

Achieving PCI DSS Compliance Without Compromising the Customer Experience

Achieving PCI DSS Compliance Without Compromising the Customer Experience

What's on the cards for a better purchasing experience with compliant call recording?

TalkOne's white paper is focused on call recording and the steps you can take to ensure that, when talking card payments, Sensitive Authorisation Data is not recorded, therefore maintaining compliance. With many technical and descoped solutions operating at an 'arms-length', we explore how an emerging paradox can be overcome, that of providing a good customer experience for your business to take card payments without exposing the actual card data to your agents and the call recording.

Meeting PCI DSS Compliance is always front of mind to protect customers and reduce the threat of being targeted by criminals. Since the standards were put in place in 2004 the type of secure technical solutions has grown, and an increasingly popular approach is to limit the exposure to the customers' Sensitive Authorisation Data (SAD) for payment to combat increasingly sophisticated fraudsters. These options operate on the principle of descoping your staff and the business from storing any sensitive data by avoiding such data even touching a company's own network and systems in the first place.

The aim is to bring businesses up-to-date with the compliant options and scope reduction techniques and to help them to consider ways to remain compliant and improve operations and customer service. Because the options are now more intricate, we have put together a visual comparison and commentary to offer clarity on the level of security plus customer friendliness, ease of operation and implementation. A quick regulatory summary is also provided in the last section for reference.

Timely Update for Businesses

Recently, senior management has had to think more seriously about customer security and their rights in light of the changes that businesses have had to make to meet GDPR legislation. This has re-enforced that PCI is more than a set of hurdles to be compliant and to avoid fines, it is a necessity to control the risk of damage to reputation and loss of business as result of a data breach. The rise of remote working is also leading some organisations seeking ways of bringing flexible yet secure remote working for their team.

An example of how some medium enterprises are working today demonstrates a very archaic approach to PCI Compliance. Whilst the method of writing sensitive customer information down, ensuring that you follow company protocol to shred and dispose of the waste in a secure way, by reputable collection service, is technically compliant; no one polices this and therefore the question is raised of exactly how complaint is this method? And is your business fully complaint in the eyes of the law?

The November update of “Protecting Telephone-based Payment Card Data Guidance” by the Payment Card Industry Security Standards Council (PCI SSC) is also witness to the massive evolution of technologies and processes that has taken place since 2011 when the 11-page guide was first written. The expanded guide of some 70 pages now includes payment channels handling Voice over IP (VoIP) communications and newer popular technologies, particularly those techniques that reduce ‘scope’ for businesses.

The scope reduction techniques that relate to voice recordings include DTMF masking, IVR, and SIP redirection technologies and pause-and-resume call recording solutions, many of which can be outsourced to a specialist third-party service provider to further reduce scope.

Internet Service Providers (ISPs) and telcos are deemed out of scope when providing just the communication link, i.e. internet provision, ISDN lines and SIP trunks. However, this is not always the case where service providers offer additional services such as call recording, call recording storage and hosted/cloud VoIP services, which either have visibility of cardholder data or can impact upon the security of the cardholder data. Depending on where the service provider is offering services, they are potentially exposed to the cardholder data, so the service provider rather than your business is very much in scope for PCI DSS assessment activities.

It is important to have an appreciation of some of the above intricacies of how these services work, and the flow of cardholder data through these solutions and across networks to understand if the organisation’s systems are exposed to the sensitive cardholder data. This can not only have an impact upon the size

of the PCI DSS scope, but also can have an impact on call recording. The next section provides an assessment of types of solutions with call flows to help illustrate these complexities for readers.

Solutions Review

There can be a misconception that in order to become PCI Compliant you are able to buy an off-the shelf-solution that will meet all your requirements. It is not the recorder and devices that are PCI DSS compliant but rather the way you deploy it. It is the combination of your processes, the transactional systems you use and your recorder that have to be verified**.** The latest version of the PCI DSS has security standards covering 12 areas; people, processes, systems, and networks to secure the storage, processing, and transmission of account data. In addition, an entity can reduce risk by devaluing account data through tokenization, making card data unreadable or by reducing its scope of where the PCI DSS applies. This section includes some of the techniques available to reduce PCI DSS scope.

