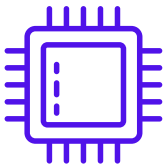

Sycurio.

Assessing the scope of PCI DSS in the contact center.

A short guide for PCI professionals

Understanding and mapping the flow of payment card data in contact centers.

Contact centers are complex and dynamic environments with high levels of human involvement and interaction with systems - this can present a range of challenges when assessing compliance with PCI DSS when handling card-not-present (CNP) payment transactions. It is widely recognized that taking payments in a supervised and managed contact center even with 'clean room' methods using spoken number 'listen and transcribe' is a high-risk activity. And, in today's changing world post COVID, with the accelerating number of remote agent environments, it is inherently insecure.

Payment card data such as primary account number, expiry and cardholder verification number is often introduced to the voice environment in two distinct forms:

1. **spoken digits**
2. **tones generated by telephone keypad input - known as Dual-Tone Multi-Frequency or DTMF**

DTMF is also used extensively across interactive customer experience platforms as a method of navigation,making encryption of all DTMF signals inappropriate and impractical in the contact center.

In addition, in regulated markets and in compliance with merchant policies, telephone conversations are often required to be recorded in their entirety. This often results in spoken digits and DTMF signals that contain payment card data are captured inadvertently in the process.

'DTMF masking' - in contact centers

Processing CNP payment card data using 'DTMF masking' is often presented as a comprehensive security solution. The capabilities of the technologies involved, the merchant telecoms environment, and how it is deployed to ensure that PCI DSS controls can be successfully implemented and managed still require careful consideration.

VoIP, SIP & DTMF - analog data in a digital telephony system

In VoIP & SIP based telephony, DTMF can be transmitted in both the media and the signal channels, so identifying which channel is being employed to carry payment card data is essential in understanding the scope for assessing PCI DSS controls.

DTMF masking & 'bleed' - residual card holder data in contact center systems

Due to the analog format of DTMF it may be present in call recordings, caches and buffers, and other contact center systems even after masking or suppression operations - this is termed 'DTMF bleed'. The identification of the presence of residual DMTF data in recordings requires specialized (but easily obtainable) software and a brief audio analysis as it cannot be distinguished by the human ear.

PCI DSS compliance - potential 'workarounds' in the contact center

'Pause & Resume'

Pausing of the call recording during the payment transaction to avoid capturing the payment card data is a common method of attempting to comply with the PCI DSS. The process is often manual and relies heavily on the agent's diligence to be effective in not recording (hence storing) payment card data (PCI DSS V4.0 3.3.1). Where 'pause and resume' is in operation, the agent, their equipment, environment, recording systems and call recordings as well as all connected systems still remain in scope for the application of appropriate controls.

Call recording encryption

Where call recording is undertaken, encryption and access control is common practice – when it is used for attempted compliance with PCI DSS it is highly problematic. The PCI DSS (both v3.2.1 requirement 3.2 and v4.0 requirement 3.3.1) explicitly state that Secure Authentication Data (SAD) must not be retained under any circumstances after authorization. Encrypted call recordings that contain SAD i.e. the card verification value / code (CV2) stored post authorization do not and can not comply with the PCI DSS.

Transfer to IVR automated payment systems

The use of automated payment systems in contact center environments is relatively common practice. The process in brief is the agent transfers the call to an independent system, the caller presents their payment card details (via DTMF or speech recognition), the transaction is processed through through the payment service provider (PSP), the caller is then transferred back to the agent. Using this payment method, the payment card data may be transmitted through separate telephony, networks and services from the original call path. This brings the automated payment system, it's additional components and nested elements, plus the network and telephony services as well as any connected system (which could be the entire company-wide network) into scope for the application of appropriate controls.

PCI DSS scope guide.

Contact center Card Data Environment (CDE)

Telecommunications Infrastructure

Telco · PSTN · ISDN · VoIP · UCaaS · Voice Gateway · Switch · Session Border Controller · PBX · IP Phone System

Card Holder Data (CHD), Secure Authentication Data (SAD) and Card Verification Values / Codes (CV2) are transmitted and potentially cached/ stored through the merchant telephony infrastructure using DTMF in the signal and/ or media channels. Carrier systems on merchant premises are very likely to be considered in scope for assessment.

Contact Center Operations Infrastructure

On Premises CC Software · CCaaS · Servers · CRM System · Call Recording · IVR System · Speech Recognition · Digital Services

Merchant contact center operations systems have elements that are integrated with, or transmit, process, or store payment card data. This brings them in scope.

Network Environment

Physical Networks · Firewalls · Servers · Routers · Auth

Network and authorisation services that support contact center operations and telecom systems. And, 'edge-of-network' security for remote agents and employees may be considered in scope.

Software & Hosted Services Environment

Desktop Applications · Served Applications · Hosted Applications · Mobile Applications · API · Databases · Storage

The transmission, processing, and storage of payment card data through desktop & served applications and their connected and nested services may be considered to be in scope.

Physical Environment

Premises · CCTV

The physical contact center and remote agent home environments present a wide range of opportunities for the exposure of payment card data.

