spoken over a traditional POTS telephone line.

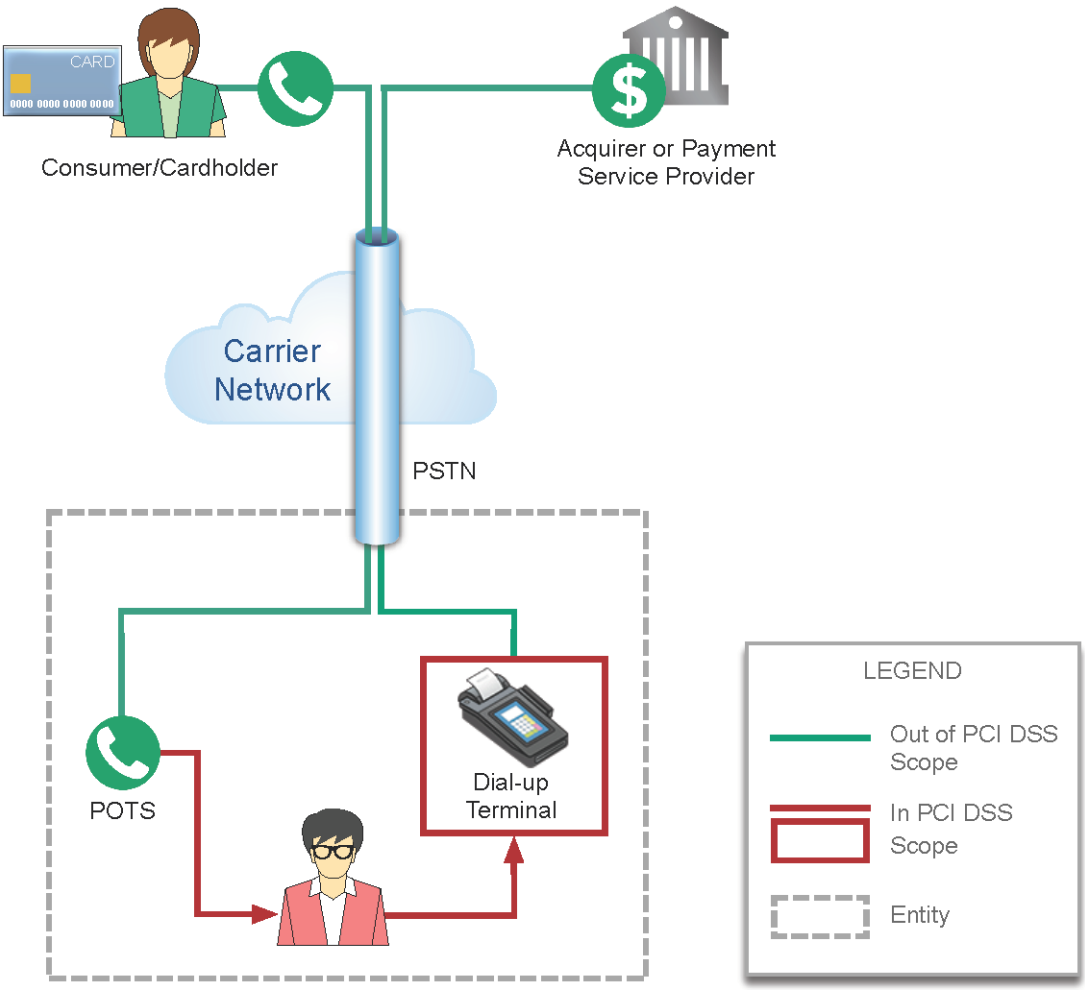


Diagram 1: Simple telephone environment using single PSTN telephone line

Transmissions between an entity and an acquirer/payment service provider (PSP) over a public telephone line or public switched telephone network (PSTN) are generally considered out of scope for PCI DSS. However, should the entity use an answering machine to capture customer account data or the person answering the call writes down the account data, then the collection of account data in the scenario would be considered "storage," and the entity's processes and environment would be considered in scope for PCI DSS.

If the payment terminal illustrated in Diagram 1 connects to the Acquirer/PSP via Internet Protocol (IP), this connection may also be considered in the scope of PCI DSS. See Appendix F, Section F.3, "Simple Telephone System – Further Examples," for more information.

Scenario 2 – Call transferred to a call center service provider

Diagram 2 below shows another example of simple telephone environment, this one using a call center service provider. In this example, the entity does not collect any payment or account data, but transfers the call to a call center service provider to handle the payment.

In this scenario the switching method within the entity's environment remains in scope of PCI DSS. If the entity has the ability to record account data, the account data will need to be protected in accordance with applicable PCI DSS requirements.

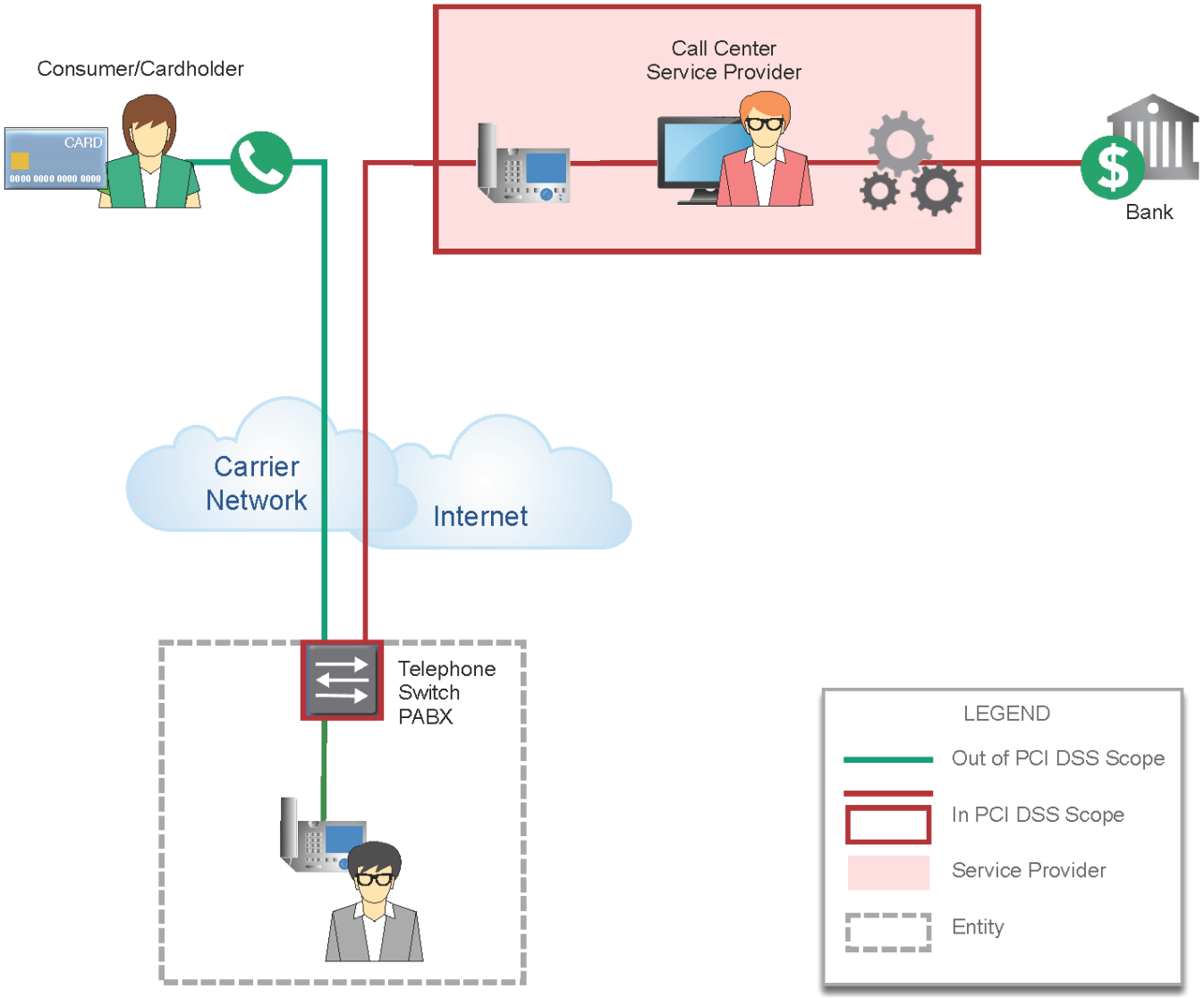


Diagram 2: Simple telephone environment with call center service provider

Where account data is received by the entity via POTS then transmitted over an IP-based or public network to an acquirer or PSP or manually entered or stored on an entity's system, PCI DSS requirements for the protection of customer account data would also apply.

Where VoIP is used for transmissions of payment card account data between a cardholder and an entity, the entity's systems and networks used for those transmissions are in scope. Securing the VoIP transmission outside of the entity's infrastructure is not considered within the entity's scope, as the entity cannot control the methods used by the cardholder to make and receive phone calls. This applies regardless of whether the transmissions are initiated by the entity or the cardholder. For further

information on the how PCI DSS applies to VoIP please see FAQ #1153 “How does PCI DSS apply to VoIP?”

2.3.2 Complex Telephone Environments

Complex environments generally utilize numerous agents that are linked to systems and servers. Often this type of environment is a customer service center or call center.

The use cases illustrated in Diagrams 3, 4, and 5 offer general examples of how PCI DSS scope applies to complex telephone environments.

2.3.2.1 Environment with no payment card data

Diagram 3 represents a telephone environment where no CHD is collected (i.e., no card data is given to the entity by the customer using a telephone) or before the CHD is provided. In this scenario, no component or system is in scope for the entity’s PCI DSS.

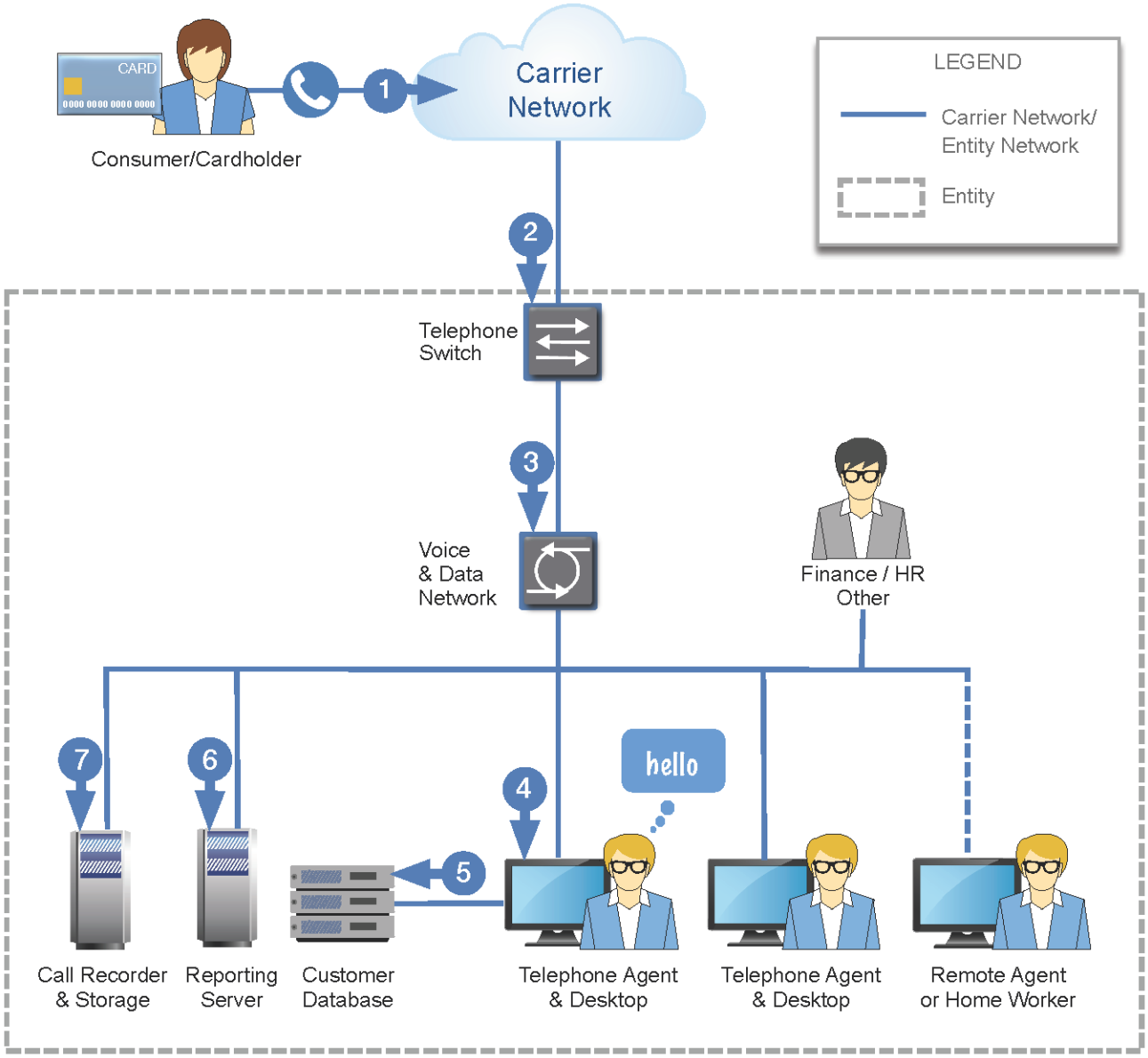


Diagram 3: Typical complex telephone environment and call flow prior to CHD being present.

Table 3 – Call flow prior to CHD being present

Step 1:	*The customer makes a call to the entity.*
Step 2:	*The call traverses the carrier network, the telephone switch answers and directs the call to an available agent.*
Step 3:	*The entity's voice and data network transmit the call to the agent.*
Step 4:	*The agent answers the call and interacts with the customer.*
Step 5:	*The agent enters data into the customer database.*
Step 6:	*The event is reported.*
Step 7:	*The call is recorded, and the recording is stored.*

2.3.2.2 *Impact of payment card data collection on PCI DSS scope*

Diagram 4 shows the impact of the collection of account data in terms of PCI DSS scope when the customer (cardholder) provides cardholder data (CHD) and sensitive authentication data (SAD) to the entity. Account data is transmitted and received within the telephone environment, processed by the entity, and stored. The systems within this environment are in scope for the PCI DSS as the systems (now represented in red) have the potential to store, process, or transmit account data.

Systems, devices, or networks within other areas of the business (shown in the diagrams as Finance/HR/Other) as well as any third parties connected to the systems handling CHD may also be in scope for PCI DSS. Carriers providing only access to public networks[2] are generally considered outside the scope of PCI DSS, hence the carrier network in this example represented in green.

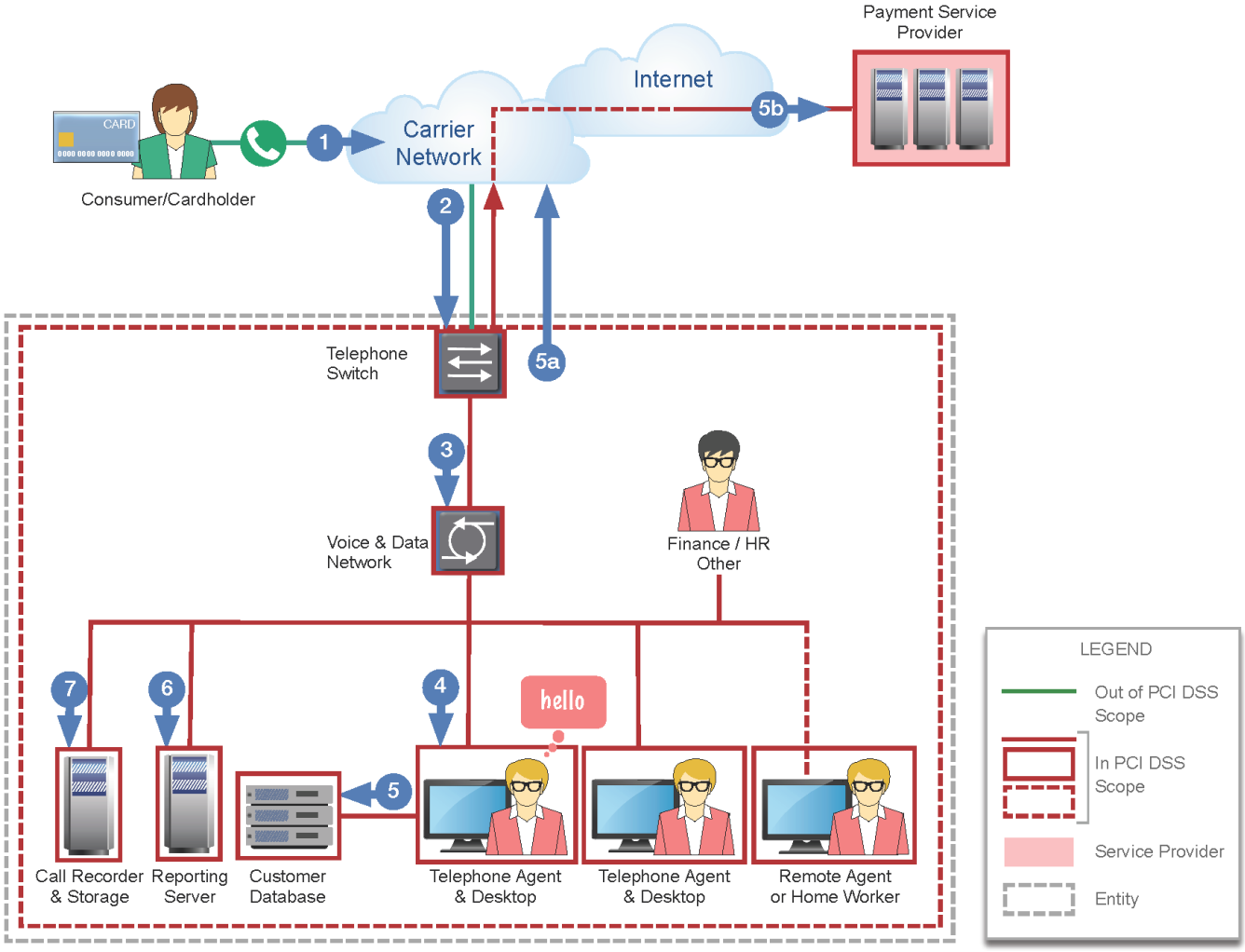


Diagram 4: Telephone environment and call flow where CHD is captured and stored

[2] Carrier networks may be in scope for other types of services. Refer to definition of Service Provider in the online *Payment Card Industry (PCI) Data Security Standard Glossary, Abbreviations and Acronyms* (https://www.pcisecuritystandards.org/pci_security/glossary#S)

Table 4 – Call flow where CHD is captured and stored

Step 1:	*The customer is connected to the agent and call recording has started, as part of the dialogue when asked they provide their account data to the agent, via the carrier network.*
Step 2:	*The spoken account data enters the telephone environment via the telephone switch.*
Step 3:	*The account data is transmitted by the entity's voice and data network to the agent.*
Step 4:	*The agent inputs the CHD into their desktop PC via the keyboard.*
Step 5:	*Customer data is entered into the customer relationship management system (CRM) / Customer Database where it is stored. (It is assumed that no CHD is stored).*
Step 5a:	*The account data is transmitted to the Payment Service Provider (PSP) or acquirer. For example, this may occur via data input into an application on the agent's desktop, via a virtual terminal accessed hosted by the PSP or acquirer over a secure Internet connection from the agent's desktop, or via a physical point of interaction (POI) payment terminal.*
Step 5b:	*The PSP processes and potentially stores the CHD and returns a payment validation reference to the agent desktop or payment terminal.*
Step 6:	*This interaction is recorded on the reporting server.*
Step 7:	*The call-recording equipment attached to the network captures the account data, and the account data is stored in the call-recording storage. Call recording ceases, it is indexed and stored. At this point, call data can be queried.*

2.3.2.3 Identification of the CDE

Diagram 5 focuses on the cardholder data environment shown in Diagram 4, illustrating the potential extent of the CDE within the call center environment (the grayed area with an orange frame).