The solutions under assessment relate to the physical environment for taking payments over the phone which deny access to materials and devices capable of recording account data. The PCI requirements of greatest relevance to businesses include the following:

- Protecting the stored data of the cardholder
- Encrypting transmission of cardholder data across public networks
- Maintaining a policy with proof that information security is addressed

The options under review are:

- Turn-off Recording – Manual Pause and Resume
- Automated IVR on Premise and in the Cloud
- On-site DTMF Blocking
- Central DTMF Blocking including standard and a timed blocking option

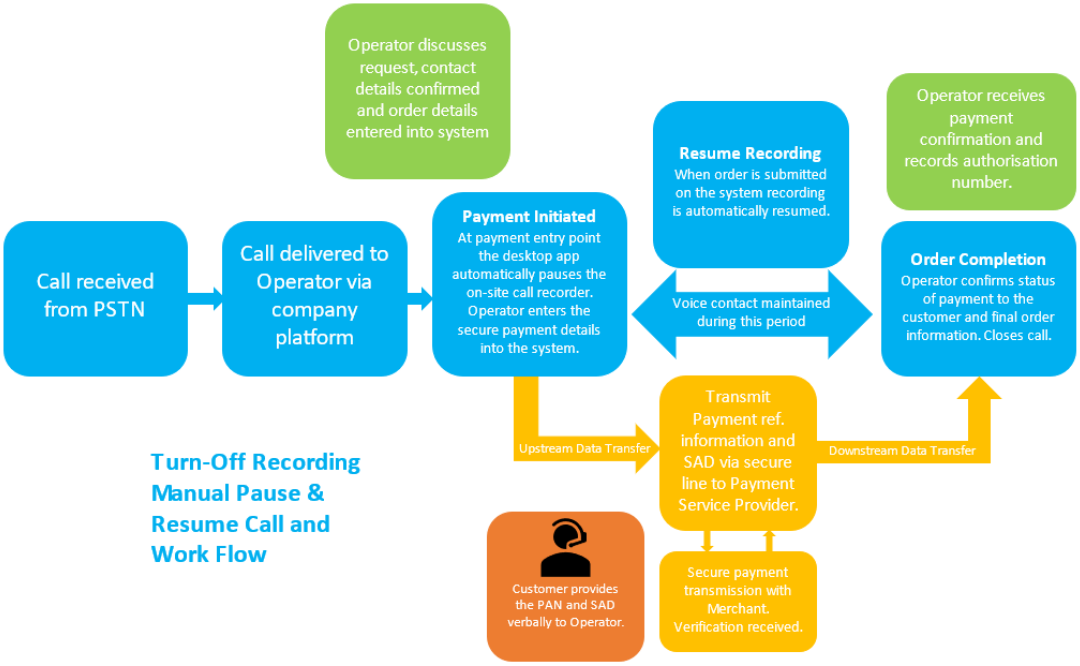
We begin with summary comparison chart of these solutions followed by a detailed description of each solution.

AUTO PAUSE AND RESUME	AUTOMATED IVR ON PREMISE	AUTOMATED IVR IN CLOUD	CONTACT CENTRE STANDPOINT	ONSITE DTMF BLOCKING	CENTRAL DTMF BLOCKING - STANDARD	CENTRAL DTMF BLOCKING - TIMED
			Ease of Compliance			
			Agent User Friendly			
			Customer Satisfaction			
			Agent Security ***			
			Site Systems Security			
			Network Security			
			Ease of Implementation			
			Remote Working			

Compliant Solutions Compared

Our comparison chart provides a useful overview of how each solution meets the key considerations for organisation's (the least compliant 'Manual switch off' solution, has not been included in the chart).

