keyivr

intelligent payment systems

WHAT IS DTMF MASKING?
THE ESSENTIAL GUIDE

How DTMF masking and suppression can help towards PCI compliance when taking card payments over the phone

INTRODUCTION

For many organisations having the ability to take payments over the phone is a must, but with the **Financial Conduct Authority (FCA)** regulations and the new **General Data Protection Regulation (GDPR)**, obtaining **Payment Card Industry Data Security Standard (PCI-DSS)** compliance can often be a challenge.

Having an all-encompassing secure and compliant solution is something organisations strive towards, with Dual Tone Multi-frequency (DTMF) masking becoming an important aspect of this.

WHAT ARE DTMF TONES?

DTMF stands for **"Dual-Tone Multi-Frequency"**, a series of audio signals generated when a telephone user presses the individual numbers of a telephone keypad (as well as the "#" and "*"), with each key producing two tones of a specific frequency.

In order to prevent a voice from imitating the DTMF tones, one is generated from a high-frequency group of tones and the other from a low frequency group. However, with the right hacking software, these DTMF signals can easily be decoded.

The Challenge Faced by Financial Services Firms

The FCA regulations impose that any financial firm that provides services to consumers must record their phone calls for training and monitoring purposes in order to prevent, detect and deter market abuse. The Payment Card Industry Data Security Standard (PCI-DSS), on the other hand, outlines that in order to be compliant no card sensitive data can be recorded or stored by the organisation.

FCA FINANCIAL CONDUCT AUTHORITY

WHAT IS DTMF MASKING AND SUPPRESSION?

DTMF masking (often called DTMF suppression) helps organisations obtain **PCI compliance** whilst continuing to take payments over the phone and record their calls. The masking software either replaces the tones or converts the two pitches into a single flat tone to ensure they cannot be decrypted by a hacker or someone within the organisation. This works as one solution to the problem, allowing customers to input sensitive card details into their phone without any concerns that the cardholder data can be exposed at the other end.

Without DTMF masking organisations could risk malicious attacks targeting their customers' data, including possible internal threats from any "rogue agents" within their contact centres. Having the ability to access card details and other personal information puts customers at a much higher risk of fraudulent activity, so corporate security is improved dramatically by removing this specific data completely from the organisation's network.

Key IVR use DTMF Suppression for our Agent Assisted Payment Solution and Secure Payment IVR, removing the tones from the agent and any call recordings

FIND OUT MORE

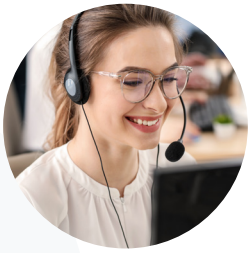
Agent Assisted Payments

Secure Payment IVR

HOW DOES DTMF SUPPRESSION WORK?

1.

Jonathan is on the phone to an agent discussing making a payment



2.

The agent asks Jonathan to start entering his sensitive payment card details into his mobile phone

3.

Using his telephone keypad, Jonathan inputs the digits from his debit or credit card, including the long card number, expiry date and CVV number

4.

The card data is sent to the agent, but intercepted beforehand, masking any sensitive tones and hiding the necessary card details on their screen

5.

This allows the organisation to process the payment securely in a PCI compliant manner. Additionally, they can record the entire call as all DTMF tones are removed

PCI DSS COMPLIANT

HOW DOES DTMF SUPPRESSION WORK WITHIN CONTACT CENTRES?

For a lot of customers, making a payment over the phone to an organisation usually means either reading their card details out to an agent, to voice recognition software or inputting digits into their telephone to be received by the organisation. In any of these circumstances, there will always be risks behind them, this may be from hackers gaining access to call logs or logged card details, along with 'rogue agents' copying customer data for malicious purposes.

DTMF masking is a great way of reducing these risks and adhering to PCI-DSS. Whilst the customer inputs their card details into their phone, the tones that are generated from each key are intercepted and the agent is presented with masked data that is stripped of any sensitive information. The agent never sees the sensitive card number, is unable to write any details down but is still informed if the card details are valid and when payment is successful.