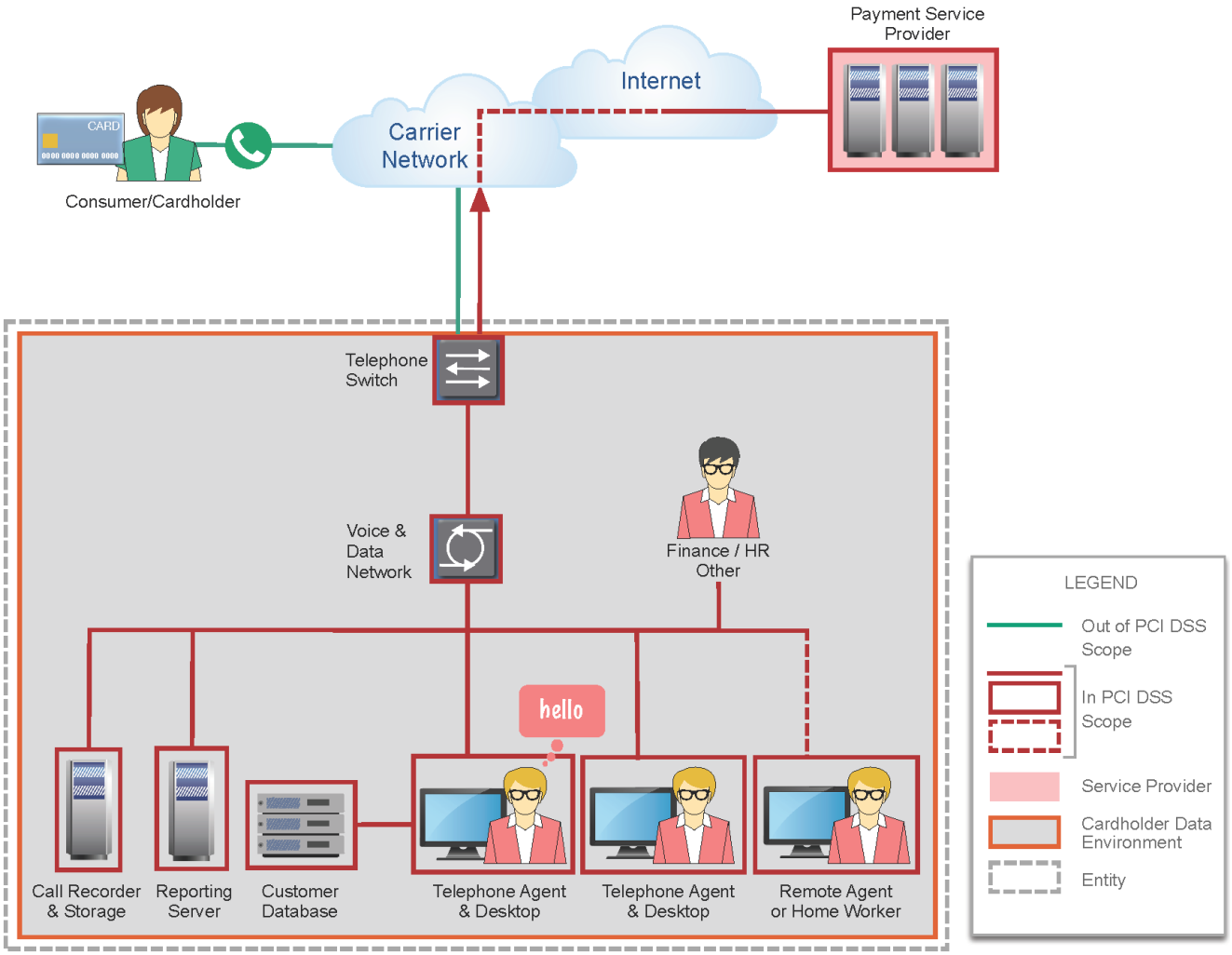


Diagram 5: Cardholder data environment (CDE)

Note: *Each business entity is responsible for determining the extent of its CDE and PCI DSS scope of its environment.*

2.4 Telephony Considerations and Demarcation Points

To fully understand the extent to which an entity's telephony environment is in scope for PCI DSS, one must first identify the key demarcation points within the telephony environment that separate the services provided by the entity and any supporting services provided by third-party service providers. Consider the following definition of a service provider provided in the PCI SSC Online Glossary[3]:

> [A] *business entity that is not a payment brand, directly involved in the processing, storage, or transmission of cardholder data on behalf of another entity. 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. If an entity provides a service that involves only the provision of public network access—such as a telecommunications company providing just the communication link—the entity would not be considered a service provider for that service (although they may be considered a service provider for other services).*

Table 5 provides some example scenarios involving the use of third-party service providers, how the use of those service providers may impact an entity's PCI DSS scope, and some additional factors that should be taken into consideration:

Table 5 – Scope for service providers

Entity	Scenario	In scope for PCI DSS?	Additional factors that may impact scope
Telecommunication companies (telco)	The entity supplies access to public network (analog, digital, and/or IP telephony based), only supporting the point-to-point distribution of call traffic.	Considered out of scope	Some telecommunication equipment owned and operated by the telco, hosted within the entity's infrastructure for the purpose of provisioning access to public network, may be considered in scope for PCI DSS.
One or several service providers (possibly including a telco) providing services such as, for example: IVR, call recording, SIP trunking.	The entities provide a service involving processing, transmitting, or storing account data on behalf of the entity or affecting the security of payment card data.	Considered in scope	The telco or service providers should have their own PCI DSS validation covering the services they provide, or they would need to be included in the entity's PCI DSS assessment. All the relevant service providers should be included in the telephony dataflow. A clear understanding of where the responsibility of each service provider for securing the telephony infrastructure starts and ends, using diagrams that include clearly marked service demarcation points.

[3] Online Glossary: https://www.pcisecuritystandards.org/pci_security/glossary#S

Documenting clear demarcation points for all supporting services and defining the moment in the call flow at which the entity takes responsibility, helps the entity define its CDE.

If at any point an entity stores, processes, or transmits account data within its environment, the entity's systems and networks through which the account data is stored, processed, or transmitted fall within the scope of the PCI DSS, and applicable PCI DSS Requirements must be met irrespective of the type of network the entity has deployed. For example, a VoIP network transmitting account data would be subject to the same PCI DSS requirements as would an internal IP-based network that transmits account data. Additionally, PCI DSS Requirement 4.1 would apply wherever account data is transmitted over a shared or public VoIP service.

Where "voice" traffic from the public telecommunications network (i.e., carrier) terminates on equipment owned and operated by the entity or a service provider and is then sent (regardless of whether it is analog, digital, or VoIP transmission) to a third-party service provider, the demarcation point is the equipment owned by the entity or the third-party service provider and should be considered in scope for PCI DSS. This scenario is represented by the Virtual Private Branch Exchange (PBX) system in Diagram 6.

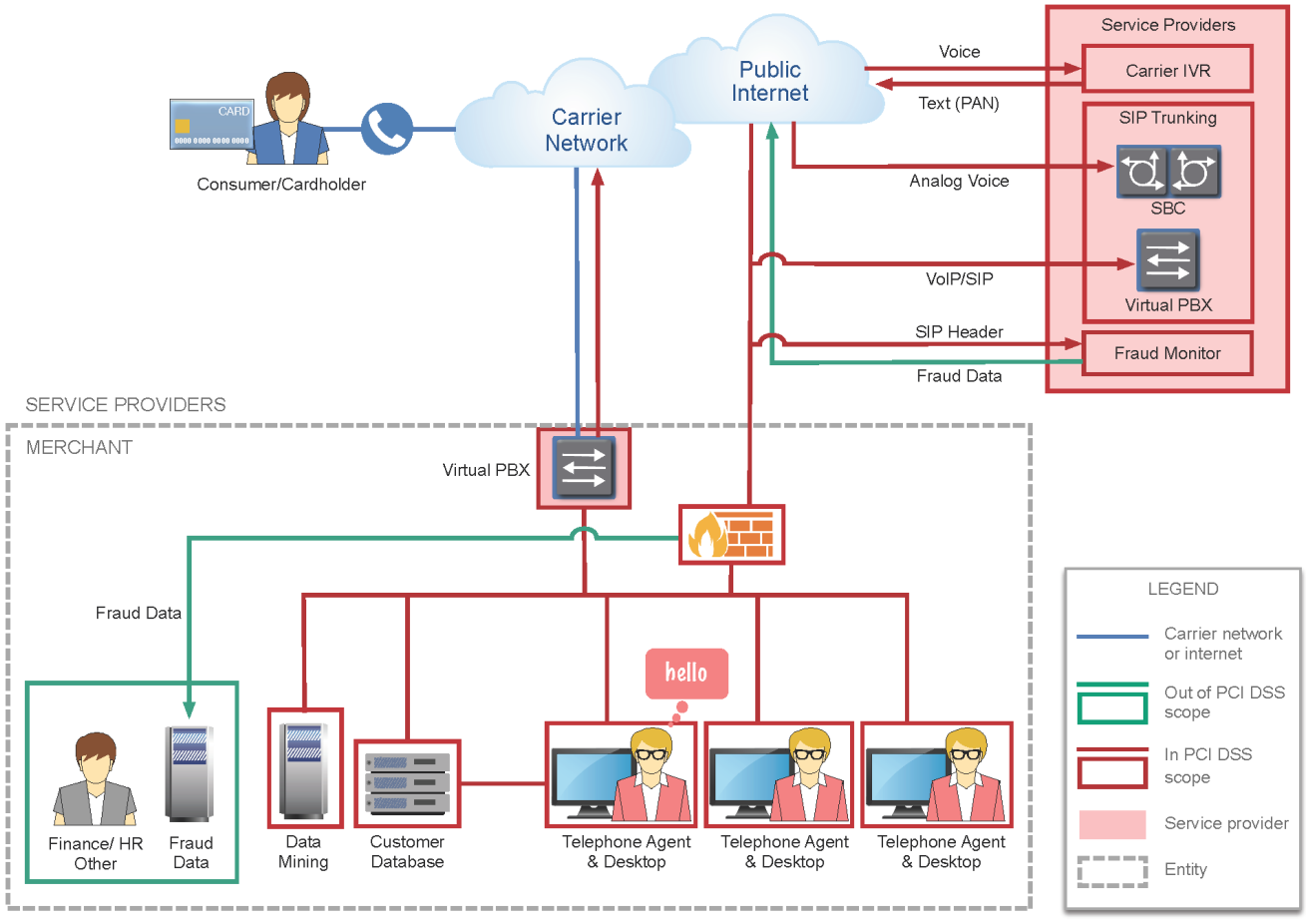


Diagram 6: Demarcation

Where the telephony traffic terminates on equipment owned and operated by the third-party service provider, this equipment should be protected, configured, maintained, and monitored in accordance with applicable PCI DSS requirements. Everything after the third-party equipment should be considered in scope. If the third-party equipment resides on the entity's premises, there may be a split PCI DSS responsibility between the entity and the service provider.

The process used by the entity or a service provider to demonstrate compliance with PCI DSS, including for controls that rely on a third-party service provider, is discussed in detail in the Information Supplement: *Third-Party Security Assurance.*[4]

2.5 Systems and Networks Mistakenly Excluded from Scope

Telephony environments are only as secure as their weakest link. Risks may not be considered when systems or networks are wrongly excluded from PCI DSS scope; this is often the result of two scenarios:

- **Improperly secured access from a third party or an application residing outside the CDE:** Components that are often improperly secured include networks and systems not directly involved in the payment process, but that have connectivity to payment systems or the telephony environment where payment card data is stored, processed, or transmitted. Examples include corporate intranets, finance systems, human resource (HR) and other personnel-management systems, shared network directory servers—possibly the entire corporate network.

- **Inadequate segmentation and systems incorrectly considered to be out-of-scope:** Any entity, system component, network, and third-party service provider with access to the CDE must be identified and that access must be secured with applicable PCI DSS controls. Alternatively, adequate segmentation must be implemented to avoid bringing other sections of the business into PCI DSS scope. Achieving viable network segmentation when a single VoIP phone system links in-scope and out-of-scope systems may prove very challenging.

  PCI SSC has published the Information Supplement: *Guidance for PCI DSS Scoping and Segmentation.* See Appendix G for a list of PCI DSS references and how to find them.

Beyond the general scenarios above, the entity's business continuity and recovery plan should be reviewed to assert if people, processes, and technology on the plan are in scope for PCI DSS. This is particularly relevant when offsite recovery facilities are involved whether they are hot, warm, or cold sites.

[4] https://www.pcisecuritystandards.org/documents/PCI_DSS_V3.0_Third_Party_Security_Assurance.pdf

2.6 Compliance validation

Any entity operating a telephony environment for processing card-payment transactions should understand that while the PCI SSC manages the PCI DSS, card-payment brands and acquirers have their own compliance programs. Entities should understand their compliance-reporting obligations before conducting scoping activities by consulting with their acquirer or the payment brands to confirm their validation requirements. Once the need to validate compliance has been confirmed and the methods in which compliance must be validated (e.g., via SAQ or third-party assessment), the PCI DSS scoping exercise can begin.

3 People

People represent the highest risk when it comes to the security of data whether compromises are intentional or accidental.

> *Insider threat occurs when a person with legitimate access misuses his privileges and compromises the operations and security of a company… when an insider who has rightful access to the data is involved, it can often go undetected. There has been a steady rise in the number of cases of insiders' threat related incidents in recent years.*[5]

3.1 Risks and Guidance in Simple Telephone Environments

The telephone environment, whether large or small, provides significant opportunities for payment card data to be compromised from outside the organization by criminals gaining access to systems and software. Compromises can also originate inside the organization from personnel who handle the calls or have access to systems and processes that support telephone-based payments.

One of the best ways to mitigate that risk is to create and maintain a culture of security within the organization.

In terms of people, the following should be highlighted:

- All personnel having access to payment card data are in scope of PCI DSS and should be trained as per Requirements 12.6.1 and 12.6.2 and screened as detailed in Requirement 12.7.
- As per Requirement 9.9.3, entities using points of interactions (POI) should provide training for personnel so they can identify and report any attempted tampering or suspicious behaviors.
- A policy should be in place to ensure that payment card data is protected against unauthorized viewing, copying, or scanning, in particular on desks.

Exposing personnel to spoken account data brings a number of risks to the organization that can be mitigated through adequate processes and technologies, but organizations should also be aware of the risk their staff face in being approached and threatened by organized crime. It is recommended that training should include awareness of those risks and understanding how the entity would support those personnel should that situation exist.

3.2 Additional Risks and Guidance in Complex Telephone Environments

The key area of risk within complex telephone environments is personnel. This would include customer service representatives, the operators or agents that take account data and customer details over the phone, as well as their supervisors and managers. For example, front-line staff and their supervisors receiving account data through a headset or via a computer screen could use a variety of techniques to acquire and record this data, from simply writing the details into a book or mobile device to utilizing key logging or

[5] Michele Moore - Cybersecurity Breaches and Issues Surrounding Online Threat Protection - 2017 -ISBN-13: 978-1522519416

recording equipment. Audio can be captured in transit and it is a trivial task for an attacker to convert audio into queryable data that can be used for fraud.

Where such personnel have access to account data or systems in the CDE, the following measures should be in place. Note that this is not a comprehensive list and that many of the best practices in this document reflect PCI DSS requirements. How these requirements apply will need to be determined for each organization.

In addition to the controls described in Section 3.1, the following controls are further examples of measures to limit the exposure of sensitive data to unauthorized parties:

- Clearly define roles and assign all system access based on need to know, to ensure that the minimum required number of personnel have access to account data. For example, assign roles so that payment card information can be entered by a sales agent, but other staff such as customer service representatives have access only to the masked PAN.
- Screen potential personnel prior to being hired (as per PCI DSS Requirement 12.7) to ensure individuals with questionable or criminal backgrounds do not gain access to account data. Screening policies should account for all types of personnel with access to the CDE or payment card data, including full-time and part-time employees, temporary workers, consultants, and contractors. As a best practice, the screening process should also cover internal transfers—where personnel in lower-risk positions who have not undergone a detailed background check are transferred to positions of greater responsibility or access—to help minimize the risk of attacks from internal sources. Examples of screening checks include previous employment history, criminal-record checks, credit history, and reference checks. The specific types of background checks performed should appropriate for the role.
- Implement controls to physically protect all forms of media and prevent unauthorized persons from gaining access to account data. Cardholder data is susceptible to unauthorized viewing, copying, or scanning if stored unprotected on removable or portable media, printed out, or left on someone's desk. Do not allow personnel with access to account data to record or store the data on any form of media that is not authorized or could lead to that data being compromised.
- Implement a security-awareness program (PCI DSS Requirement 12.6), delivered at the start of employment and at least annually thereafter, to make sure that all personnel are properly trained and knowledgeable about the business's security policies and procedures. This includes reviewing security policies and procedures with all in-house and at-home/remote agents at least annually to ensure that security processes and procedures are not forgotten or bypassed. As a best practice, consider requiring personnel to acknowledge the security policy as part of their daily sign-in process.
- Particular attention must be given to home workers. Some of the examples of controls may be difficult to implement. Organizations should evaluate the additional risks associated with processing account data in unsecured locations and implement controls accordingly. All staff should be made fully aware of the risks related to remote or home-working and what should be required to maintain the ongoing security of systems, processes, and equipment supporting the processing of telephone-based payment card data.