A cautionary note on the difficulty of distilling a complex set of factors using a measurement scale, e.g. 'Ease of Implementation' incorporates several pros and cons which can cancel each other out, resulting in a neutral score. Some further explanation is contained in the following pages and established service providers will be able to offer detailed advice (see final page).



Turn-off Recording – Manual Pause & Resume

How it Works

At the appropriate points in the call payment process the operator clicks on a pause recording button and a resume recording button using the desktop application supplied as part of the call recorder, which is either on the premise or in the cloud. The operator then asks the customer to provide their CHD and SAD verbally and the operator enters the customer's details directly into their desktop application. Via a secure line to the Payment Service Provider, confirmation is then sent to the operator's desktop that the payment is authorised and the operator communicates this to the customer.

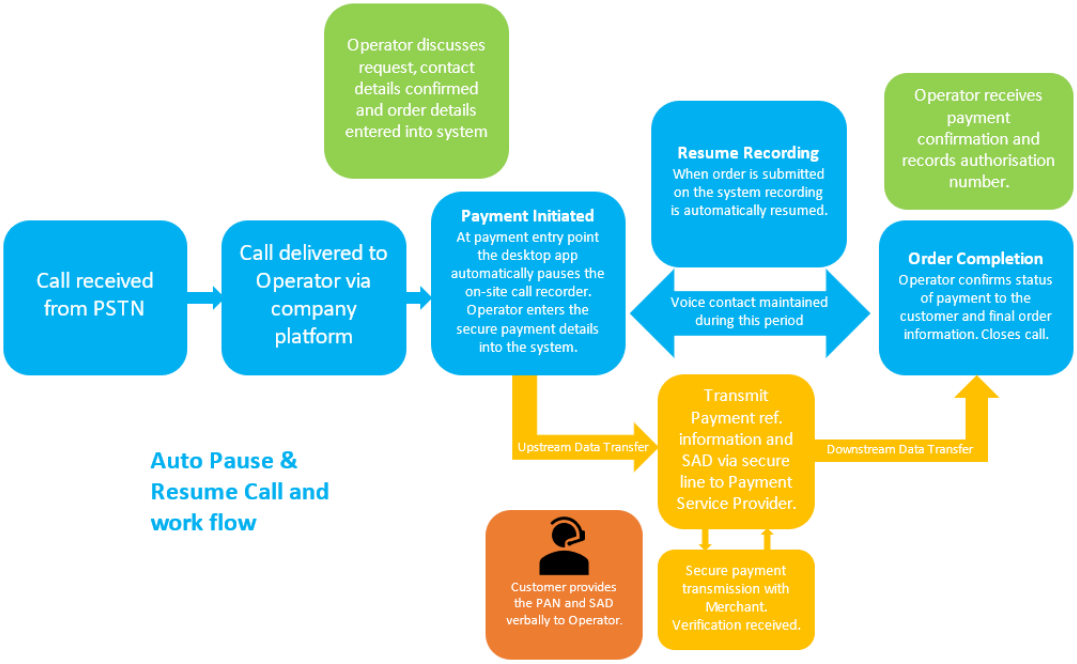
Pros and Cons

While the operator is on hand to lend assistance throughout the call, they still have access to the card data in order to process the purchase. The amount of oversight and supervision required for manual solutions is much greater than for automated solutions.

Manual pause-and-resume demands constant monitoring and verification that the manual processes are being followed for every single transaction and that call storage does not contain any Card Holder Data (CHD) or SAD.

A properly implemented pause-and-resume solution could reduce applicability of PCI DSS by taking the call-recording and storage systems out of scope, but the technology does not reduce PCI DSS applicability to the operator, the operator desktop environment, or other systems in the telephone environment.

The November 2018 PCI guidance has not gone as far as to state that this option is non-compliant, but it would require a high level of management to prove it is, as we've described. The current PCI guidance is to ''encourage business operators to remove SAD from recordings preferably automatically, (with no manual intervention by staff)".



