







Sycurio.

DTMF masking for PCI DSS compliance.

DTMF masking for PCI DSS compliance.

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 handling compliance with PCI DSS in card-not-present (CNP) payment transactions.

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 signals are also used extensively across interactive customer experience platforms as a method of navigation.

DTMF based payments in the contact center

It is recognized that taking payments in a supervised and managed contact center even with 'clean room' policies using spoken number 'listen and transcribe' is a high-risk activity – and in a remote agent environment it is inherently insecure.

Processing CNP card holder and authentication data (referred to in this document as CHD & SAD) 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 with careful consideration.



DTMF – a brief technology overview

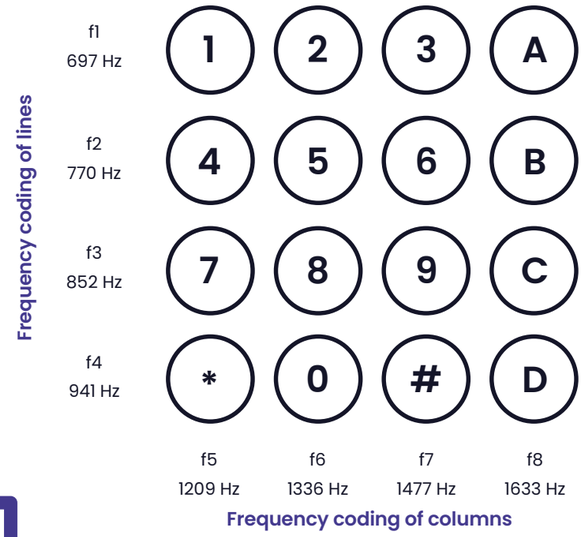
Introduced in the early 1960s, Dual-Tone Multi-Frequency signaling has been proven to be a robust technology; its relative simplicity has ensured its ubiquity across both analog and modern digital networks. In modern network and security environments care needs to be taken to ensure that when it is used to transmit sensitive data it is handled appropriately.

Each symbol/datapoint in DTMF is coded by using two frequencies which are sent at the same time within defined tolerances. The frequency pairs are designated by the columns and lines of the telephone keypad which are assigned a frequency.

Lines are assigned frequencies between 600 Hz and 1 kHz and columns between 1.2 and 1.7 kHz.

For example, the DTMF signal for '1' consists of the pair of frequencies 697Hz and 1209Hz, the DTMF signal for '2' consists of the pair of frequencies 770Hz and 1336Hz etc.

Creating DTMF signals using a keypad



Identifying DTMF signals

In an unencrypted, unmasked, or unsuppressed audio stream – such as recordings or unsecured live telephone calls – the identification of these paired frequencies can be easily achieved and automated using a range of commercial, 'free' and open-source software tools. This makes the extraction of structured strings of information such as payment card data a threat from anybody with a curious mind and access to Google.