4 Process

PCI DSS specifically addresses physically securing all media. In the context of securing telephone payments in all telephone environments, processes should be implemented and managed to reduce opportunities for fraud of all personnel exposed to account data.

PCI DSS also makes clear that even if encryption technologies are in place, an entity should not store sensitive authentication data after authorization. For all telephone environments, sensitive authentication data (SAD) includes the card security code/value that may be taken during a telephone call. The only entities that can store SAD after authorization or for other purposes are issuers and companies supporting issuing services with a business need to retain the data. These entities are required to protect the data in accordance with PCI DSS Requirement 3.2.

If SAD is received and recorded, the entity MUST render all data unrecoverable upon completion of the authorization process. Implementing a process to prevent the recording of sensitive authentication data may be considered a best practice. This applies irrespective of the complexity of an entity's telephone environment.

If any part of the telephone environment is outsourced to a third-party service provider, both the entity and service provider should clearly understand their responsibilities for securing their respective systems, processes, and personnel, and document accordingly. PCI DSS Requirement 12.8 mandates policies and procedures to manage service providers.

4.1 Risks and Guidance in Simple Telephone Environments

In simple telephone environments where technology is not deployed to prevent spoken account data from being listened to by personnel and calls are not intentionally recorded, restricting the recording of account data is essential to maintain a secure environment. This may mean implementing processes to restrict access to: notebooks and pens, mobile phones capable of taking notes, any device that enables voice recordings, and—where account data is input into a system—any device capable of taking pictures.

Processes should also be put in place to prevent the use of other transportable technology devices where account data is processed through systems—e.g., memory sticks, Bluetooth recorders, and/or key loggers. These processes are not explicitly required by PCI DSS but can be implemented as part of the entity's security policy to fulfil the requirement to protect payment card data.

In all cases where calls may be intentionally recorded, entities should ensure that sensitive authentication data is not stored after authorization, as made clear in the foregoing paragraphs.

4.2 Additional Risks and Guidance in Complex Telephone Environments

Without appropriate segmentation, the convergence of voice and data networks can have the effect of bringing entity's wider infrastructure into PCI DSS scope. The implementation and monitoring of all the processes detailed within the PCI DSS will therefore apply and ideally be part of the entity's security policy identified in Requirement 12.1. Mitigating the risks associated with spoken account data focuses on

minimizing the opportunities of account data being recorded by personnel in written or electronic format, typically by denying access to materials and devices capable of recording account data.

To prevent unauthorized access by individuals with any malicious intention, policies and procedures should be defined to ensure that all personnel—including onsite employees, home workers, and remote agents—are aware that any unauthorized copying, moving, sharing, or storing of payment card data is prohibited. Additionally, the physical environment within which an office worker or home worker is taking card payments over the telephone should be effectively monitored and access controlled. Examples of required controls include:

- Ensure that at-home/remote workers use a multi-factor authentication process when connecting to the telephone environment or to any systems that process account data.
- Restrict physical access to media containing payment card data, such as call or screen recordings, as well as networking/communications hardware.
- Ensure only authorized personnel are allowed in business areas where telephony equipment and agent desktops are located. For company premises, this includes implementing procedures to clearly identify visitors and make sure all visitors are escorted when in the telephone environment. Securing systems and data located in home-worker environments can be challenging and difficult to enforce. At a minimum, home workers should be required to ensure that any systems they use to process account data, and any account data to which they have access, is securely maintained and not accessible to any unauthorized individual.
- Provide awareness training annually for all personnel to understand the importance of physical security and keeping the workspace secure—for example, not to write passwords on sticky notes attached to the desktop—and define clear responsibilities for remote agents regarding physical security of all telephone equipment in their homes or remote locations.
- If account data is ever written or printed on paper, ensure it is securely stored, then shredded when no longer needed. If any part of the telephone environment is outsourced to a third-party service provider, both the entity and service provider should clearly understand their responsibilities for securing their respective systems, processes, and personnel, and document accordingly.

Where account data is input into systems:

- Ensure and verify that the PAN is masked when displayed (the first six and last four digits are the maximum number of digits to be displayed), for personnel without a legitimate business reason to see the whole PAN.
- The display of full PAN on items such as computer screens, payment card receipts, faxes, or paper reports can result in this data being obtained by unauthorized individuals and used fraudulently. Ensuring that the full PAN is only displayed for those with a legitimate business need to see the full PAN minimizes the risk of unauthorized persons gaining access to PAN data.

5 Technology

The PCI DSS is very clear on the requirements and controls necessary to keep technology secure, and the PCI SSC Prioritized Approach (document links available in Appendix G) helps stakeholders understand where and how they can act to reduce risk earlier in the validation process using a prioritized, milestone-based approach. For example, the first milestone is to remove sensitive authentication data and limit data retention.

By limiting exposure of payment data in your systems, you simplify scope and validation, reducing the chance of being a target for criminals.

5.1 Risks and Guidance in Simple Telephone Environments

Using desktops and other types of terminals introduces risks. To prevent unauthorized access to or diversion of account data from such devices, these technologies should be suitably secured and checked regularly for viruses or other malware as well as for signs of physical tampering—for example, the addition of a keyboard-logging device. Wherever possible, avoid solutions that expose personnel to CHD/SAD.

Additionally, any customer database systems, third-party CRM applications, or order-processing systems into or through which account data is being processed, transmitted, or stored should be secured. Below, among other possible controls, examples of such controls include:

- Ensure that at-home/remote workers use a multi-factor authentication process when connecting to the telephone environment or to any systems which process SAD/CHD.
- For all personnel, prohibit unauthorized copying, moving, and storing of account data onto local hard drives and removable electronic media when accessing payment card data via remote-access technologies.
- Ensure that the PAN, once entered into the system, is masked when displayed; no more than the first six and last four digits should be displayed. Note that individuals may view additional PAN digits when there is a legitimate business to do so—for example, if a supervisor needs to review the full details of a particular transaction. Any individuals not specifically authorized to view the full PAN should only ever have access to masked PANs.
- Consider technology solutions (described later in this guidance) where personnel do not have to hear or enter account data into the system. For example, some technologies allow the cardholder to use their telephone keypad to enter account data into a secure webpage, either directly or via a secure link provided via SMS or e-mail, thus preventing the entity from being exposed to the cardholders' account data.
- Require all personnel to use only company-approved hardware devices—e.g., mobile phones, telephone handsets, laptops, desktops, and systems. This is especially relevant to remote/at-home working, ensuring that the entity can maintain control of systems and technology supporting the processing of telephone-based payment card data.
- Ensure that all desktop/terminals, including those in remote/at-home working environments:
  - Have personal firewalls installed and operational.

  - Have the latest version of the corporate virus-protection software and definition files.
  - Have the latest approved security patches installed.
  - Are configured to prevent users from disabling security controls.
- Ensure the PCI security training (Requirement 12.6.2) for home workers conducting card-not-present (CNP) transactions addresses their responsibility to maintain the physical security controls for their telephony, IT systems, and work environments.

5.2 Additional Risks and Guidance in Complex Telephone Environments

Implementing and maintaining PCI DSS requirements within a complex telephone environment can be particularly challenging. Potentially high volumes of payment card account data are received in clear and handled by staff. This data may be stored in audible format. Data will be transmitted and processed across various networks with service providers using telephony-specialized technologies, making the evaluation of the PCI DSS scope difficult.

It is important to note that a system is considered “in scope” regardless of the volume of payment information it handles. An essential activity for each business is therefore to evaluate the risks for its own telephone environment. The use of a telephone service provider to route voice traffic to the organization should be included in any risk assessment the entity may perform. Some of the typical risk areas associated with telephone-payment environments include:

- IT networks and telephony systems—e.g., switches, interactive voice response (IVR) systems, network directory services, DNS, DHCP
- Physical environment used by all personnel, be they agents, customer service representatives, and/or operators
- Voice and screen recordings
- Technologies or services used to reduce scope if they are not taken into the scope themselves

5.2.1 Securing IT Infrastructure

One of the first areas of consideration is the internal IT infrastructure that supports the telephone calls and their associated payments. This includes the telephony equipment such as switches, internal legacy telephony and VoIP networks, and IVRs, as well as devices providing general network services, such as network directory services, DNS, DHCP, etc. As with any IT network, there is risk of unauthorized external and internal access; any technologies used to store, process, or transmit account data, and any networks connected to those technologies, must therefore be appropriately secured. The risks of interception of VoIP and "traditional network" traffic are the same. The difference is that VoIP traffic needs to be rendered audible to be exploited, and it is harder to look for patterns associated to CHD without listening to the traffic.

The following controls are highlighted:

- Maintain systems to secure configuration standards and regularly test for vulnerabilities.

- Implement physical and logical controls for wired data networks, wireless data networks, and internal telephony VoIP networks.
- Segment in-scope systems from other networks—e.g., the "Finance/HR/Other" areas of the business shown in the telephone environment diagrams above—to prevent unauthorized access to the network and CHD.
- Disable network services that are not needed across all in scope system components—for example, IVR systems are often shipped with all network services enabled, some of which may be subject to security vulnerabilities that could allow unauthorized access to the system. Disabling network services that are not required for IVR functionality or for business purposes helps reduce the risk of vulnerability. Examples of common services that are often enabled by the vendor but may not be needed include Telnet, FTP, NTP, and send mail.
- Ensure proper user authentication is implemented for all personnel, including staff, agents, administrators, and any third parties.
- Use strong cryptography to protect any CHD that is stored—for example, in audio recordings or in a database—or otherwise render the stored data unreadable—for example, via truncation or hashing. Sensitive authentication data (SAD) must not be stored after authorization, even if encrypted. This applies even where there is no PAN in the environment.
- Restrict access to call-recording and CRM data containing CHD to only those with a business need.
- Establish and maintain access logs tracking the user's log-in account and corporate role.
- Use strong cryptography to secure transmission of any sensitive payment card data over public networks. Examples of transmissions that need to be secured include but are not limited to:
  - Wired and wireless networks used by at-home/remote agents and supervisors.
  - Any public network segments used to carry or send screen or voice recordings containing payment card data.
  - Voice or data streams (i.e., VoIP telephone systems) containing CHD sent over open or public networks. Examples of open, public networks include but are not limited to the Internet, wireless technologies such as 802.11 and Bluetooth, cellular technologies, and satellite communications.
- Configure firewalls and network controls to prevent unauthorized transmissions of call-recording data to any network segment or device without a legitimate business need to access this data.
- Never send CHD over an unencrypted, end-user messaging medium such as chat, social media, SMS (short message service)/text, or e-mail, or other non-encrypted communication channel.
- Ensure that systems such as IVR, for example, do not output cardholder data in any logs.
- For the home/remote worker supported as an extension of the entity's network, make sure that their environment is secure in accordance with the PCI DSS and any controls agreed with your acquirer or payment card brand.

5.2.2 Architectural Aspects

The architectural aspects of the overall telephony network should be considered—for example, understanding how VoIP traffic is routed, or how demarcation points are managed between different entities. Some telephony services may also offer secure configuration options. Session Initiation Protocol (SIP) and Real-time Transport Protocol (RTP) both have secure variants—SIPS and SRTP, respectively—which may help protect the data connection process and data stream.

Please refer to Appendix E, "Further Considerations on VoIP," for more information.

5.2.3 Desktop Systems

Desktops within the telephone environment may involve a variety of technologies, including desktop applications for payment acceptance, web browsers, iframes hosted by third parties to the agent organization, as well as virtual desktops, thin clients, remote desktop connections to other systems, or other applications intended to replace conventional workstations for contact center agents. Because these are the endpoints where agents hear payment card data spoken on a telephone then enter those data elements accordingly, the endpoint at which the agent enters the data is in scope for PCI DSS. This endpoint transmits payment card data, and the organization must consider applicable PCI DSS requirements for these systems, as well as for any connected-to or security-impacting systems around it.

5.2.4 Softphones

Many organizations are leveraging newer features of telephone systems including the use of software phones (softphones) which are software programs used to make a voice call over the network. Softphones will typically be installed on an end user's workstation with either a headset or a USB-style phone used for the conversation.

It is important to note that the use of such systems to capture payment card account data would bring the workstation—and probably the network it is connected to—into PCI DSS scope.

For more information, refer to the Information Supplement, *Guidance for PCI DSS Scoping and Network Segmentation,* mentioned in Appendix G. This Guidance is intended to provide further understanding of scoping and segmentation principles as applicable to a PCI DSS environment.

5.2.5 Dual-Tone Multi-Frequency (DTMF)

DTMF is the sound one can hear when pressing the buttons on a telephone keyboard, a different tone, or frequency is associated with each digit key. It is easy for trained hears to recognize a number from the tones generated by a telephone keyboard. DTMF suppression is removing these tones, DTMF masking is replacing the tones by either a random tone or a flat tone. DTMF masking will be explored further in Section 6.

Depending on how it is deployed and whether it transmits payment card account data, DTMF masking is one of the technologies that can be used to reduce the risk to account data in the environment.

5.2.6 *Voice and Screen Recordings*

The challenge many call centers face is that local laws or regulation may require call recordings to be retained for a number of years, depending on the type of service provided. Any such requirements the organization may be subject to should be defined and incorporated into the data-retention policy. Organizations should consider the use of technologies which prevent CHD entering the call recording, while allowing the full call to be recorded

To ensure the security of any CHD within call recordings, the recording of a verbal transmission of CHD, or where DTMF tones are processed unaltered, must be correctly stored and secured in accordance with PCI DSS requirements. Additionally, the capture and storage of screens or video recordings where CHD is visible must be equally secured.

Every possible effort must be made to eliminate SAD from the telephone environment. If an organization has a legitimate constraint that prevents it from removing SAD from its recordings, the organization should discuss this with its acquirer and/or payment brand. If SAD cannot be eliminated, it must be secured in a manner consistent with PCI DSS and must not be able to be queried

Appendix D, “Call Recording Decision-making Process,” illustrates some high-level decision points related to the presence of SAD in call recordings.

CHD should only be stored as necessary to meet the needs of the business and, to comply with local laws and regulations. If any CHD is stored, an appropriate data-retention policy to ensure that the data is stored only when absolutely necessary should be implemented. Storage should be kept to a minimum, and a secure disposal procedure should be in place to delete the data as soon as it is no longer needed.

Specific considerations around storage of account data to avoid unauthorized access to SAD include:

- Backups and archives of the recording solution must also be protected and should not provide a backdoor to the solution. Consider storing call-recording archives on a system or media that is not connected to a network.
- Implement strong authentication controls for all personnel with access to voice and screen recordings, and for any other storage of CHD. Ensure that personnel do not share user IDs and passwords.
- Restrict logical access to recordings and CRM data containing payment card data based on the individual’s business need. For example, by implementing screen-recording-playback interfaces that display payment card information only to managers, and having it blacked out (or masked) for all other personnel.
- All interaction with the recordings should be logged according to PCI DSS Requirement 10.
- Systems storing CHD may be located on a secured internal network that is segregated from Internet-facing networks and other untrusted networks.
- PAN data must be rendered unreadable. This can be done by using strong cryptography to encrypt the entire PAN, one-way hashing it, truncating it, or replacing it with a token anywhere it is stored, including in voice and screen recordings, databases, log files, and back-up media.

Note: *If truncated PANs and hashed pans are both present an entity's environment, additional controls must be in place to ensure that the hashed and truncated versions cannot be correlated to reconstruct the original PAN.*

- Remember that storage of sensitive authentication data after authorization is not permitted, even if the data is encrypted. If any recordings include card verification code data, the organization must ensure that all SAD is securely deleted from the recording or is otherwise rendered unrecoverable upon completion of the authorization process. Where possible, implement processes and technologies that prevent CHD from entering the telephone environment and prevent SAD from being recorded in the first place.
- If a technology solution (e.g., pause-and-resume or stop-start) cannot block the audio or video from being stored, the sensitive authentication data (SAD) MUST BE DELETED from the recording as soon as the transaction is processed.
- Where pause-and-resume is used for call recordings, especially where initiated by the agent, it is recommended to verify that the call recordings do not contain CHD or SAD be undertaken on a regular basis—preferably weekly.
- Gaps in security coverage can occur when call and screen-recording services are provided by a third party. Entities should develop a payment card data flow that marks each entity's area of responsibility so that business agreements among organizations clearly communicate expectations and responsibilities.

The PCI SSC provides a great deal of supplementary guidance information. A list of relevant documents is available in Appendix G.

6 Approach to Scoping and Securing Telephone Environments

Organizations should ensure that appropriate security controls are in place covering people, process, and technology wherever account data is stored, processed, or transmitted. The best way to do this is adopting and implementing the latest version of the PCI DSS, as summarized below. A link to the full version of the document is available in Appendix G.

PCI Data Security Standard – High-Level Overview

Build and Maintain a Secure Network	**1.** Install and maintain a firewall configuration to protect cardholder data **2.** Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	**3.** Protect stored cardholder data **4.** Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	**5.** Protect all systems against malware and regularly update anti-virus software or programs **6.** Develop and maintain secure systems and applications
Implement Strong Access Control Measures	**7.** Restrict access to cardholder data by business need to know **8.** Identify and authenticate access to system components **9.** Restrict physical access to cardholder data
Regularly Monitor and Test Networks	**10.** Track and monitor all access to network resources and cardholder data **11.** Regularly test security systems and processes
Maintain an Information Security Policy	**12.** Maintain a policy that addresses information security for all personnel

In addition, an entity can reduce risk and reduce its attractiveness to criminals by devaluing account data through tokenization, making card data unreadable or by reducing its scope of where the PCI DSS applies. The following section looks at some of the techniques available to reduce PCI DSS scope.

6.1 "No Cardholder Data Environment" Approach and Other Forms of Scope Reduction

This section looks at some of the common approaches to secure and/or remove telephone-based account data from telephone environments.

Whichever methods are used, the goal is to ensure that SAD is never stored after the transaction is authorized, and account data is secured and/or removed from systems and storage.

As a starting point, consider whether the organization should aim at excluding telephone-based card payment data entirely. This approach may be part of a structured business strategy to reduce risk by not accepting telephone payments. For organizations that receive very small volumes of telephone payments and perhaps already have a secure alternative payment channel—for example, a PCI DSS compliant e-commerce channel—this approach may provide a simple solution to mitigating a real business risk by avoiding the risk altogether.