Agent & Remote Agent

Agent · Remote Agent · Telephone Equipment · Computer Equipment · Payment Terminal · Home Workspace · Home Network

Agents, their equipment and potential home environment are in scope. Particular attention is required when assessing remote agents and their home environment security.

Agent Attended Payment Links

Messaging Applications · Email · SMS · Social Channels

The use of digital payment links in exception handling and in omnichannel contact centers are increasingly common. The payment link generation system and the channels of delivery should be considered in scope.

Automated Digital Payment Systems

IVR Systems · Chatbot Systems · Voicebot Systems

Automated and agentless payment systems using DTMF, speech recognition and chat-type interfaces should be considered in scope, especially due to potential inadvertent submission of payment data. Their nested third-party services and components may also be considered in scope.

Payment Services Integration

PSP · Tokenization

The PSP and tokenization systems integration should be considered to be in scope.

Any Connected System
PCI DSS compliance scope is "infectious" and it should be highlighted that any connected system to any of the below in scope environments is automatically deemed in-scope to PCI DSS, thus minimizing scope reduction is critical to a successful PCI DSS compliance initiative.

Sycurio - a powerful toolset for contact center PCI DSS compliance.

Reducing PCI DSS scope in contact centers

Sycurio's platform and technologies are used by enterprises to remove their telecommunications, contact center systems, network & software infrastructure, and agents from the scope of PCI DSS.

All payment transactions are completed inside Sycurio's PCI DSS Level 1 infrastructure bypassing the merchant entirely and moving their contact center PCI DSS reporting requirements to 'SAQ-A' - with Sycurio providing the merchant with the annual Attestation of Compliance (AoC) certificate.

Our patented payment capture methods are used globally across all enterprise topologies and are directly integrated with telecommunications carriers, Contact Center as a Service (CCaaS) and Unified Communications as a Service (UCaaS) platforms and services.

Sycurio's payment link capability enables merchants to request and process digital payments without accessing payment card data directly - removing payment process exception cases, automated telephone & ecommerce systems and agents from the scope of PCI DSS.

Sycurio enterprise deployment

Sycurio is a self-contained single-tenant environment, it is hosted (at the merchant's choice) in on-premises equipment, private cloud, public virtual private cloud (VPC) and cloud/on-premises hybrids. It interconnects directly with the merchant telephony system at the highest possible level – removing components in the telephony and contact center systems below it from PCI DSS scope.

As Sycurio overlays existing merchant infrastructure and systems it has no impact on other deployed environments compliance status.

How Sycurio works

1. When a payment transaction is initiated SecureMode is engaged via:
   - an agent in their CRM, or
   - a Computer Telephony Interface (CTI) command in an automated payment system
2. The caller enters the requested payment card data – usually primary account number (PAN) and card verification code (CV2) via DTMF using their telephone keypad. Sycurio masks the data from the merchant and agent and holds it in secure memory
3. The agent or system collects the non-sensitive information verbally (name, expiry dates, address) - this is entered into the customer CRM
4. When all required information has been captured, the agent or system triggers the transaction data submission to the processor, which invokes the following Sycurio process
5. Sycurio combines the sensitive and non-sensitive data and transmits it to the processor
6. The processor authorizes or declines the transaction and signals Sycurio. Who then destroy the data held in memory and pass the result back to the merchant
7. SecureMode is automatically deactivated at the end of the transaction process
   - by entering the last digit of the card verification code, or
   - the call connection is lost

   The agent may reset the SecureMode connection manually – allowing the customer to re-enter their payment card data if a mistake is made
8. The payment card data does not enter the merchant's environment at any point - it is captured, temporarily stored, processed, and securely deleted entirely in Sycurio's independent PCI DSS Level 1 infrastructure hosted in its own self-contained single-tenant environment, thus drastically minimizing the scope of compliance.

Sycurio.

PCI DSS Level 1 Service Provider

DTMF masking & secure digital payment link generation

Sycurio PCI DSS scope guide.

Contact center Card Data Environment (CDE)

Telecommunications Infrastructure

Telco, PSTN, ISDN, VoIP, UCaaS, Voice Gateway, Switch, Session Border Controller, PBX, IP Phone System

By integrating at the highest level in the telecommunications infrastructure Sycurio enables all payment card data to bypass the merchant and be transmitted directly to the payment service provider. This removes the merchant from the majority of the PCI DSS scope.

Contact Center Operations Infrastructure

On Premises CC Software, CCaaS, Servers, CRM System, Call Recording, IVR System, Speech Recognition, Digital Services

All CHD, SAD and CVC data transmitted via DTMF is captured in Sycurio's infrastructure and replaced with flat audio tones or asterisks before it enters the merchant environment.

Network Environment

Physical Networks, Firewalls, Servers, Routers, Auth

The network and authorization environment are not exposed to payment card data as it does not enter the merchant environment.

Software & Hosted Services Environment

Desktop Applications, Served Applications, Hosted Applications, Mobile Applications, API, Databases, Storage

Connected and nested applications and services are not exposed to payment card data as it does not enter the merchant environment.