Auto Pause & Resume

How it Works

This approach ensures the recording system stops during the payment process when sensitive customer information is being given. Pre-coded steps are written into the organisation's platform process which sets the recording to pause, such as when the payment screen is launched. The customer is asked to provide their CHD and SAD verbally and the operator enters the customer's details using their desktop application. Once payment has been passed beyond the payment screen to 'submit' for example, a second trigger is generated to restart recording.

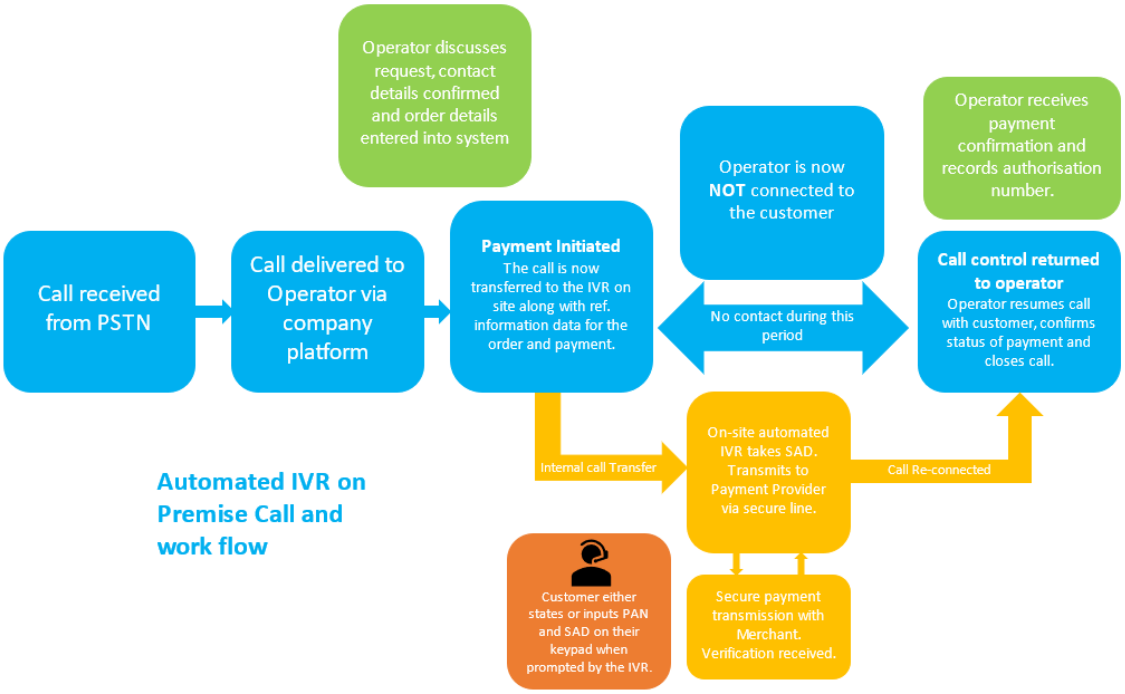
Other audible systems can be triggered when keywords are spoken. Although rarer in nature, another similar option is to mute / unmute the call recordings rather than pause and resume. This latter option means a single call detail record is retained. Via a secure line to the Payment Service Provider sends confirmation to the operator's desktop that the payment is authorised and the operator communicates this to the customer.

Pros and Cons

Auto pause and resume requires the system to be integrated with the workflow allowing the operator to be of assistance throughout the call. A downside is the information could still be heard by the operator and in the room so could still be recorded by a third party and of course, noted down.

For compliance, it does need to be shown that the solution is reliable (e.g., no failures or delays before the recording is paused) and it cannot be bypassed by operators. This option can result in two separate call records that need to be linked for complete call metrics.

While 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 operator, the operator desktop environment, or any other systems in the telephone environment.



Automated IVR on Premise

How it Works

At the point in the call that the SAD is required the operator transfers the call to the self-service IVR solution that is located at the same location as the company. The operator no longer has contact with the customer during this payment process. The interaction between the customer and computer uses both voice (speech recognition) and Dual-Tone Multi-frequency (DTMF) tones to collect information from the customer in an automated process.