For organizations committed to taking payments over the telephone, consideration should be given to techniques that minimize exposure of PAN and SAD to the telephone environment and balance that with user/customer experience requirements, with the object of significantly reducing the CDE or eliminating the CDE altogether.

Outsourcing to PCI DSS validated service providers may be considered as an option for securing telephone environments. Please see Section 7 for further guidance.

For organizations accepting telephone-based payments, reducing PCI DSS scope through network segmentation and then applying all 12 Requirements to the reduced environment remains a valid technique for securing the telephone environment.

It is recommended that organizations refer to the Information Supplement, *Guidance for PCI DSS Scoping and Network Segmentation,* mentioned in Appendix G.

The types of agent interaction are discussed in the next sections; however, for all types of agent interaction, consideration must be given to how and where account data is transmitted, processed, or stored. Technologies and processes may also be implemented to restrict the presence of account data to a limited number of systems, helping to reduce the size of the CDE.

6.2 Technologies, Overview, and Classifications

In the context of securing telephone payments and providing a simplified overview of what is available, technologies can be classified in two ways: First, by the user experience delivered to the organization's customers; and second, by the dependency of the technology on an organization's telephony infrastructure.

In terms of customer experience or contact type, technologies can be classified as being one of the following types:

- **Attended –** Where the entity remains in direct voice contact with its customer for the entire duration of the telephone payment transaction.
- **Unattended –** Where the entity does not remain in direct voice contact with its customer for the entire duration of the telephone payment transaction, and all or part of telephone payment component of the call is handled by a different technology path—e.g., IVR or some type of redirection to a web payment process.

In terms of technology dependency on the entity's telephone infrastructure, technologies can be further classified as either:

- **Telephony based –** Where the technology application is wholly dependent on the entity's telephony infrastructure, effectively using voice or DTMF tones, through the use of the telephone keypad, to facilitate the transaction.
- **Digital based –** Where the technology application sends a message or email to the customer with a link to a PCI DSS compliant web-based payment page where the customer is invited to input their PAN and SAD using a connected device such as smartphone, tablet, laptop, or desktop computer.

Both telephony-based and digital technology-based types are capable of supporting both attended and unattended customer-experience options. In addition, all four classifications of technology type (Telephony Attended, Digital Attended, Telephony Automated and Digital Automated) have the potential to reduce the scope of the PCI DSS, devalue the account data, and potentially ensure no CDE exists.

Note: *See Appendix C, "Payment Call Environment-identification Tree," for a chart that allows the reader to identify their telephone environment and consider the type of scope-reduction technology that is appropriate.*

6.2.1 Attended Transactions

The terms "attended" and "unattended" transactions are used generally in the face-to-face/card-present payment channel and work equally well when describing telephone-based transactions.

A typical "transaction journey" for "attended" transactions might be:

- When telephony-based technologies are deployed (pause-and-resume, see Section 6.5.1):
  1. The customer and order details are spoken by the customer to the agent.
  2. The agent enters the customer and order details into a system.

3. The agent initiates the pause-and-resume system to temporarily halt the recording and informs the customer to provide their CHD and SAD verbally.
4. Using the desktop application, the agent enters the customer's details.
5. The recording is resumed and the agent confirms this to the customer. The agent completes the transaction, supporting verbally as appropriate.
6. The agent hears all the CHD and SAD.
7. The agent then receives confirmation that the payment is authorized and communicates that, or any other outcome returned from the PSP, back to the customer.

- When telephony-based technologies are deployed (DTMF):
  1. The customer and order details are spoken by the customer to the agent.
  2. The agent enters the customer and order details into a system.
  3. The agent initiates the DTMF masking (also known as "clamping") application and informs the customer (to keep their data secure) to input their PAN and SAD using their telephone keypad.
  4. Using the desktop application, the agent monitors the customer's progress to complete the transaction, supporting verbally as appropriate.
  5. The agent hears flat tones and sees asterisks depicting the payment card numbers appear on their screen, perhaps only displaying the last four digits, putting the agent in a position to support the customer.
  6. The agent then receives confirmation that the payment is authorized and communicates that, or any other outcome returned from the PSP, back to the customer.
- When digital technologies are deployed:
  1. The customer and order details are spoken by the customer to the agent.
  2. The agent enters the customer and order details into a system.
  3. The agent initiates the digital application and sends the customer a link to a secure internet payment page.
  4. The customer validates the URL, confirms the transaction amount and the delivery address, submits card account data into the payment page and provides the 3DS authentication parameters (where required).
  5. The agent monitors the customer's progress to complete the transaction, supporting verbally as appropriate.
  6. The agent and customer then receive confirmation that the payment is authorized, or any other outcome returned from the PSP.

6.2.2 Unattended Transactions

A typical "transaction journey" for an "unattended" transaction might be:

- When telephony-based technologies are deployed:
  1. The customer and order details are spoken by the customer to the agent.
  2. The agent enters the customer and order details into a system.
  3. The agent informs and transfers the customer (to keep their data secure) to an automated call-handling system (or IVR).
  4. The agent has the option to terminate the call whilst the customer progresses the transaction independently. The type and related scripting of the IVR system used will be different for each entity. Within the IVR journey the IVR then asks the customer to input their PAN and SAD using their telephone keypad.
  5. The IVR application receives confirmation that the payment is authorized and communicates that, or any other outcome returned from the PSP, back to the customer. An option to return to the agent may be implemented.
- When digital technologies are deployed:
  1. The customer and order details are spoken by the customer to the agent.
  2. The agent enters the customer and order details into a system.
  3. The agent initiates the digital application and sends the customer a link to a secure internet payment system.
  4. The customer validates the URL, confirms the transaction amount and delivery address, submits card account data into the payment page and provides the 3DS authentication parameters (where required).
  5. The agent has the option to terminate the call whilst the customer progresses the transaction independently as an ecommerce transaction.

An entity may choose to deploy a fully automated version of a telephony-based or digital-based solution with no agent interface as an alternative to the examples above or as an “out-of-hours” alternative to the above (for example, automated speech recognition).

6.3 Digital-based Attended and Unattended Solutions

Digital technology solutions have no dependency on the organization’s telephony infrastructure. The level of impact on an organization’s scope is dependent on how the chosen technology is implemented by the vendor.

In general terms, both attended and unattended digital technologies could use the public Internet to deliver links to the customer. The customer would access that link via their connected device (smartphone, tablet, laptop, or desktop) and then use it to send transaction data directly to the entity’s PSP/payment gateway. Sending a link to an online secure payment system to a customer via a messaging service may be considered the same as an e-commerce entity using redirection to third-party payment pages. The impact of such a system on the entity’s PCI DSS scope would need to be evaluated. In such case, the integrity and validity of the link to an online secure payment system must also be considered.

6.4 Telephone-based Attended and Unattended Technologies

All telephony-based technology solutions have a dependency on the organization's telephony infrastructure. The level of that dependency and the impact on an entity's scope are based on the actual design and how the chosen technology is implemented.

In general terms, both attended and unattended classifications of telephony-based technologies may use DTMF tones, which are transmitted by a telephone device (mobile, data, or fixed line) when the customer enters PAN and SAD via their telephone keypad. DTMF tones are easily detectable by phone systems and computers, and anyone with the right equipment can convert the tones back to the original digits or characters.

Alternatively, the organization may use pause-and-resume technology, and in this case the agent will hear all of the CHD and SAD; and the organization must adopt and implement all relevant security procedures detailed in this document in order to secure that data.

6.4.1 Attended Telephony Technologies

Attended technology solutions enable the entity to remain in constant voice contact with its customer for the entire duration of the telephone transaction. These technology types rely on DTMF suppression or DTMF masking to reduce PAN and SAD exposure in these transactions. These technologies typically replace the DTMF tones with flat sounds before they reach the agent, who often hears only a single repetitive tone. The result is that the different tones made by the customer's telephone keypad are concealed such that the agent cannot identify them by their sound. To be effective, the sound replacing the original DTMF tone must not be linked to it, whether the masking tone is always the same sound or a random sound.

Storing only suppressed tones rather than original DTMF tones can reduce applicability of PCI DSS requirements for call recordings—for example, recordings and audio files containing only flat tones that cannot be converted back to the original data do not need to be rendered unreadable per PCI DSS Requirement 3.4. In this scenario, the entity would need to verify that the recordings contain only flat tones, and that the suppression method ensures the tones cannot be converted back to the original data. Even if only suppressed tones are stored and are not subject to Requirement 3.4, recording systems may still be in scope for other PCI DSS requirements if they have connectivity to the systems where CHD is present.

Where the DTMF tones are not replaced with flat, token, or random sounds, the specific numbers associated with each key press can be recovered, meaning that PAN and SAD is retrievable and the unaltered DTMF tones are fully in scope for applicable PCI DSS requirements.

To complement audio suppression of the DTMF tones, some solutions also integrate with the agent desktop environment to prevent PAN and SAD being captured or displayed on the agent's screen. For example, while the agent is hearing suppressed DTMF tones, their desktop could show the payment-entry field being propagated with a pre-defined character, such as an asterisk (*). In this scenario, any screen captures of the agent desktop would show only the asterisk and would not contain any PAN or SAD.

Depending on the particular implementation, DTMF suppression and masking technologies may be able to prevent PAN and SAD from entering the telephone environment, further reducing the applicability of PCI DSS to that environment. Of course, it would first have to be verified that all PAN and SAD are replaced with predefined sounds and characters before they reach the environment, and no PAN or SAD is present in the environment in any other form. Some implementations of DTMF masking rely on DTMF-detection—this may introduce a delay in the masking, and the initial portion of the DTMF tones may not be masked (this is called "DTMF bleed"). It is important to ensure that all DTMF tones, including any initial small portions of "DMTF bleed" that may be inadvertently allowed through a masking process, are not present in the environment.

A properly designed and deployed DTMF-masking solution can take not only the telephony environment, but also the agent environment and CRM system out of scope. Entities should avoid solutions that leave agent environments in scope unless there is an unavoidable business requirement to do so.

6.4.1.1 *Off-premises deployment of DTMF masking*

Diagram 7 shows an off-premises deployment of DTMF masking. In this scenario, a service provider receives the voice call before it reaches the entity. The DTMF-masking device separates the voice from DTMF. Masked DTMF is sent to the entity through the carrier network. DTMF is processed and is either directly forwarded or sent as payment card data to a payment service provider through a secured line over the internet. Variations of this scenario may exist where, for example, the telecom company manages DTMF masking or the payment service provider manages both DTMF masking and the payment. This type of deployment could allow the telephony systems to be out of scope for PCI DSS.

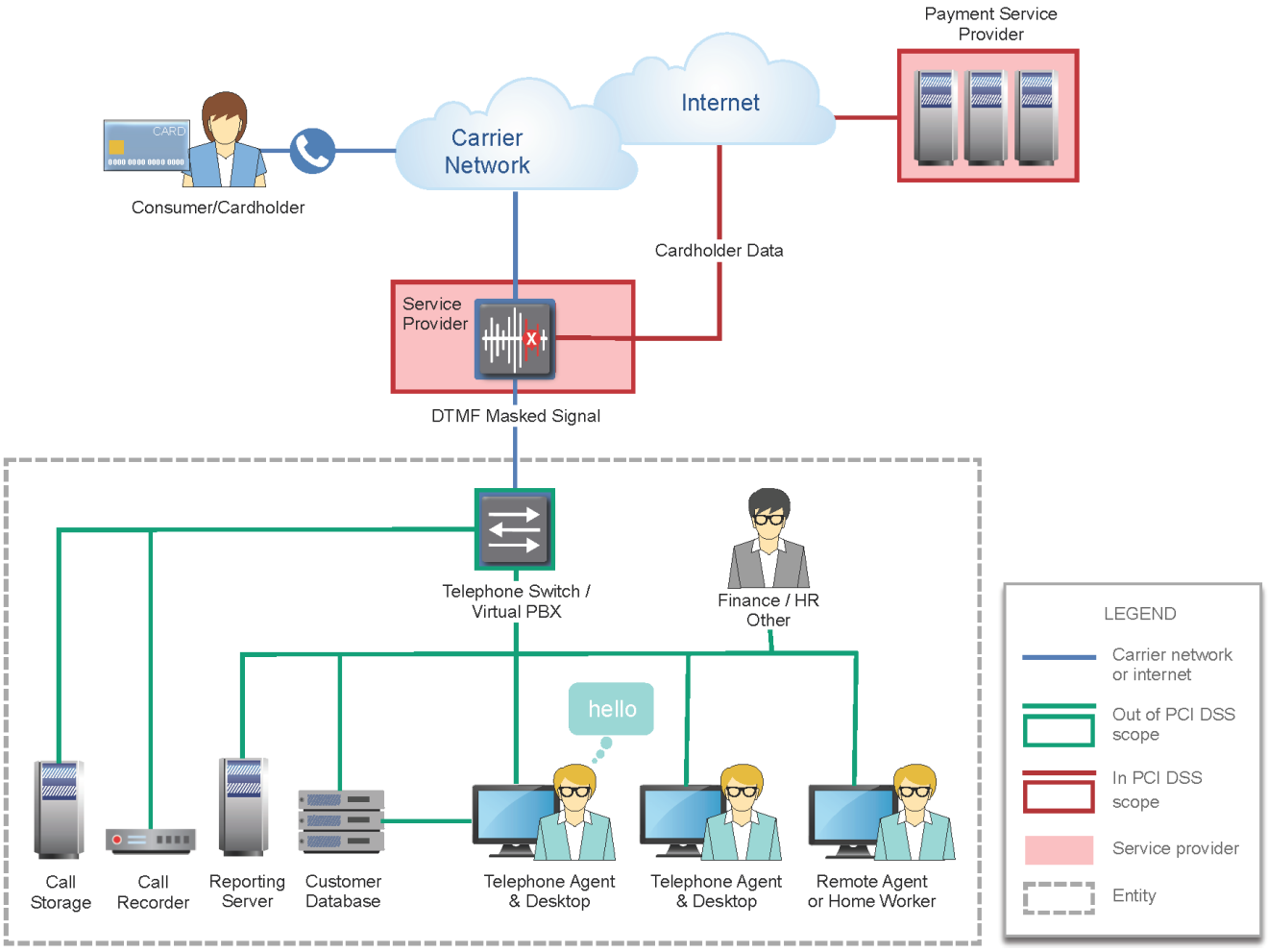


Diagram 7: Off-premises deployment of DTMF masking

6.4.1.2 *On-premises deployment of DTMF masking*

On-premises deployment is also possible. Diagram 8 shows an example of such implementation. A device hosted within the entity infrastructure separates the DTMF from the voice and sends back the masked DTMF into the entity's telephone systems. DTMF is either directly forwarded or sent as cardholder data to a payment service provider through a secured line over the internet. The cardholder data is securely sent to a payment service provider. In this instance, the Session Border Controller

(SBC) and the DTMF masking system are in scope for PCI DSS. The telephone switch is shown in scope as it may be considered as a demarcation point or as a "connected to" device. However, further analysis may be necessary to determine if the remaining part of the entity's network is in scope for PCI DSS. (see the PCI SSC Information Supplement, *Guidance for PCI DSS Scoping and Network Segmentation*). The devices will need to be securely configured and patched. Any remote access must be configured as per PCI DSS requirements. The connection to the payment service provider must be secured. Finally, the SBC and the DTMF devices must be correctly configured to ensure that no DTMF bleed occurs. It is recommended to include a regular review of the signal to validate the efficiency of the DTMF solution.

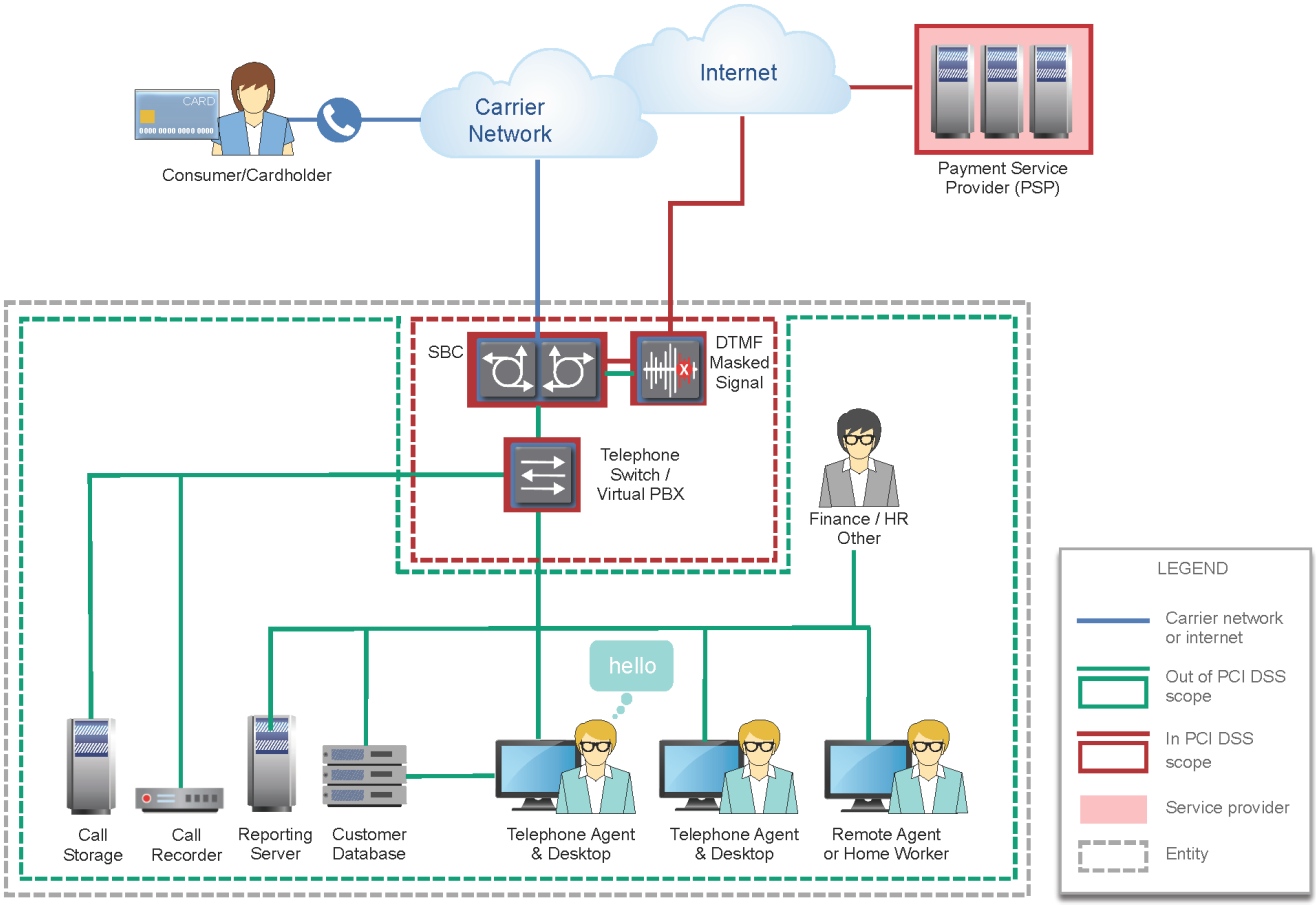


Diagram 8: On-premises deployment of DTMF masking

6.4.2 Unattended Telephony Technologies

In an unattended transaction, the agent is not in contact with the customer for the entirety of the call. Technologies used for unattended transactions are often referred to as IVR (interactive voice response) applications or automated call-handling solutions. In this scenario, the agent typically switches the call to the IVR or call-handling solution for the duration of time needed to communicate the payment details. Depending on the technology used, the transmission of account data could be either by voice (the

customer speaks the account data), or by DTMF (the customer uses their telephone keypad to input the account data).