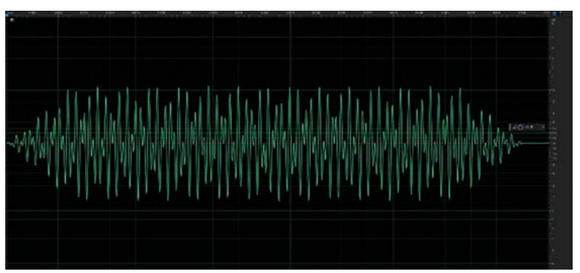


Fig 1.1 - DTMF '1' 100ms signal

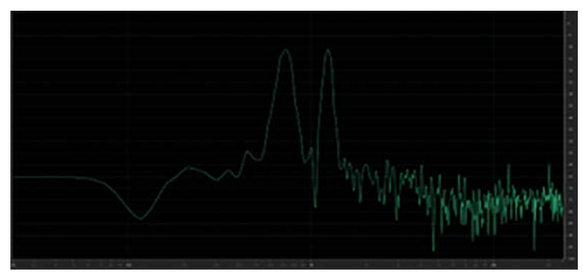


Fig 1.2 - DTMF '1' Frequency analysis showing 697Hz and 1209Hz peaks



Fig 2.1 -DTMF '2' 100ms signal

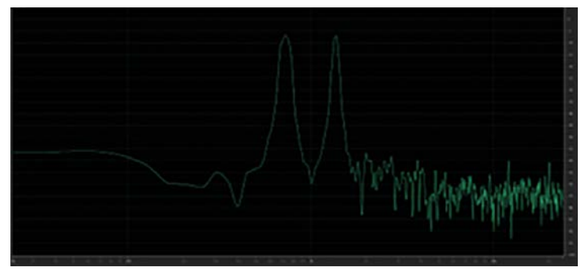


Fig 1.2 - DTMF '2' Frequency analysis showing 770Hz and 1336Hz peaks

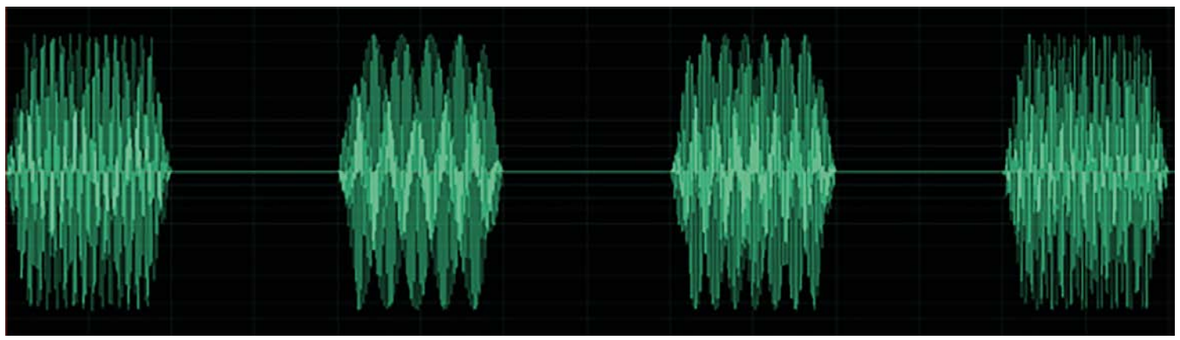


Fig 3 - DMTF '1,2,3,4' 100ms waveform audio signal

DTMF in contact centers.

DTMF routing in telephony

The routing of DTMF signals can be achieved in both analog and digital telephony environments. Telecommunications systems operate within a complex supply chain which includes carrier infrastructure, hardware, software, and increasingly cloud-delivered services – it is worth noting that legacy components in telecom environments are quite common and maybe very difficult to secure.

In VoIP & SIP based telecoms systems DTMF can be processed in two standard ways:

- 'In-band' as audible tones in the RTP media stream
- 'Out-of-band' as a non-audible signal in the media stream
  - Using the RFC2833 standard - as signaling in the RTP path, but not part of the RTP media
  - Using SIP Signaling - as SIP messages completely out of RTP

In summary, DTMF signals can be transmitted in either or both the media and the signal channels of telecommunications systems.

From a data security perspective, it is important to have a clear understanding of the type and topology of the telecom infrastructure a client operates. This knowledge will determine the path(s) of DTMF based CHD and SAD, and which components (and their respective responsibilities) are in-scope for applying PCI DSS controls.

DTMF 'masking' and 'suppression'

There are two distinct methods for redacting DTMF signal data from the audio stream – masking (overwriting the data with a single non-sensitive 'flat tone') and suppressing (removing the data completely leaving a blank or silent section in the audio stream).

Both serve the same purpose from a data security perspective, however, in the contact center environment masking is the generally preferred solution. Masking provides the dual benefit of enabling an agent to hear the progress of a customer inputting data via their keypad without being able to decern the actual content. And, in call-recordings there are no 'blank' sections which can be considered problematic from a regulatory perspective.