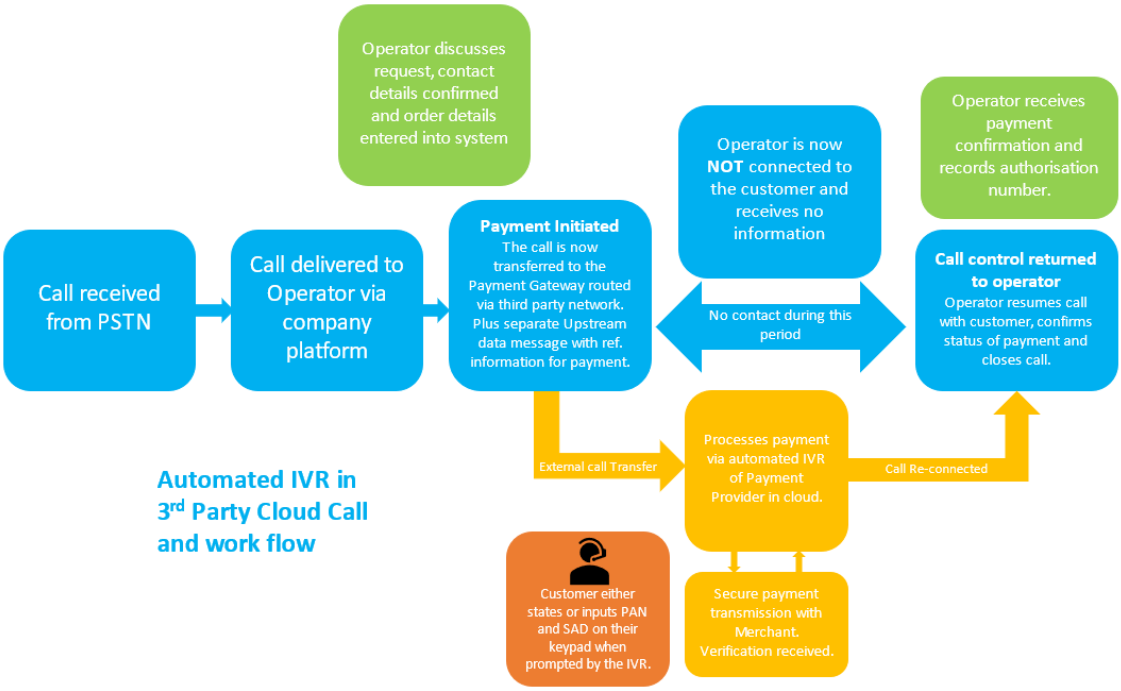
Via a secure line to the Payment Service Provider confirmation is given to the IVR application that the payment is authorized and communicates this to the customer. Some systems provide the option to return to the operator after the payment is completed or if there have been problems processing the payment.

Pros and Cons

The operator is eliminated from the loop so there is no danger of sensitive information being recorded in the operator's environment.

The main disadvantage is that the caller is handed over to an automated system taking the operator out of the loop, reducing the amount of completed transactions and potentially customer support and satisfaction.

For on premise IVRs without any suppression or masking of DTMF, this option does not reduce scope for the presence of account data in systems.



Automated IVR in Third-Party Environment

How it Works

The customer is transferred to a self-service (IVR) solution that is managed by a payment provider with their equipment in the cloud by setting up another call in the external phone network. The interaction between the customer and computers uses both voice (speech recognition) and DTMF tones to collect information from the customer in an automated process. Some systems provide the option to return to the operator after the payment is completed.

Pros and Cons

The operator is eliminated from the loop so there is no danger of sensitive information being recorded in the operator's environment.

The main disadvantage is that the caller is handed over to an automated system taking the operator out of the loop, reducing the amount of completed transactions and potentially customer support and satisfaction.

Outsourcing the payment processing to an IVR solution provider does remove the presence of account data in the organisation's environment.

External IVRs are connected via the public network so there is less control over the call.