The IVR or call-handling solution may be part of the entity's own telephone environment or be located at a third party, such as a PSP or acquirer. The technology may also provide the customer with an option to return back to an agent and re-establish voice contact after payment is complete, or during the transaction in the event that the payment is unsuccessful.

In all instances, the intent of these solutions is to bypass the agent when account data is transmitted, thus avoiding any exposure of account data to the agent. Moreover, DTMF suppression and DTMF masking, described in the previous section, can also be used to reduce the presence of account data in systems such as call-recording solutions.

When properly implemented, an unattended transaction solution could reduce applicability of PCI DSS requirements to the agent and agent desktop environment. However, it would first need to be verified that PAN and SAD bypass the agent environment, and neither the agent nor the agent desktop environment have the ability to access or retrieve account data.

6.5 Other Common Forms of Scope Reduction

6.5.1 Pause-and-Resume

The goal of pause-and-resume technologies is to prevent account data being recorded by temporarily halting the recording during the communication of account data and resuming the recording only when all payment data transmissions are complete. Pause-and-resume technologies may be manual or automated, and whilst a properly implemented pause-and-resume solution could reduce applicability of PCI DSS by taking the call-recording and storage systems out of scope, the technology does not reduce PCI DSS applicability to the agent, the agent desktop environment, or any other systems in the telephone environment as shown in the Diagram 9 on the following page.

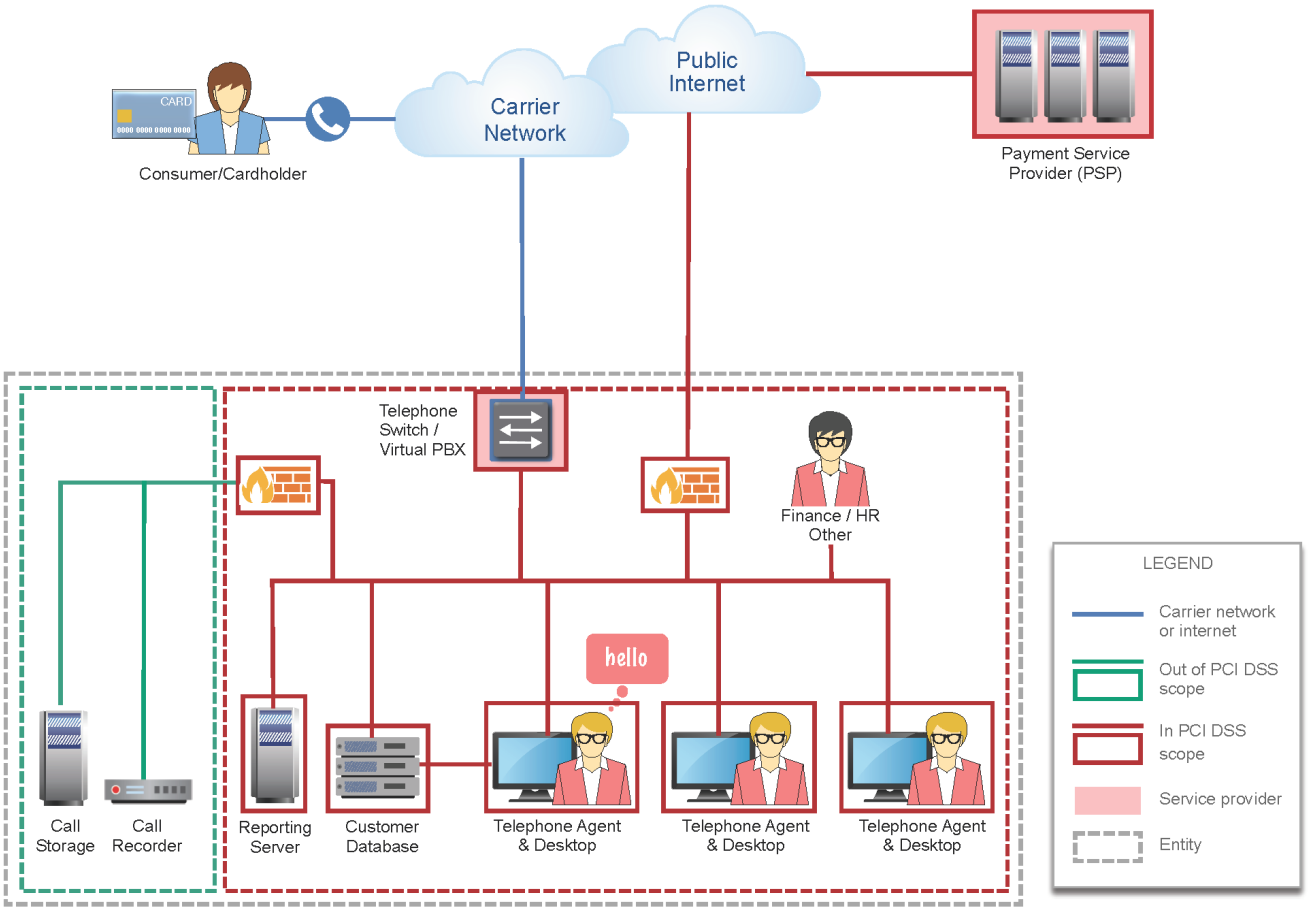


Diagram 9: Pause-and-resume

Manual pause-and-resume implementations rely completely on agent personnel to pause and restart the recording at exactly the right time. Common challenges with manual pause-and-resume include:

- The agent forgetting to pause the recording at the right time, resulting in the unintended capture of CHD and potentially SAD. Entities are encouraged to ask their call center operator how they remove SAD from recordings—preferably automatically (with no manual intervention by your staff).
- The agent forgetting to restart the recording after the transaction, resulting in a breach of regional or local legal requirements and in loss of other data that may have been of value to the business.

Manual pause-and-resume implementations require constant monitoring and verification that the manual processes are being followed by all agents for every transaction. As well as monitoring agent processes, the entity will need to regularly confirm that the call recorder and call storage do not contain any CHD or SAD. This can be achieved by supervisors regularly listening to recorded conversations.

The degree of oversight and supervision required for manual solutions is much greater than for automated solutions.

Automated pause-and-resume solutions are typically integrated with a desktop application used by staff during the transaction process. In an automated pause-and-resume solution, the agent no longer has the burden of remembering to manually stop and restart the recording, as the solution will automatically perform this function as part of a predefined step during the transaction process. For example, the technology could set the recording to automatically pause when the agent clicks on a payment-entry field or launches a payment screen within the application, and automatically resume when the agent clicks "submit" or moves to the next screen in the application.

The effectiveness of an automated solution relies largely on its integration with the agent's workflow process and the agent performing the correct steps at the correct time. If any ability exists for the agent to bypass the integrated process, the pause-and-resume technology could be circumvented and rendered ineffective.

6.5.2 *Outsourcing to a Specialist Third-party Service Provider*

Outsourcing to a PCI DSS validated third-party service provider may be considered as another option for securing telephone environments. Please refer to section 7 in this document for further guidance.

6.5.3 *Physical Segmentation*

Some organizations may choose to implement call center segmentation. This can be achieved by separating calls associated with payments from other types of calls through the use of a secure room.

The physical segmentation approach can be valid to deal with "exceptions" even when technology to prevent spoken card data is deployed. It can also be deployed within a simple telephone environment.

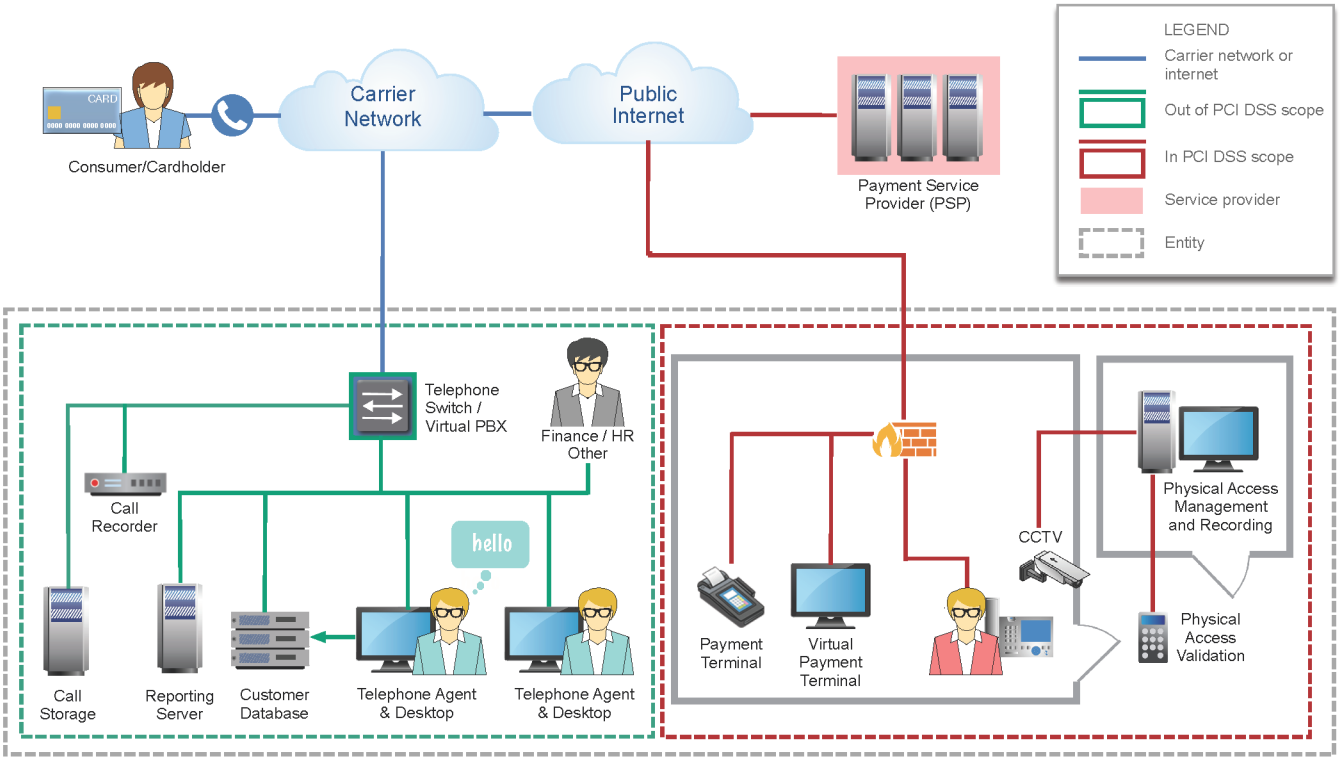


Diagram 10: Implementation of physical segmentation

Diagram 10 shows an example of a possible implementation of physical segmentation. Many other types of configuration can be implemented, and this diagram is only presented as an illustration of one of them. Beyond the network protection and isolation measures, the following controls are based on PCI DSS requirements for (a) physical access to payment card data, and (b) and monitoring. Some areas, such as the use of employees' personal devices, are internal policy.

6.5.3.1 Physical controls

- The room is a secure physical area where payment details are taken over the telephone and processed.
- Physical access to the secure room is limited, controlled and monitored.
- Physical access rights are granted based on individual job function, regularly reviewed, and revoked immediately upon termination.
- The customer service representative (CSR) must use one or two authentication factors—e.g., token, swipe card, personal code—through an access-control device to enter the room (note that while PCI DSS Requirement 9.1 mandates only one authentication factor, using multi-factor authentication is considered best practice).
- Physical access is monitored using an access-control mechanism or a video camera (or both), and the records are stored for at least three months unless legal restrictions apply.
- The access-control and monitoring systems must be protected against tampering or disabling.
- Any workstation in the secure room is locked to prevent unauthorized use.
- The CSR is not allowed to take into the room personal electronic devices; any pens and paper are replaced with personal whiteboards and dry-wipe marker pens.
- The room has no printing facilities beyond the payment terminal/POS receipts.

6.5.3.2 Procedural controls

- To enforce compliance, the CSR in the non-restricted area is not allowed to receive cardholder data from the customers.
- At the point of transaction, the CSR either transfers the call to a CSR in the secure room (potentially leaving the PBX in scope for PCI) or informs the customer that they will call them back.
- The secure room CSR either calls the customer back through a separate VoIP or POTS connection or picks up the call, which is transferred from the PBX to the secure room.
- When in possession of the card data, the secure-room CSR processes the payment via a payment terminal or a virtual terminal connected to a payment service provider. Following this, the CSR can record the transaction details on the CRM system (not represented) and securely dispose of or file any paper record or receipt

6.6 Additional Considerations

Entities may also be subject to rules from regional regulatory bodies or legal requirements that impact how they manage telephone payments. A few examples: General Data Protection Regulation (GDPR) is the European Union data-protection and privacy regulation; the U.S. Federal Act, Communications Assistance for Law Enforcement Act (CALEA), also known as the "Digital Telephony Act"; the Financial Conduct Authority (FCA) in the UK regulates banks, mutual societies, and financial advisers to protect customers and promote fair competition.

An example of impact on merchants is that those using DTMF masking/suppression for their telephone payments may also be required to accept some telephone payments verbally to support customers with disabilities or who are otherwise unable to pay by pressing their telephone keypad. Entities with these obligations will need to implement appropriate processes and technologies to secure all account data that is received verbally by call agents and systems during processing and remove all SAD upon completion of the transaction.

Entities need to understand how different technology deployments impact the data captured in call and screen recordings, and the controls that will be consequently needed to protect CHD and remove SAD from the recordings. For example:

- Recordings **will** capture clear-text CHD and SAD if spoken by the cardholder or captured through DTMF tones, and where the entire conversation is recorded.
- Recordings **will not** capture CHD or SAD if DTMF masking/suppression is implemented prior to the data reaching recording systems (when DTMF is the **only** acceptance channel).
- Recordings **may** capture CHD or SAD if pause-and-resume is used, depending on the accuracy of the pause-and-resume process.

In order to meet PCI DSS, controls should be in place to ensure that SAD is either not recorded or, if it is recorded, that it is securely deleted immediately upon authorization of the transaction. Where an entity has failed to prevent the storage of SAD after authorization, the business MUST take all possible steps to immediately delete SAD. Additionally, analysis of the failure should be performed, and corrective measures identified and implemented to prevent the failure reoccurring.

If SAD contained within audio recordings can be digitally queried—if SAD is easily accessible—it must not be stored. If these recordings cannot be data mined, storage of SAD after authorization may be permissible as long as appropriate validation has been performed. This includes the physical and logical protections defined in PCI DSS that must still be applied to these call-recording formats.

For further information on call recording, see Appendix D, “Call Recording Decision-making Process.” Consideration should also be given to the organization’s backup, failover, and disaster-recovery (DR) processes—for example, how is account data handled if the DTMF-masking or pause-and-resume technology fails? What are the alternative processes if payments cannot be taken via the primary telephone channels? Is the DR approach PCI DSS compliant? In all cases, the business needs to ensure that appropriate PCI DSS processes and controls are in place to secure the CDE and any other in-scope systems. Businesses should

also identify and continue to monitor the locations and data flows of all CHD within the telephone environment. The deployment of data-discovery tools can be useful in determining where CHD and potentially SAD exists.

Further considerations should be given to monitoring the effectiveness of the controls with, in particular, Data Loss Prevention (DLP), including leak detection and protection. A system adapted to the environment that can be considered as DLP may involve a multitude of technologies from basic firewall access control to specialized systems using data fingerprinting.

7 Third-party Service Providers

7.1 Impact on Scope

Many entities rely on third-party service providers to provide some part of their telephony services, and in some cases their entire call-handling capability. In the context of telephone-based payment card data, third-party relationships often include IVR providers, call-handling companies, call centers, hosting providers, technical support and maintenance providers, contact centers, and/or customer service providers.

The definition of service providers is available in Section 2.4.

An important consideration is that a telecommunications company providing just the communication link would not be considered a service provider for that service. This means that a carrier providing only ISDN lines and SIP trunks, with no additional services, may not have any PCI DSS responsibilities. In this scenario, the entity or service provider would consider the carrier network a public or untrusted network, and applicable PCI DSS controls would need to be in place to protect account data transmitted over such networks. Carriers or other entities providing services such as call center services, call-recording technologies, call-recording storage, hosting of call-recording technologies, or other functionality that impacts account data would be considered service providers for PCI DSS purposes.

When looking at a telecommunication company's services, organizations should have a clear understanding of the details of the services being provided—including where scope begins and ends and the demarcation points of those services. For example, two telecommunications companies might provide what appears to be the same service (telephone connectivity), with one doing so over the Internet and the other through a private network. The controls required to protect data sent over these connections will be different for each service.

If an entity is using multiple service providers, a detailed understanding of responsibilities for each provider and the entity itself is critical to ensure there are no gaps in the protection of payment card data. The entity should also understand how the different services interconnect and the methods and tools used to manage the interconnections.

The use of a third-party service provider does not relieve the entity of ultimate responsibility for its own PCI DSS compliance, nor does it exempt the entity from accountability and obligation for ensuring that its payment card data and CDE are secure. The entity must manage the relationship with the service provider as per PCI DSS Requirement 12.8, including listing of service providers, maintaining agreements and acknowledgement of responsibilities, carrying out due diligence prior to engagement, and monitoring the service provider's PCI DSS compliance status. For more information on this topic, it is recommended to review the Information Supplement, *Third-Party Security Assurance,* published by the PCI SSC.