Once the transaction data is verified by the system, the payment service provider (PSP) seamlessly processes the payment. As no sensitive information ever enters the organisation's contact centre and the customer can trust that their payment data is protected.

DTMF SUPPRESSION AND PCI COMPLIANCE

The Payment Card Industry Data Security Standard (PCI-DSS) is a set of security standards designed to ensure that all companies that accept, process, store or transmit credit card information maintain a secure environment. Once this standard of compliance was introduced in 2004, it gave way for DTMF suppression to be used as a method of improving card payment security over the phone, ensuring that organisations could become fully compliant.

Not only is DTMF masking used when a customer is on the phone to a call agent, as previously mentioned, but it can also be used with IVR systems and is often referred to as IVR Payment Technology. This is due to the convenient way organisations can securely take payments 24/7/365 without the need for human intervention. Although DMTF masking has the added benefit of shielding sensitive data from a call agent, when used with a Payment IVR it will continue to flatten or mask the keypad tones from anyone with the malicious intent to intercept the call and decipher the data.

THE BENEFITS OF DTMF MASKING

AVOID COMPROMISED DATA

Due to the way any sensitive data is intercepted and masked, there is no way it can be compromised by 'rogue agents' that might steal the information for malicious purposes

REMOVES THE NEED TO PAUSE AND RESUME

No need for pause and resume technology, where the agent pauses the call recording at the moment the customer reads out their card details and resumes the recording afterwards. This can have high maintenance costs and still leaves room for human error.

PROTECTING YOU AND YOUR CUSTOMERS

The Financial Conduct Authority (FCA) outlines that any firm that provides services to consumers and takes payments over the phone must record their calls for training and monitoring purposes. Because no sensitive data is present on the call, it cannot be picked up by call recordings, dramatically reducing the risks behind data breaches.

IMPROVED CUSTOMER EXPERIENCE

A seamless payment process gives way for a better customer service and a reduction in average handling time (no customer wants to spend a long time on the phone to an agent).

COST-EFFECTIVE WAY TO REDUCE THE RISK

With new technology, security and compliance challenges leading to an increase of financial risk, pressure from banks, regulators and GDPR to be PCI compliant has risen. DTMF masking and suppression is a cost-effective way of reducing any risks involved with taking card payments over the phone.

INCREASED CONSUMER TRUST

Improves the trust between customers and businesses as they are perceived as taking care of sensitive personal information.

TWIN CLAMP TECHNOLOGY - ADDITIONAL PROTECTION ON TOP OF DTMF MASKING

By clamping the phone signal at the start and end of the network, the risk of any data leakage across all phone networks is removed completely. Rather than simply masking the numbers reaching the organisation, Key IVR's Agent Assisted Payment solution strips out all sensitive information altogether, leaving the audio behind. This not only meets FCA regulations by allowing the entire call to be recorded, but organisations can stay PCI compliant, dramatically improving their corporate security and customer trust.

ABOUT KEY IVR

Key IVR provides secure cloud payment solutions to organisations and contact centres across the globe, protecting hundreds of businesses and their customers. Businesses can increase their revenue and conversion rate by taking PCI-DSS compliant card payments over the phone, with an automated IVR, on the web, via SMS or on a mobile app.

Our reliable omni-channel SaaS platform is trusted by some of the world's leading brands, processing over 4bn per annum and reducing the time it takes to collect payments. It is available 24/7 in 14 languages and integrated with all leading Merchants and Payment Gateways worldwide.

START PROTECTING YOUR CUSTOMERS

Talk to Key IVR and let us help you reduce serious security risks within your Contact Centre with our PCI-DSS compliant solutions. We work with you to design a solution that tackles your individual business challenges.

Find out more about our Contact Centre or Agent Assisted Payments services. Alternatively, please contact us on **+44 (0) 1302 513 000** or email **sales@keyivr.com** to discuss your requirements.

Aaron Smith

Technical Account Manager & Payment Specialist

PCI DSS COMPLIANT V3.2.1 Level 1 Service Provider

bsi. ISO/IEC 27001 Information Security Management

CICM CORPORATE PARTNER