DTMF masking and 'bleed'

The dynamic replacement of sensitive DTMF numeric data with a non-identifiable DTMF symbol such as '*' in the media or signal stream is usually achieved using a proprietary or licensed CODEC. The performance of this type of technology to cleanly substitute (mask) sensitive data is dependent on a range of factors such as signal noise, latency and systems engineering & design. Failure to mask all the signal leaves traces of the sensitive data in the media stream - this is known as 'DTMF bleed'.

Almost all DTMF bleed cannot be heard by the human ear (unlike the DTMF tones which with a little practice can be deciphered), but it can be easily identified and often decoded using non-specialized audio processing software.

The following illustrative diagram shows a single DTMF tone ('1' 100ms) which has been masked with another tone ('A'). Approximately 15ms of the tone remain in the media stream – this would be easily identifiable. With the correct toolset it is possible to extract incompletely masked DTMF signals from recorded audio streams and data packets with samples as short as 2-5ms.

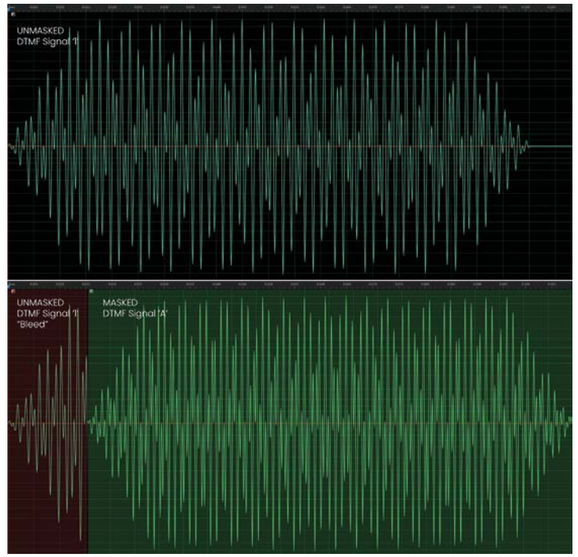


Fig 4 – Illustration of a clean and a partially masked DTMF signal exhibiting DTMF 'bleed'

DTMF 'bleed' in call recordings

As an indication of incompletely masked DTMF signals, it is possible to identify them in media streams by viewing their waveforms in a non-specialized audio editor such as Audacity - they may exhibit 'spikes' and or 'gaps' as displayed in the sample below.

However, to verify that the media stream does actually contain recoverable sensitive data it may require further investigation, or direct interaction with the masking system vendor to obtain proof of compliance.

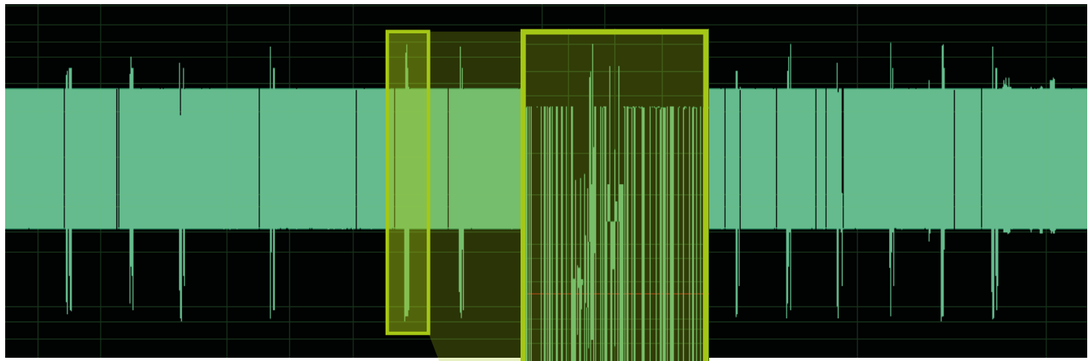


Fig 5 – Example audio stream exhibiting DTMF bleed

PCI DSS guidance on DTMF and call recording.

The PCI SSC Protecting Telephone-Based Payments Special Interest Group

The PCI SSC information supplement 'Protecting Telephone-Based Payment Card Data' (v3.0 2018-11) makes it clear that all elements of the telephone infrastructure and the card data environment (CDE) that transmit, route, transfer, process, or store (even in a temporary cache) CHD and SAD are in scope for PCI DSS unless appropriate DTMF masking or suppression solutions are in place.