7.2 Common Telephony-related Services

This section explores some of the services commonly provided to telephone environments, along with considerations for scoping and implementation of security controls. Most of the following services can also be hosted in house.

7.2.1 Private Branch Exchange (PBX) Services

PBX is a telephone system that switches calls within an organization. With the growth of VoIP, many organizations are looking for PBX services that can be routed via IP over private or public data networks from the service provider to the organization. Payments accepted over these PBX services are in scope for applicable PCI DSS requirements.

7.2.2 SIP Trunking

SIP trunks replace classic ISDN and T1 lines, providing connectivity between an organization's PBX systems and the service provider's SBC. SIP Trunks can connect directly to end-user devices within the organization or, alternatively, an organization's internal calls can be routed by the SIP trunk provider through a virtual hosted PBX service. As the technology matures, technical boundaries between an organization and a SIP-trunk provider may become harder to define. Scoping for these services will therefore require an understanding of how connections are made between the different entities.

7.2.3 Interactive Voice Response (IVR)

IVR technologies are used for interactions between human callers and computers and can use both voice (incorporating speech recognition) and DTMF tones to collect information from the customer in an automated process. Entities may choose to outsource their payment processing to an IVR solution provider to reduce or remove the presence of account data in the entity's environment.

7.2.4 Fraud Detection/Monitoring

The evolution of telephony technologies also supports development of fraud-detection and monitoring capabilities in telephone environments. For example, data captured from SIP headers and RTP media streams may provide useful input to a fraud-analysis and decision-making process. If any account data (PAN or SAD) is included in such an analysis, PCI DSS requirements will apply to that process.

7.2.5 Voice Analytics

Voice, or speech, analytics use specialized speech-recognition techniques to analyze and extract information from spoken data and are typically used to monitor agent quality and improve customer management. Modern solutions can analyze call data in real-time or be combined with transcription and storage services to perform detailed data mining of call transcripts or audio recordings. As these tools are designed to categorize and locate specific types of data, their use in environments where account data is present needs to be carefully controlled and monitored.

7.2.6 Call Recording

The example provided in Section 6.5.1 (Diagram 9, Pause-and-resume) only considers an implementation of call recording WITHIN the entity. Diagram 11 below represents a number of entities that outsource call recording using the same Level 1 Service Provider.

Note: *Storing SAD after authorization is not allowed—refer to Appendix D, "Call Recording Decision-making Process."*

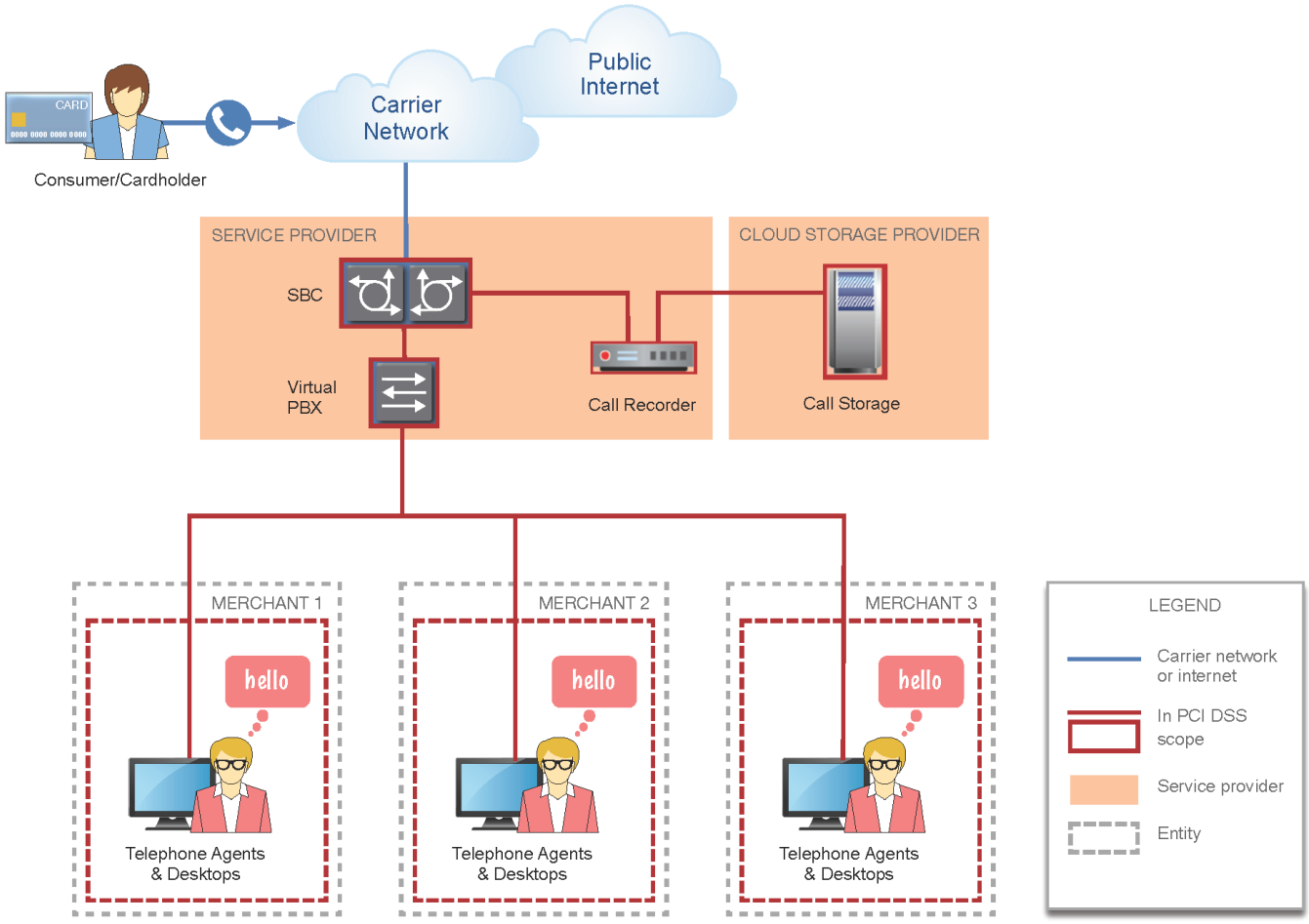


Diagram 11: Outsourced call recording

The data from the entities may be merged at the level of the service provider and the cloud storage provider. Beyond the service-provider-specific PCI DSS requirements, the assessor assessing the entities and the entities themselves may verify that the provider complies with the requirements in PCI DSS Appendix A1, "Additional PCI DSS Requirements for Shared Hosting Providers."

Assessors assessing the service provider should consider whether the service provider or the cloud-storage provider should comply with the requirements in PCI DSS Appendix A1, "Additional PCI DSS Requirements for Shared Hosting Providers," by considering how they are servicing the entities, and protecting each entities data, where shared services are at play.

7.2.6.1 Selecting a call-recording service

PCI DSS Requirement 12 states that the entity must maintain and implement policies and procedures to manage service providers with whom cardholder data is shared, or that could affect the security of cardholder data. This includes a written agreement by service providers acknowledging that they are responsible for the security of cardholder data they possess or otherwise store, process, or transmit on behalf of the customer. If the entity chooses to suppress or mask the payment card data before it is recorded, these requirements may not apply and a non-PCI DSS recording service may suffice. However, if payment card data is not suppressed or masked, or if it is possible that payment card data may be accidentally recorded, the entity should choose a PCI DSS compliant call-recording solution including the protection and secure deletion of the data in line with the entity's data-retention policy.

Appendix A: Glossary / Terminology

The *PCI DSS Standard Glossary, Abbreviations and Acronyms* is available on the PCI Security Standards Council website[6], defines many of the terms used in this document. Additionally, the following terms and abbreviations are used throughout:

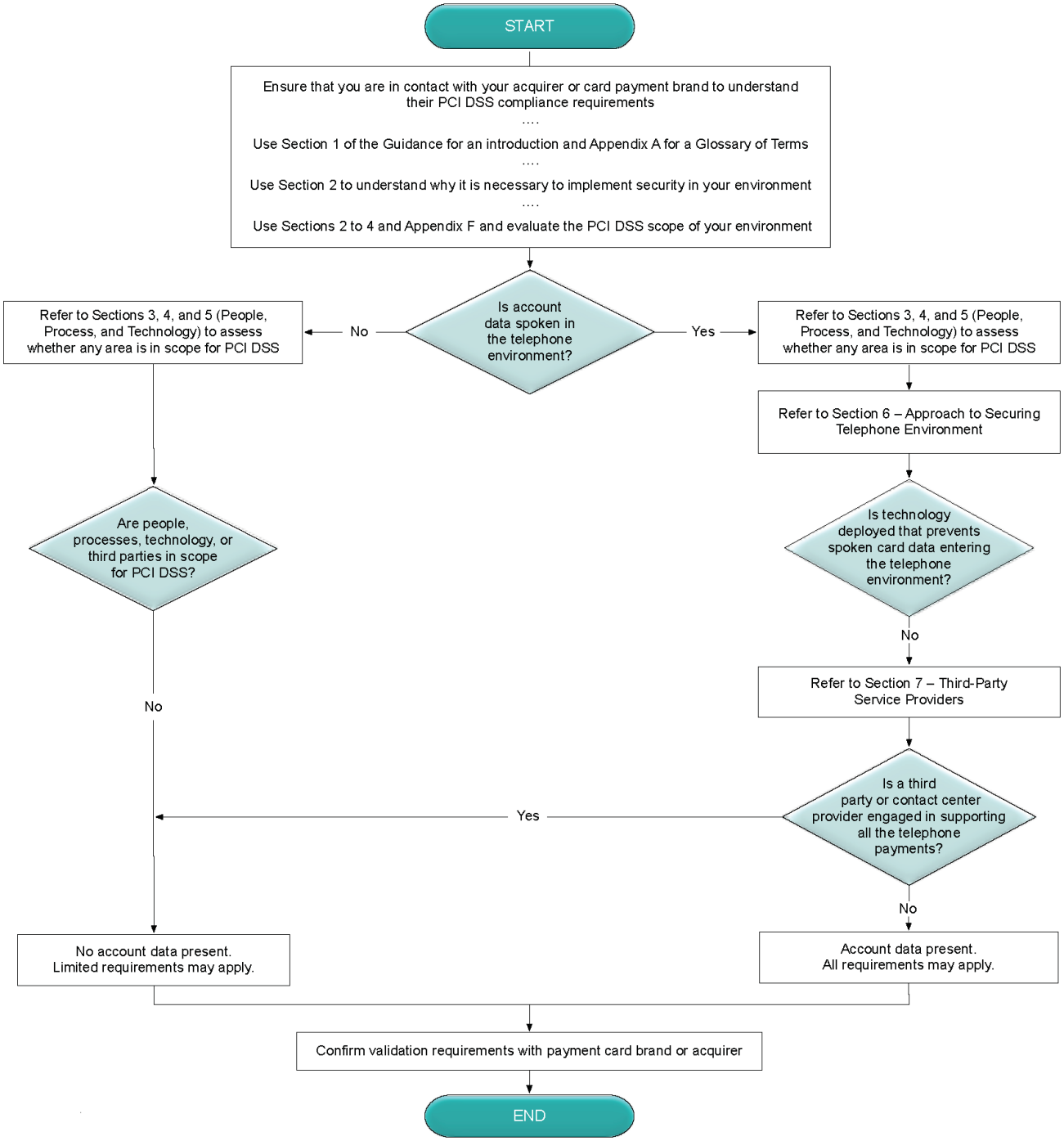
Term	Definition
3DS	EMV® Three-Domain Secure (3DS) is a messaging protocol that enables consumers to authenticate themselves with their card issuer when making card-not-present (CNP) e-commerce purchases. The additional security layer helps prevent unauthorized CNP transactions and protects the entity from CNP exposure to fraud. The three domains consist of the entity/acquirer domain, issuer domain, and the interoperability domain (e.g., payment systems).
ACD	Acronym for "automatic call distributor." A programmable device deployed in the telephone or data network capable of directing telephone calls (data) to a predefined termination point. Also referred to as a telephony switch.
Agent	Person or persons employed by a business whose role it is to make or take telephone calls. Also referred to as operator or customer service representative.
Agent desktop	An agent's computer connected to a network.
Call flow	A road map of how calls will be handled from the moment they enter the telephone system to the end of the call. Call flows can be used to handle even the most complex call scenarios.
Call recording	General description of the file containing the recording of a telephone call. It is also referred to as: voice recording.
Carrier	A telecom carrier is a company that is authorized by regulatory agencies to operate a telecommunications system.
CRM	Acronym for "customer relationship management" system. A customer or booking database or reservation system.
CSR	"Customer services representative." See the term "Agent" as the terms are used interchangeably in this document.
Demarcation point	In telephony, the demarcation point is the point at which the public, switched telephone network or Internet telephony service provider network (VoIP) ends and connects with the customer's on-premises network. The demarcation point is also the dividing line that determines which entity is responsible for installation, maintenance, and service. A network interface device can often serve as the demarcation point.

[6] https://www.pcisecuritystandards.org/pci_security/glossary

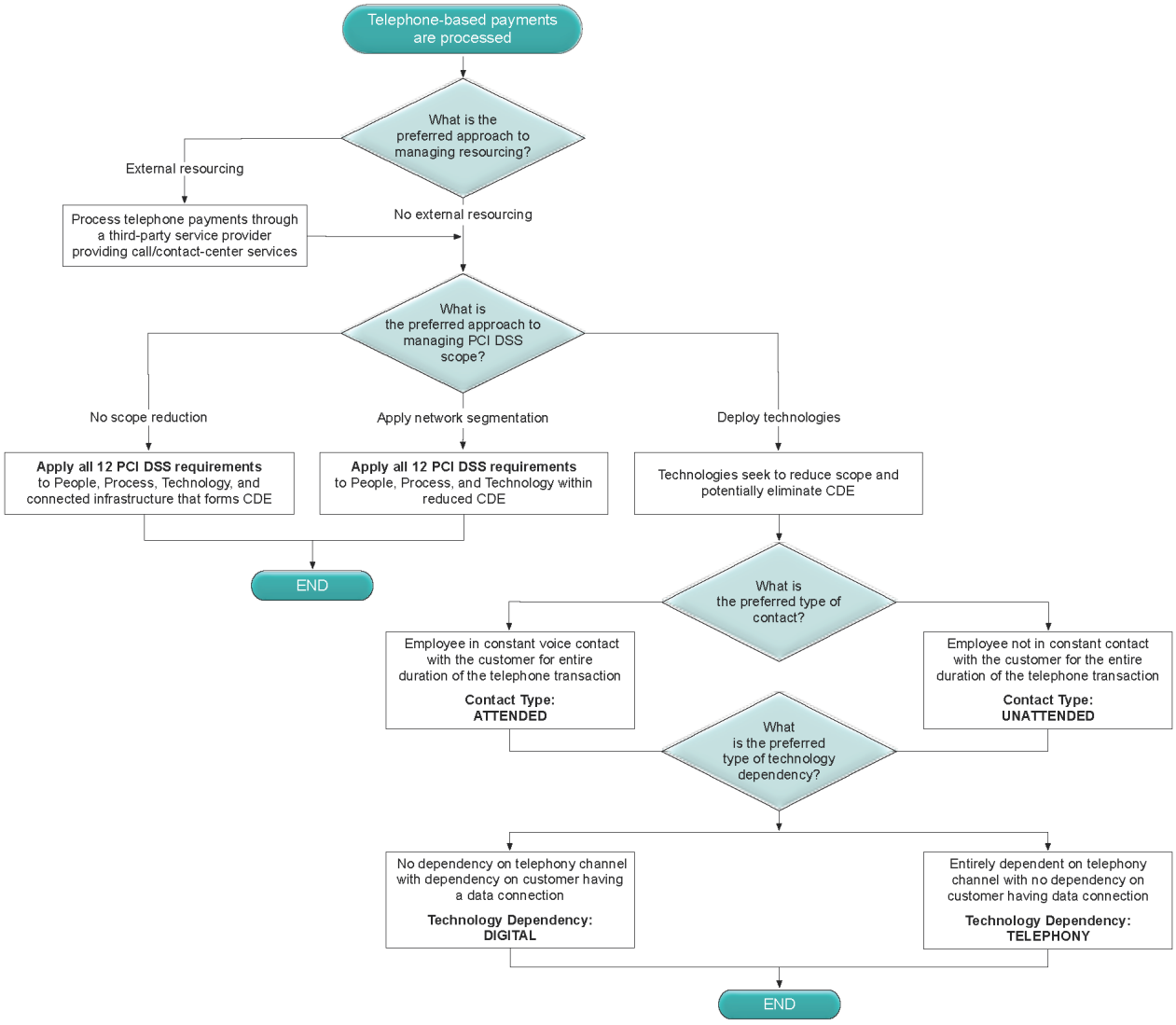
Term	Definition
DTMF	Acronym for “dual-tone, multi-frequency.” A telecommunication signaling system using the voice-frequency band over telephone lines between telephone equipment and other communications devices and switching centers. DTMF is also known under the trademark “Touch Tone” for use in push-button telephones.
EMV	Acronym for “Europay, MasterCard and Visa.” EMV is a global standard, originally created by these three companies, for processing chip-based payment card transactions.
ISDN	Acronym for “integrated services for digital network.” Described as a set of communication standards for simultaneous digital transmission of voice, video, data, and other network services over the traditional circuits of the public switched telephone network (PSTN).
IVR	Acronym for “interactive voice response.” An automated process that allows the customer to make choices by pressing the required digit on their telephone handset.
Pause-and-resume	General description of manual or automated applications that pause and resume the call-recording application at a point during the call.
PBX or PABX	Acronym for “private branch exchange or private automatic branch exchange. A private telephone network used within an organization.
POTS	Acronym for “plain old telephone service.” Describes the voice-grade telephone service employing analog signal over copper cables.
PSP	Acronym for “payment service provider.” Sometimes referred to as “payment processor” or “payment gateway.”
PSTN	Acronym for “public switched telephone network.” Describes all the circuit–switched telephone networks operated by telephony operators at various levels, from national to local, providing infrastructure and services for public telecommunication.
RTP	Acronym for “real-time transport protocol.” Provides end-to-end network transport functions suitable for applications transmitting real-time data, such as audio, video or simulation data, over multicast or unicast network services. Secure real-time transport protocol (SRTP) is a protocol that can provide confidentiality, message authentication, and replay protection for RTP traffic. See also *SRTP.*
Screen recordings	Recordings or screenshots of agent desktop screens showing the data that they are capturing and/or entering into an application, often a CRM system or customer database.