Additional costs are incurred for each outgoing call, at a local rate or higher e.g., 0844 numbers.

DTMF Blocking Overview

Using this technology call recording does not need to be paused or masked. The principal is DTMF suppression captures the DTMF tones and alters them so that the cardholder details (such as cardholder name, expiration date and service code) are not identifiable by the operator, the recording environment, as well as any unauthorised person who may be listening in. The customer inputs their card information using their own telephone keypad, and the generated DTMF tones are altered or removed from the organisation's transmission.

The transmission containing the SAD is sent direct to the payment provider. From a **data network perspective** there is a secure payment transmission from the company to the payment provider which upstream sends the organisation's reference number, amount and currency and card holder details (CHD). Downstream the Payment Service Provider sends confirmation to the operator's desktop that the payment is authorised, and the operator communicates this to the customer.

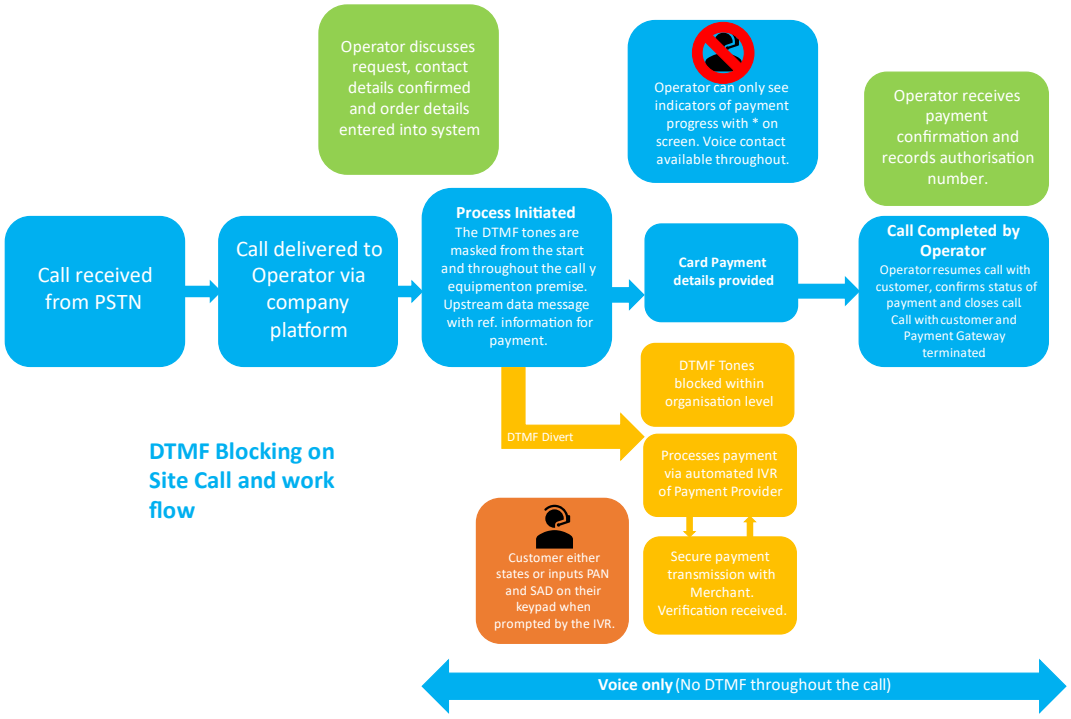
From the **customer and operator perspective** DTMF blocking allows both parties to have voice contact with each other throughout the entire telephone transaction.

The customer will experience a similar type of experience for the three types of implementations of DTMF blocking as follows:

- The operator takes the customer call and order details are obtained, name, address and payment amount is confirmed.
- The operator enters the customer and order details into a system.
- The operator initiates the DTMF masking application and informs the customer to keep their data secure, asking them to input their SAD on their phone keypad.
- The operator monitors the customer's progress on their desktop to complete the transaction, still in voice contact and supporting them if needed.
- The operator only hears flat tone. Some solutions show asterisks on their desktop screen as the customer enters digits, enabling the operator to support the customer if needed.
- The operator receives confirmation from the payment provider that the payment is authorized or not and communicates the result to the customer

DTMF blocking solutions offer different levels of security and additional functions for the operator and organisation according to how and where the

DTFM tone is diverted and suppressed. As well as the generic pros and cons of DTMF Blocking there are variations and impacts as a result of how and when the DTMF process takes place.