PCI DSS Version 4.0 (Requirement 12.5) does not extend the scope but does reinforce the requirements to fully understand and document third-party systems (TPSP) nested inside or connected to the client 'cloud-based services' and apply appropriate controls. These include for example: Contact Center as a Service (CCaaS), Unified Communications as a Service (UCaaS), CRM, IVRs and call recording systems. This important requirement can present a wide range of components to identify and control as the payment data flow passes through the telephony infrastructure and it may also traverse nested elements of other solutions.

Remote workers (agents), their devices & networks, and home environments require special consideration. If they are exposed to unmasked or unsuppressed DTMF that contains CHD and SAD they are considered within the CDE and subsequently in-scope.

"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."

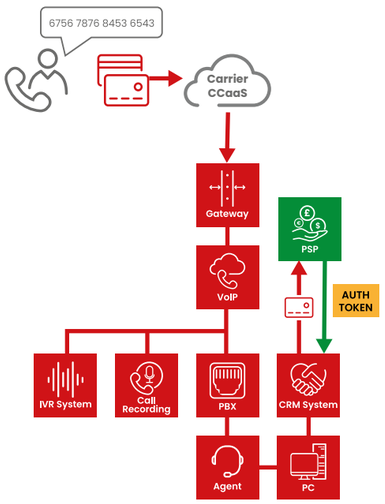


Fig 6 – Components in scope for PCI DSS in telephone based CNP payment transactions (red)

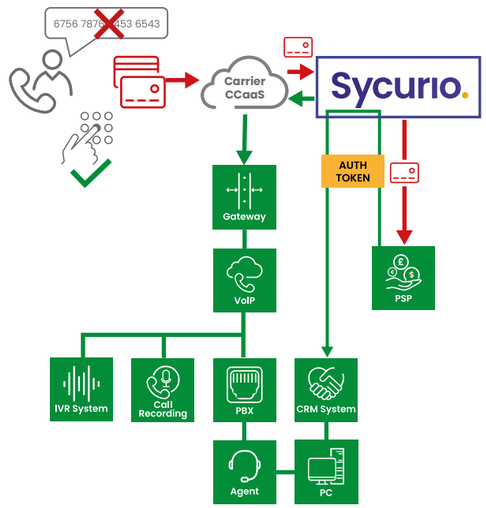


Fig 7 – Components in scope for PCI DSS in telephone based CNP payment transactions where an effective DTMF masking or suppression solution is in operation (red)

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. Nested third-party services and components may also be considered 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 tokenisation 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.

Notes & Resources.

Sycurio.

Cardholder Data (CHD), Sensitive Authentication Data (SAD) and Card Verification Code definitions

This document uses the PCI SSC definitions of card holder data (CHD) and sensitive authentication data (SAD) in card-not-present (CNP) environments. For brevity and clarity, the definition of SAD includes Card Verification Code and any other data that may not be stored under any circumstances as defined in the PCI DSS.

DMTF tolerances and variations

The tolerances and signal length for each DTMF datapoint may vary across regional standards, carrier networks and vendor implementations - please refer to local telephony standards.

Glossary

Real-time Transport Protocol (RTP) - a network protocol for delivering audio and video over IP networks.

RFC 2833 specifies a payload format for carrying DTMF signaling information within RTP packets.

PCI SSC referenced documents

Protecting Telephone-Based Payments Special Interest Group information supplement 'Protecting Telephone-Based Payment Card Data' (v3.0 2018-11) – Section 6.4.1

Payment Card IndustryData Security Standard
Version 4.0 - March 2022

Useful tools for decoding DTMF from media streams

- DTMF Tone Analyser: http://dialabc.com
- DTMF Tone Generator: https://www.audiocheck.net
- Audio Analysis: https://www.audacityteam.org/
- https://support.digium.com/s/article/How-can-I-decode-DTMF-using-Audacity-and-Multimon

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