Term	Definition
SBC	Acronym for “session border controller.” A dedicated hardware device or software application that provides security, interoperability, routing and other functions in a Session Initiation Protocol (SIP) network. In general, it governs the manner in which phone calls are initiated, conducted, and torn down.
SIP	Acronym for “session initiation protocol.” A multimedia communications protocol used for controlling communication sessions, including voice and video calls over internet protocol (IP) networks. A SIPS (session initiation protocol secure) URI* can be used to specify that the resource be contacted securely. This means, in particular, that TLS is to be used between the user-agent client (UAC) and the domain that owns the URI. * *URI: Acronym for uniform resource identifier. It is a string of characters to identify a resource. The syntax is defined by RFC 3986. A URL is a type of URI.*
SRTP	Secure Real-time Transport Protocol (SRTP) is a protocol that can provide confidentiality, message authentication, and replay protection for RTP traffic. See also *RTP*.
Switch	General term given to a device that directs telephone calls or data to a single or multiple predefined destination within a network.
T1 line	A T1 line is a dedicated transmission connection between a client and a service provider.
Telephone environment	General term used to describe the system components, networks, processes, and personnel that comprise an environment within which a card-not-present transaction is performed by telephone.
Telephone service provider (TSP)	Company providing telecommunications services such as telephony and data communications access. Also known as: communication service provider (CSP), digital service provider (DSP), telephone company, telco, or telecommunications operator.
VoIP	Acronym for “voice over internet protocol.” A method that enables use of Internet Protocol (IP) as the transmission medium for telephone calls by sending voice data in packets over IP networks. VoIP uses signaling protocols such as SIP (or SIPS) as a session initiation and session control, and real-time media and data transmission protocols such as RTP or SRTP. In addition, VoIP relies on various open-source and proprietary audio and video codecs that optimize the media stream based on application requirements and network bandwidth.

Appendix B: Document Quick-reference Guide



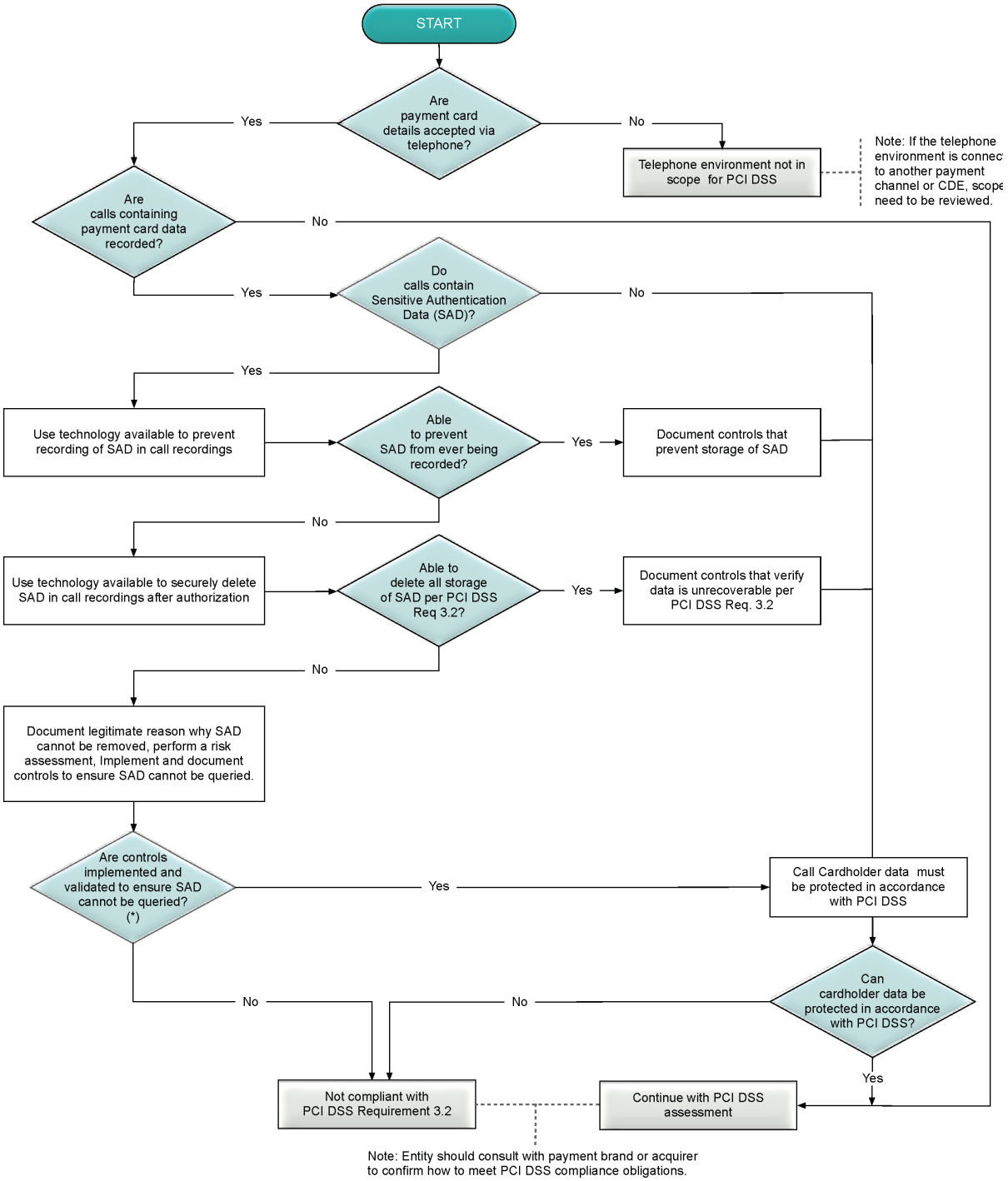
Appendix C: Payment Call Environment-identification Tree



Appendix D: Call Recording Decision-making Process

D.1 Flowchart

The flowchart below provides a high-level decision-making process for call recordings.



** See D.2 regarding SAD in call recordings.*

D.2 Regarding SAD in Call Recordings

D2.1 Entities that Issue Payment Cards or Perform/Support Issuing Services

Entities that issue payment cards or that perform or support issuing services are allowed to store sensitive authentication data ONLY IF they have a legitimate business need to store such data and they store it in accordance to PCI DSS requirements.

D2.2 All other Entities

For all other entities, every possible effort must be made to eliminate sensitive authentication data from the telephone environment. If an organization has a legitimate constraint that prevents it from removing SAD from its recordings, the organization should discuss this with its acquirer and/or payment brand. In these circumstances, there must be a detailed justification why sensitive authentication data cannot be eliminated (for example, a legislative or regulatory obligation[7]) and a comprehensive risk assessment performed at least annually and upon significant changes to the environment. The detailed justification, risk-assessment results, and documentation of the controls in place (and validated) to ensure that SAD cannot be queried must be made available to the acquiring bank and/or payment card brand as applicable to allow them to accept or reject the solution in place.

If sensitive authentication data cannot be eliminated, it must be secured in a manner consistent with PCI DSS and must not be able to be queried. Data that can be retrieved through use of a search tool or by issuing a system instruction/task or a set of instructions/tasks is considered able to be queried. 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

[7] PCI DSS does not supersede local or regional laws, government regulations, or other legal requirements.

D2.3 Rendering SAD Non-queryable

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

For SAD to be considered "non-queryable," it must not be able to be retrieved or listened to using the types of functions listed above.

An example of an approach that may help to render SAD non-queryable could include, but not be limited to, the following steps:

a) Remove call recordings from the call-recording solution. Ensure deleted recordings cannot be recovered from the call-recording system.

b) Take the call recordings offline. For example, store the call recordings on a system that is not connected to the network, or store recordings on offline media.

c) Physically secure the call recordings. For example, lock physical media in a safe or locate offline system in a secure area with restricted access.

d) Enforce dual-access (as per "Dual Control" in the PCI DSS glossary) controls to the call recordings.

e) Allow only single call recordings to be retrieved or listened to, or only as specifically defined and authorized by a senior manager.

f) Assign responsibility for retrieved or listened-to call recordings and permit access only for the reason retrieved. Ensure recordings are securely deleted or destroyed when no longer needed.

Note that rendering SAD non-queryable could be assimilated to a compensating control. This would therefore need to be documented as required by PCI DSS.

Appendix E: Further Considerations on VoIP

Voice over IP (VoIP) can be used by VoIP telephones, mobile phones, and mobile or traditional computer software, mainly to transport voice streams. It is implemented using protocols based on open standards or proprietary protocols.

E.1 Protocols, Ports and Network.

VoIP is generally implemented using two main protocols: H.323 and Session Initiation Protocol (SIP). Vendors using "unified communications" can include further protocols due to video (telepresence) and instant-messaging (IM) capabilities. Some examples of other protocols are: Real-Time Transport Protocol (RTP), H.248, Skype protocol (proprietary), Jingle.

H.323 and SIP each use two separate data streams, one for the signaling and one for the media (this can be voice data). The signaling stream will utilize well-known ports, often over Transmission Control Protocol (TCP). The media stream can tolerate the loss of some packets; it uses User Datagram Protocol (UDP) transport layer which is dynamic in nature.

This means that traffic-filtering devices need to be configured to allow a much greater range of ports to allow the traffic to pass correctly. Implementing Network Address Translation (NAT) can add to these complications because the devices may not necessarily know where to send traffic that is seen.

Finally, the use of UDP may render the detection of malicious content or payload more difficult.

Firewalls and network devices should be VoIP-aware so they are capable of monitoring the VoIP traffic and dynamically open the necessary ports and network translations to facilitate the traffic. This means that firewalls can still be secure, maintaining the state of the traffic by only opening ports when required for the voice call.

E.2 VoIP Attacks and Vulnerabilities

VoIP equipment and software are susceptible to vulnerabilities that could allow someone with malicious intent to gain access to your network, intercept and gather customer data, or initiate a denial-of-service attack.

It is important that these devices and software are included in the vulnerability-management process with, in particular: monitoring vulnerabilities, internal and external vulnerability scanning and patching.

In addition to vulnerability management, the configuration of VoIP devices and software must be secure, including, but not limited to disabling unnecessary services and accounts, changing default passwords, and implementing a strong password policy. Securing remote access, whether Internet or shell access, is paramount and must be done in accordance with PCI DSS.

E.3 Encryption and Eaves dropping

Securing VoIP phone data is conceptually easier than traditional telephone signals using encryption or secure protocols such as SRTP. For example, however, many consumer VoIP devices do not support encryption of the signaling or the media streams. We have already mentioned that successfully implementing secure protocols across several telecom carrier may present some challenges.

A lack of encryption may result in eavesdropping on VoIP calls when access to the data network is possible. Packet analyzers such as, for example, Wireshark or tcpdump, make capturing VoIP conversations and data trivial.

E.4 Unified Communications

The concept of unified communications begins to integrate communication features of voice/video communications. It is not unusual for vendors to tightly integrate instant messaging, video or telepresence, telephony, facsimile, electronic mail and other communication services into clusters of servers that are not easily segmented or isolated from one another. As a result, entities can find that their only option to minimize the PCI scope of their VoIP environment is to implement multiple instances of in-scope VoIP and out-of-scope VoIP.

Appendix F: Further Scoping Considerations

F.1 Introduction

The aim of this appendix is to highlight a few scenarios the entity and the assessor should be aware of to help them defining the scope for PCI DSS.

F.2 SIP Redirection

When a service provider is used by the entity to process payments, it is important to review how the service is implemented as it can impact the PCI DSS scope. In the following examples, the entity uses a service provider that will capture the cardholder data via an IVR system or DTMF capture, or any other technology, and process the payment on behalf of the entity. All the data the entity should receive is a truncated version of the PAN or a tokenized PAN with the transaction data and an acknowledgement of the transaction result. The service provider location and the account data flow must be understood. These examples are provided to highlight that SIP redirection does not necessarily completely remove the entity's infrastructure from PCI DSS scope.

In the Diagram F1 below, the service provider is situated close to the carrier network and the account data will be "intercepted" before it reaches the entity's infrastructure rather than being redirected from it. This redirection should not have any impact on the entity's infrastructure scope for PCI DSS.

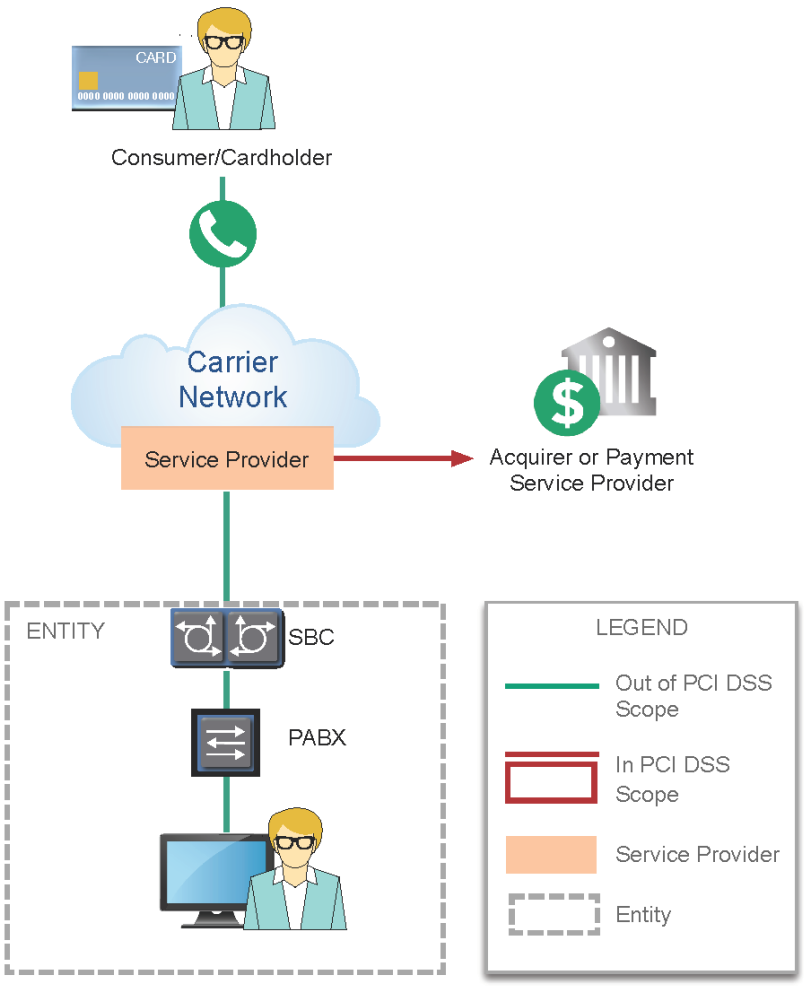


Diagram F1: The account data is used before it reaches the entity's infrastructure

In Diagram F2, the account data is redirected to the service provider by a device hosted within the entity's infrastructure. If a service provider supplies a device onsite, upstream of an SBC or other telephony infrastructure, to redirect or re-invite the call away to carrier network service, this device is in scope for PCI DSS requirements. If this device were compromised, a simple carrier preselect (CPS) or least-cost routing (LCR) alteration could re-route telephony through to a snooping service prior to delivery to the carrier IVR or DTMF capture service.

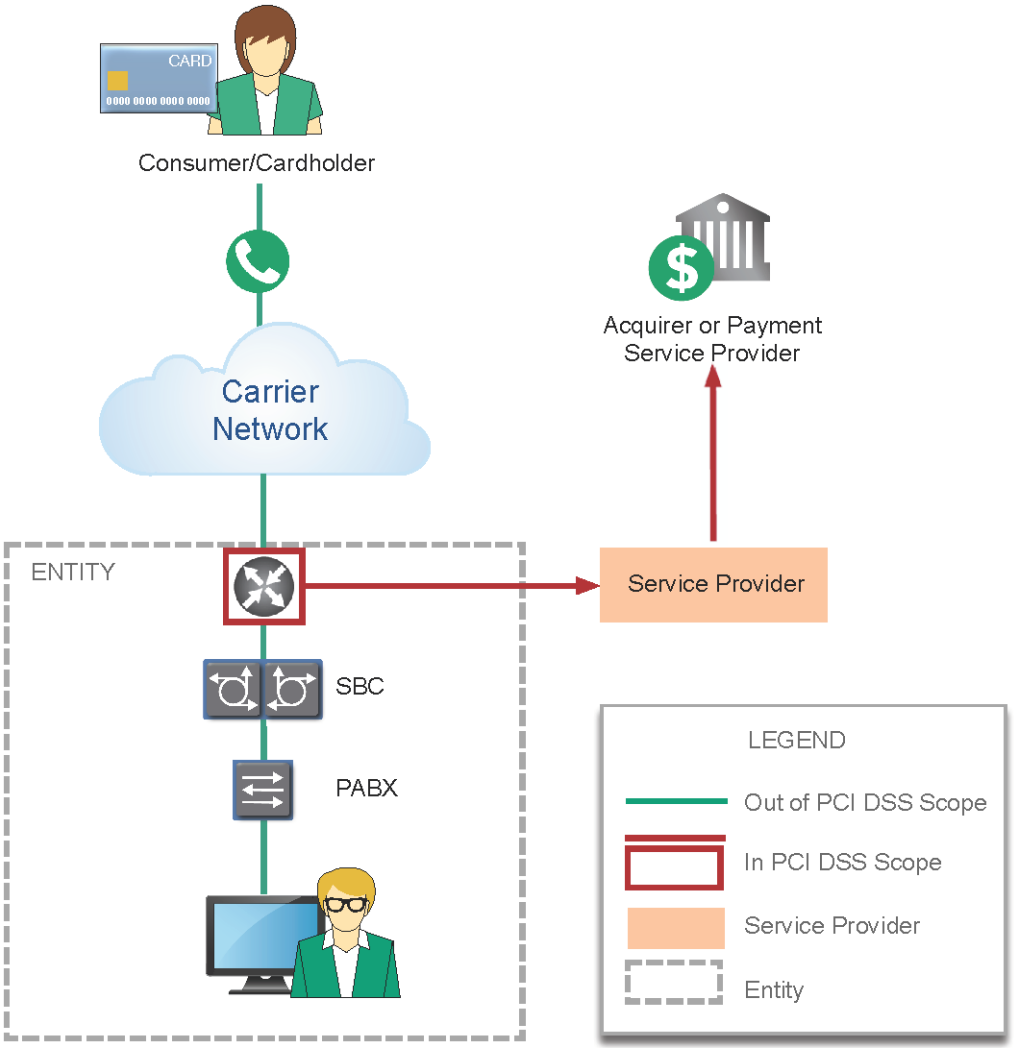


Diagram F2: The account data is redirected from the entity's infrastructure

If account data is transmitted via this device or the device transfers the call at point of transaction, it is part of a payment card data environment. The devices, premises, and networks connected to the redirection device may therefore be in scope for PCI DSS requirements. The entity and assessor should refer to the section, "Scope of PCI DSS Requirements," of PCI DSS and the Information Supplement, *Guidance for PCI DSS Scoping and Network Segmentation*, to evaluate the scope for PCI DSS. In assessing the device, the aspects to be considered may include (but are not limited to): access control (local or remote), configuration/hardening, patching, change management, security testing, physical security, logging/monitoring, service-provider management.

