DTMF masking for PCI DSS compliance.

Sycurio.

For many organizations, the contact center is the beating heart of their customer service operation and the front line for communicating with customers. Perhaps even more importantly, the contact center can act as a major hub for payment transactions. For this reason, it's vital to employ a solution that will efficiently process these payments in a manner that is both compliant with industry and state regulations and protects sensitive customer data.

When considering how to secure telephone payments in your contact centers, there are a number of technologies available to companies. DTMF masking, clamping or suppression is one of them. Let's take a look into what this technology entails and how it compares.

What is DTMF masking?

Dual-Tone Multi-Frequency (DTMF) is an in-band telecommunication signalling system using the voice-frequency band over telephone lines between telephone equipment and other communications devices and switching centers.

When using DTMF masking, rather than someone verbally speaking any numerical information to a customer service representative (CSR), it is typed into the caller's telephone keypad. Each touch of the keypad generates a corresponding signal which is sent down the call line. Prior to the signalling reaching the contact center environment, it is intercepted by a device which converts it to a data packet, and then passes it directly to its final destination.

In this way, sensitive information such as credit card numbers, social security numbers, bank account numbers and other authentication information can be passed through the telephone keypad without the listener being able to discern its meaning. As well as giving companies a way to process sensitive customer information without it being handled directly by the contact center, DTMF masking also alleviates the need for solutions like 'pause and resume', or 'stop/start' call recording. It also enables organizations to process payments over the phone, without having to worry about bringing their entire contact center into scope for Payment Card Industry Data Security Standard (PCI DSS) compliance.

How does it work for credit and debit card payment processing?

DTMF suppression can be used to process credit and debit card payments taken over the telephone. Instead of having a customer read their payment information aloud to the contact center agent, customers can simply share their card number by inputting it into their telephone keypad. During this process, the incoming data is intercepted, and the agent is presented with masked digits on their desktop in real time.

Once the customer has input their card numbers and the system has verified that this information is correct, the transaction data is seamlessly passed through to the Payment Service Provider (PSP) for processing, by-passing the agent and their desktop as it does so.

Throughout the transaction, no sensitive data enters the contact center and is not stored or recorded anywhere.

PCI DSS compliance for contact centers.

The PCI DSS is made up of 12 requirements, which cover securing networks, protecting data, access control measures, information security practices, and monitoring and testing. Its overarching aim is that cardholder data be protected by any organization that stores, transmits, or processes this information.

Compliance is enforced by regular audits carried out by either a professional Qualified Security Assessor (QSA), Internal Security Assessor (ISA), or through a Self-Assessment Questionnaire (SAQ). Non-compliance can result in fines, imposed by the card issuers via the acquiring banks, for any merchant who fails to meet the required standard. However, with the right technology in place, any organization can comply with these regulations.

Any organization that takes card payments is subject to the rules laid out in the PCI DSS, and these rules also apply to payments taken over the phone. For those companies taking payments inside a contact center, they must make sure that they:

- Demonstrate evidence of compliance to over 400 security controls which are applicable to any part of the contact center environment handling card data
- Ensure that sensitive authentication data (CVC2/CVV2 security code) is not stored in any format anywhere, including call recordings
- Vet new customer service representatives and conduct appropriate background checks, which is an expensive and time-consuming process
- Make sure data cannot be removed from the call center by any means; usually by restricting the use of pens and paper and banning mobile phones from the contact center. Fortunately, DTMF masking technologies like Sycurio's can stop cardholder data being exposed to the contact center environment, greatly reducing the number of applicable PCI DSS controls for the merchant

DTMF masking for PCI DSS compliance. (cont)

Sycurio.

Alternative technologies for PCI DSS compliance.

In the past, four methods have been used to help with PCI DSS compliance in the contact center:

'Pause and Resume' call recording solutions

Pausing the call recording when a payment is being taken is often suggested as a means for contact centers to comply with PCI DSS. In reality Pause and Resume solutions only help merchants with a small part of their PCI DSS footprint, i.e., not storing payment card information on call recordings. The CSR, the desktop, plus the rest of the contact center infrastructure is still in scope for PCI DSS.

Encryption of call recordings

Many organizations believe that encrypting their call recordings will address the risks associated with storing sensitive card data. However, while good encryption is easy, good key management is not. Managing these encryption keys provides additional headaches to the business and leaves data susceptible to being exposed through poor key management. In addition, under PCI DSS the CVC2/CVV2 security code cannot be stored under any circumstances, even if it is encrypted.

White or clean room contact center environments

To meet PCI DSS requirement 9—restrict physical access to cardholder data—some merchants attempt to implement a white or 'clean-room' environment. Customer service representatives must go through security checkpoints before entering and leaving the contact center, and they are not allowed to have access to the internet or email, their mobile phones, personal items, or even a pen and paper. In these working environments, employee morale can be low, leading to high staff turnover rates.

Automated payment IVR solutions

Using interactive voice recognition (IVR) or keypad entry, these systems allow payments to be taken outside of the standard contact center environment. This is achieved by having the IVR system on a segregated part of the company's network or using a third-party hosted solution. However, using these solutions means calls must be routed to an automatic system where customers are more likely to drop out at the sign of difficulty, which in turn could result in a lost sale or customer.

Benefits of implementing DTMF masking.

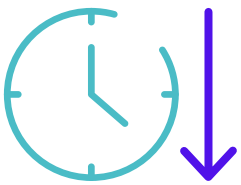
Implementing a DTMF masking solution like Sycurio.Voice provides the simplest route to PCI DSS compliance in the contact center and also provides other benefits:

Better customer experience

82%
of consumers want more human interaction[1]

Sycurio's DTMF masking solution never requires a call to be rerouted or transferred. CSRs remain in constant verbal communication with the customer while taking a payment, allowing easy assistance if any issues occur.

Reduction in average handling time



Sycurio can reduce AHT by 8% in payment transactions

Sycurio.Voice provides a single point of numerical entry, reducing opportunities for error during the collection of payment information. Because of this, information doesn't need to be recaptured or corrected by the customer service representative, removing any need for a representative to read back or confirm the card details to the caller. In addition, while the customer enters their payment information, the CSR is free to carry out wrap up activities during this time.

DTMF masking for PCI DSS compliance. (cont)

Sycurio.

Better agent experience

Not exposing CSRs to sensitive payment data removes the need for restrictive PCI DSS controls. Agents can be given access to the tools they need to do their job effectively without having to go through excessive security procedures. Adopting Sycurio.Voice also allows for the use of omnichannel support without the risk of card data being stolen by a rogue agent.

Lower risk of data being exploited

47%
of consumers are concerned that their data will be hacked[2]

86%
say data privacy is a growing concern[2]

Because payment card data is no longer being stored, transmitted, or processed within the contact center infrastructure, hackers are not able to steal payment information. They can't hack what you don't hold!

Partial solutions have been adopted by a significant number of businesses. However, these fail to fully meet the customer service requirements demanded by consumers. DTMF masking is the only solution that keeps payment card and sensitive data completely out of the contact center, while maintaining the highest level of customer experience.

1. PWC: The Future of CX. **2.** KPMG Corporate Data Responsibility Bridging - The Consumer Trust Gap 2021.