Physical Environment

Premises, CCTV

The physical environment is protected as it is not exposed to payment card data as it does not enter the merchant environment.

Agent & Remote Agent

Agent, Remote Agent, Telephone Equipment, Computer Equipment, Payment Terminal, Home Workspace, Home Network

Contact center and remote agents are removed from scope as they have no access to payment card data - they hear replacement 'flat' DTMF tones and see '*' in their transactions. Their environments and equipment are removed from scope.

Agent Attended Payment Links

Messaging Applications, Email, SMS, Social Channels

Digital payment links are generated and processed in Sycurio's infrastructure. Agents and the merchant's connected systems have no access to payment card data - removing them from PCI DSS scope.

Automated Digital Payment Systems

IVR Systems, Chatbot Systems, Voicebot Systems

Automated digital payment links are generated and processed in Sycurio's infrastructure via the APIs. The merchant's systems have no access to payment card data (they access transaction status data only) - this removes them from PCI DSS scope.

Payment Services Integration

PSP, Tokenization

The PSP and tokenization systems are integrated diectly with Sycurio who maintain PCI DSS compliance on behalf of the merchant.

About Sycurio
A globally trusted security partner.

Sycurio (formerly Semafone) helps organizations transform and simplify how they manage payment security, regulatory compliance and consumer data protection. Our solutions and services enable enterprises to safeguard every customer interaction, in every channel - optimizing and securing their customer experiences to build trust and lasting loyalty.

We've come a long way since our inception in 2009, when our pioneering and patented technologies first revolutionized how call and contact centers enable compliant and secure telephone payments.

Today, our data security solutions and services help organizations transform and simplify how they manage payment security, regulatory compliance and consumer data protection.

By listening to our customers and partners – and anticipating their evolving needs – we continue to deliver innovative and effective transaction security solutions. Ensuring we can all transition with confidence into a digital-first world.

Sycurio.Voice

Secures and simplifies PCI DSS compliance for contact centers taking telephone payments

Sycurio.Voice secures payment card data by preventing it from being exposed to people, processes, environments, and systems. Callers simply enter their card payment details directly into their telephone keypad or via speech recognition. The payment card data is then passed directly to the payment processor through Sycurio, entirely bypassing the merchant network and systems.

Sycurio is a globally trusted and effective solution that significantly reduces the cost and complexity of enterprise PCI DSS compliance.

- Significantly reduces PCI DSS compliance scope and security management costs
- Moves the entire contact center and remote agents out of scope for the majority of PCI DSS compliance obligations by routing it away from the agent and infrastructure directly to the payment processor. Sycurio supplies the merchant with the annual Attestation of Compliance (AoC) certificate moving them to self-assessment (SAQ-A) status.
- Overlays seamlessly with the existing telecoms and contact center infrastructure with no impact on existing compliance
- Enables entire calls to be recorded without compromising PCI DSS
- Measurably improves the customer experience by reducing average handling times (AHT) and increasing first time resolution (FTR)

Sycurio.Digital

SaaS-based PCI DSS compliant digital payments links for all merchant engagement channels

Sycurio.Digital is a digital payments link solution engineered to deliver secure customer payment experiences without engaging in the complexities of embedding PCI DSS compliant payment requests across multiple platforms.

Presented as a shortform URL, highly configurable payment links can be embedded in almost any digital surface, software or systems by using the API or agent user interface. The link connects directly to Sycurio's PCI DSS Level 1 infrastructure where it is passed directly to the merchant's payment processor. The merchant receives real-time information during the process but has no access to payment card data.

As Sycurio manages the entire transaction, all payment card data completely bypasses the merchant systems and removes them from PCI DSS scope.

Sycurio.Digital can be deployed in agent chat and messaging applications, AI driven chat and voicebots, IVR systems, social messaging, web services, mobile apps, e-and social commerce, SMS, email, and physical print using QR codes.

Sycurio.

This short guide has been created to educate infosecurity and compliance teams to highlight areas where payment card data may transit or be present in contact center environments. It should not be used independently of the professional advise and guidance provided by PCI SSC Qualified Security Assessors with specific contact center experience.

About Sycurio

Sycurio (formerly Semafone) is a leading provider of flexible cloud-based solutions and services that simplify how organizations manage data protection, regulatory compliance, and payment security. Sycurio holds a range of patents which cover a number of aspects related to the use of DTMF signaling to capture payment card data from a contact center customer during a live phone call and transmit it securely to a payment system. We are a global market leader in DTMF masking and other transaction security technologies. Our customers trust our PCI DSS Level 1 infrastructure to provide them efficient payment services that significantly reduce their PCI DSS scope, operational costs and risk.

If you'd like more technical information on how we secure merchant transactions, please contact our PCI DSS Technical Compliance Team at **sycurioknowspci@sycurio.com**

Certifications

PCI DSS Certified
LEVEL 1 SERVICE PROVIDER

ISO27001:2013

VISA
Level 1 Service Provider

mastercard
SDP Compliant
Service Provider

CYBER ESSENTIALS