When payment card data is redirected to a service provider over a public network, whatever the format (voice, video, picture), it is in scope for applicable PCI DSS controls as the transmission is initiated by the entity—or, by delegation, the service provider.

The payment card data must be protected by strong encryption. This can be done by encrypting the data itself or by using a secure connection via, for example, the use of a VPN or a secure protocol—e.g., SRTP, knowing that encryption using such a protocol is difficult across several telephone operators. Also, the

redirection mechanism must be protected to ensure that the data is not redirected to a rogue site.

F.3 Simple Telephone System – Further Examples

In complement to Section 2.3.1, "[PCI DSS Applicability to] Simple Telephone Environments," the following diagrams represent further examples of possible implementations.

Diagram F3 shows a scenario where the payment details are taken over POTS or VoIP and processed through a payment terminal connected to a payment processor via IP. The payment terminal and the connection to the payment processor would be in scope for PCI DSS.

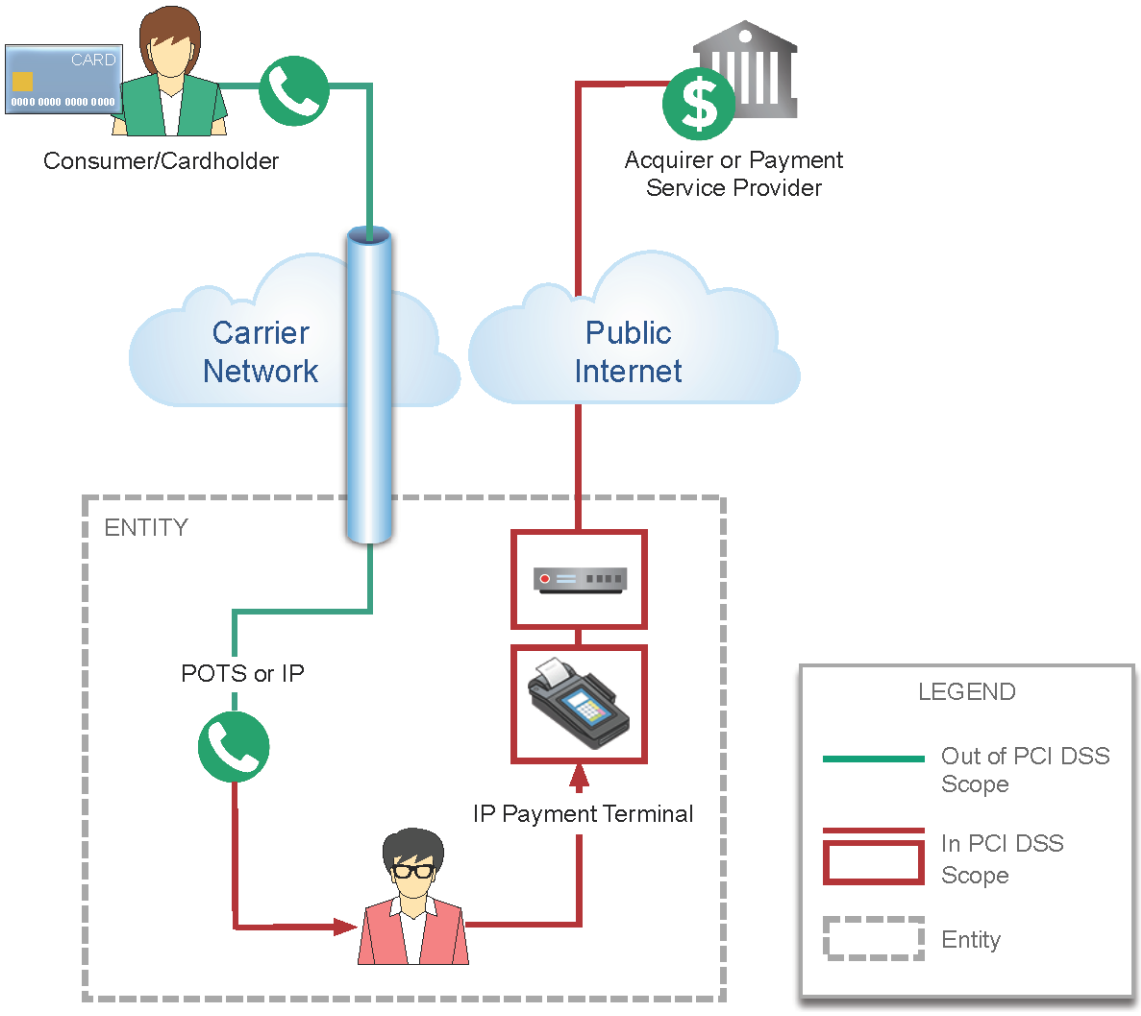


Diagram F3: POTS or VoIP telephone and payment terminal connected via IP

Diagram F4 shows a scenario where the payment details are taken over POTS or VoIP and processed through a virtual terminal hosted by a payment service provider via Internet. The entity's computer would be in scope for PCI DSS.

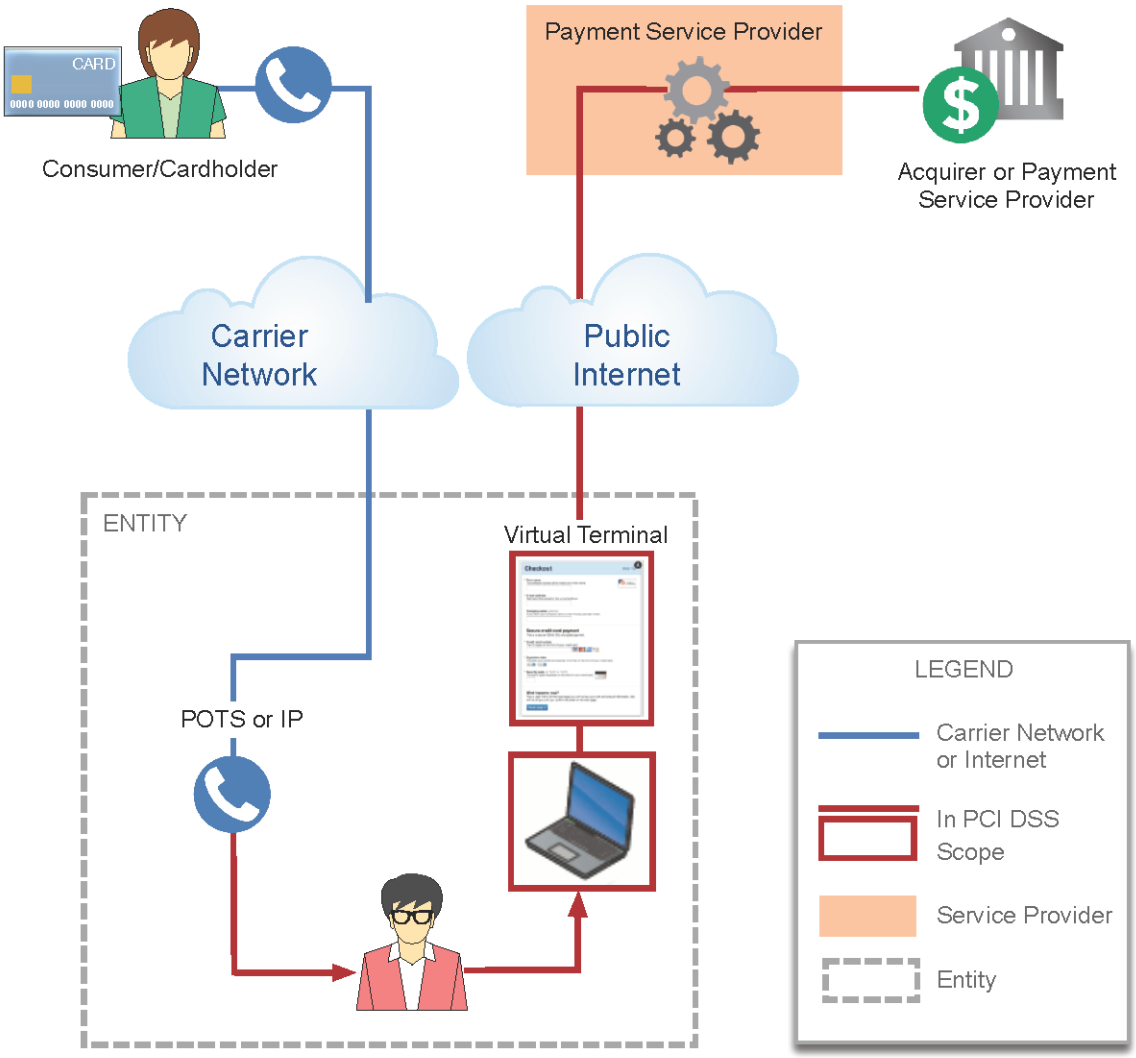


Diagram F4: POTS or VoIP telephone and virtual payment terminal from a payment service provider

F.4 Payment Terminal Connected to a Network Via a VoIP Telephone Socket

Some VoIP telephones provide the user with multiple connections sockets (e.g., RJ-45) to an IP network. One will be for telephony, the other(s) to connect devices such as, for example, a computer or a payment terminal to the office network. The telephone device acts as a switch or a router. Depending on the configuration of the telephone device, the telephony and secondary network segments could be either the same or segregated.

In the example below (Diagram F5), the entity allows customers to pay via a website. The website infrastructure is completely segmented from the office network. No payment card data is captured using telephones. The operators receive the payment card data to process via a printed payment card data extract and process the payments using a PCI P2PE payment terminal connected to the VoIP telephone.

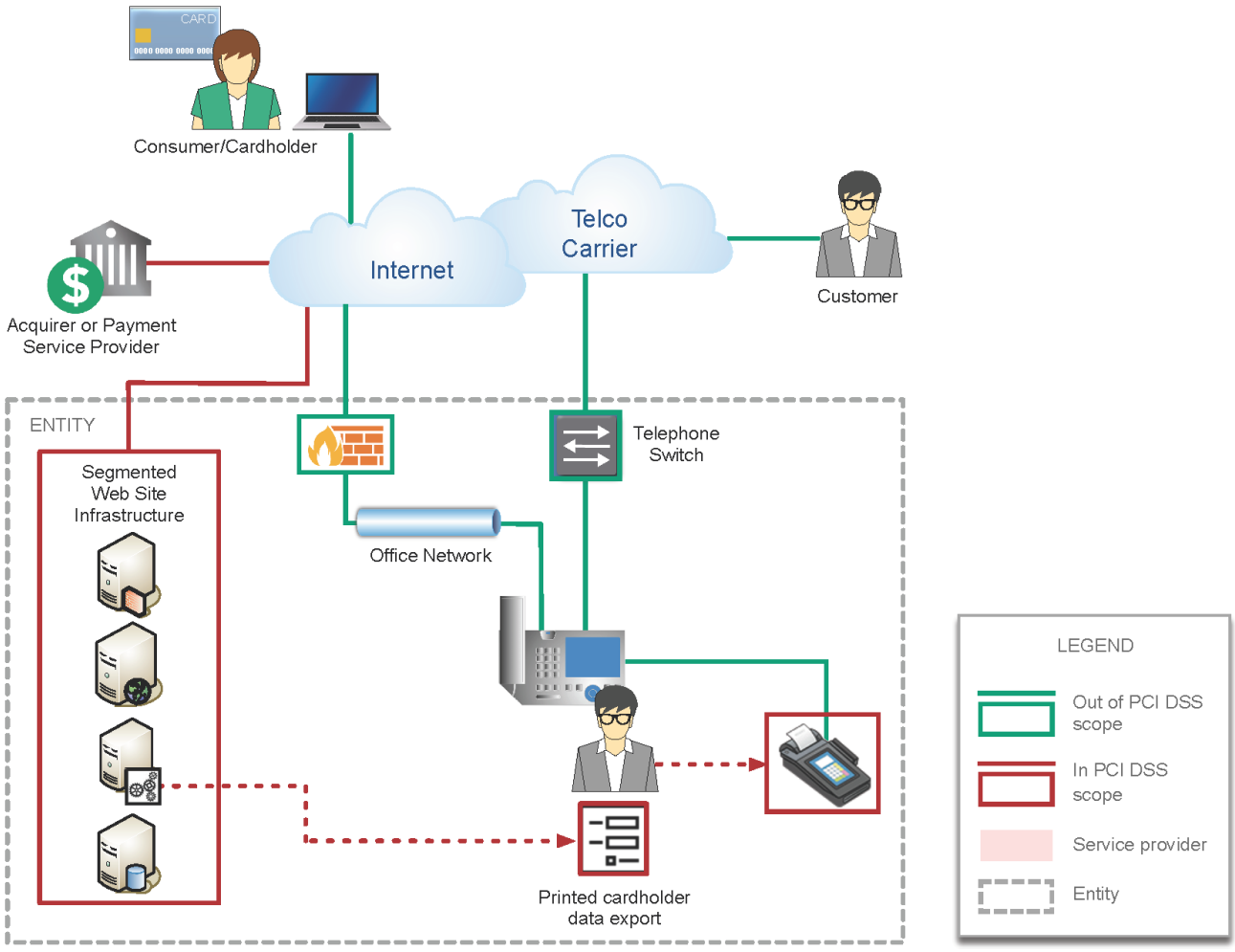


Diagram F5: Payment terminal connected to a network via a VoIP telephone socket

This type of solution ensures that the card account data is encrypted between the PCI P2PE payment terminal used to initiate the payment with the acquirer. The networks connected to the telephone, including the telephone itself, are kept out of scope for PCI DSS.

In this scenario, the web site infrastructure, the PCI P2PE payment terminal, and the printed payment card data extract are in scope for PCI DSS.

F.5 Use of "Chat" for Card Payments

When entities consider using their telephone environments to support customer communication using a "chat" application, it is worth highlighting once again that PAN cannot be sent unprotected. This applies to all end-user messaging technologies.

If an entity requests PAN via end-user messaging technologies, the entity should provide a tool or method to protect these PANs using strong cryptography or render PANs unreadable before transmission.

The data transmitted would be in scope for applicable PCI DSS controls. The eventual transmission of SAD would need special attention, especially its secure deletion after authorization.

Appendix G: Other PCI DSS Reference Documents

Reference documents from the PCI SSC Small Merchant Taskforce useful to simple and complex telephone environments:

- *Guide to Safe Payments*
- *Common Payment Systems*
- *Questions to Ask Your Vendors*
- *(Small Merchant) Glossary of Payment and Information Security Terms*

These resources are available from the Document Library on the PCI Security Standards website: https://www.pcisecuritystandards.org/document_library, filtering with "Small Merchants."

Reference documents useful to simple and complex telephone environments.

- *PCI DSS Requirements and Security Assessment Procedures*
- *PCI DSS Quick Reference Guide*
- Prioritized Approach for PCI DSS
- *PCI SSC Prioritized Approach Tool*
- *Understanding SAQs for PCI DSS*
- *PCI DSS SAQ: Instructions and Guidelines*
- Information Supplement: *Guidance for PCI DSS Scoping and Network Segmentation*
- Information Supplement: *PCI SSC Cloud Computing Guidelines*
- Information Supplement: *Third-Party Security Assurance*
- *Connected-to Service Providers*

These resources are also available from the Document Library on the PCI Security Standards website: https://www.pcisecuritystandards.org/document_library.

Frequently Asked Questions: The following is a non-exhaustive list of FAQs that may apply to telephone-based payments.

- FAQ #1153: "How does PCI DSS apply to VoIP? "
- FAQ #1210: "Are audio/voice recordings permitted to contain sensitive authentication data?"
- FAQ #1156: "Are call center environments considered "sensitive areas" for PCI DSS Requirement 9.1.1?"
- FAQ #1069: "Does PCI DSS apply to paper with cardholder data (for example, receipts, reports, etc.)?"
- FAQ #1139: "Can I fax payment card numbers and still be PCI DSS Compliant? "

The FAQs are available on the PCI SSC web site: https://www.pcisecuritystandards.org/faqs

Glossary: Payment Card Industry (PCI) Data Security Standard Glossary, Abbreviations and Acronyms: https://www.pcisecuritystandards.org/pci_security/glossary

Appendix H: Contributing Organizations

The PCI SSC would like to acknowledge the contribution of the following organizations in the drafting and preparation of this document:

Adobe Systems Incorporated
Aeriandi LTD
AIG Global Services
Bell Canada
BT PLC.
California State University, Fullerton
Coalfire Systems
Compliance3
Conduent
Convergys Corporation
Crowe Horwath LLP
Dignity Health
Eckoh UK Ltd
Elavon Merchant Services
Federation Des Caisses Desjardins Du Quebec
FortConsult A-S
Gap Inc.
Google
HP Inc.
Information Risk Management (IRM)
IQ Information Quality
Johnson & Johnson Services
Navient Solutions, LLC
NCC Group PLC
NTT Security Ltd.
Oklahoma State University
Optiv Security
PetSmart
Price and Associates CPAs, LLC, dba A-LIGN
Schellman & Company, LLC
Sec-1 Ltd.
SecureCo Pty Limited
Security Metrics
Semafone Limited
SERVIRED
Sirius Computer Solutions, Inc.
Spectrum Health System
Sprint Nextel
Syntec Ltd
The Liquor Control Board of Ontario
Trustwave
U.S. Payments
Uber Technologies, Inc.
United HealthCare Services, Inc.
United States Postal Service
Vendorcom
Verizon/CyberTrust
Vodafone Ltd
West Monroe Partners, LLC
Whirlpool Corporation

About the PCI Security Standards Council

The PCI Security Standards Council is an open global forum that is responsible for the development, management, education, and awareness of the PCI Data Security Standard (PCI DSS) and other standards that increase payment data security. Created in 2006 by the founding brands American Express, Discover Financial Services, JCB International, Mastercard, and Visa Inc., the Council has more than 700 Participating Organizations representing merchants, banks, processors, and vendors worldwide. To learn more about playing a part in securing payment card data globally, please visit: pcisecuritystandards.org.