On-site DTMF Blocking

Additional Pros and Cons

DTMF blocking occurs on site by a DTMF masking system on the business premises, so sensitive card data does enter the company.

The recordings and storage will be of suppressed tones rather than original DTMF tones which can reduce applicability of PCI DSS requirements for call recordings, if it can be verified that the tones cannot be converted back to the original data.

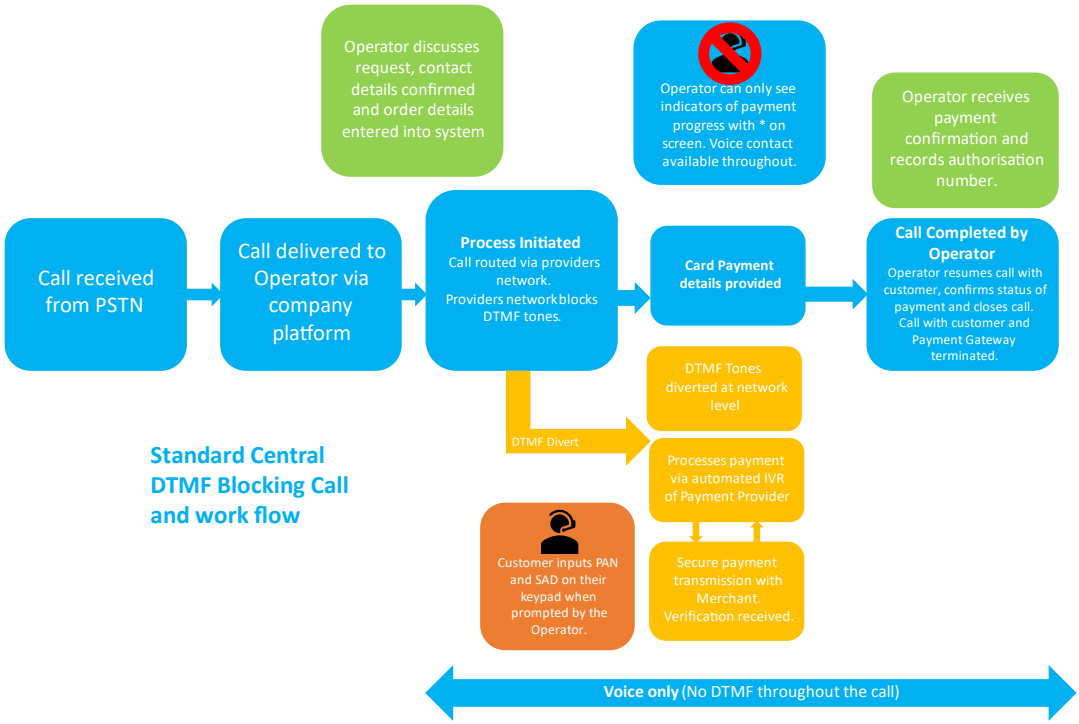
Recording systems may still be in scope for other PCI DSS requirements if they have connectivity to the systems where CHD is present.

The DTMF tone is being received by the business so it important that there are no delays in the deactivation/blocking of the tones. If this occurs, DTMF bleed means the operator and the call recording, will hear some DTMF tones.

Central DTMF Blocking

The main difference with this central solution is DTMF tones and the sensitive data never enters the business, as the automated payment system and IVR operates at the network routing/gateway layer, outside of your organisation's network. The DTMF tones are diverted at this network level by separating the voice from DTMF, so only a masked tone is heard by the operator at the company site. The secure payment transmission containing the SAD is sent direct to the payment provider. The Payment Service Provider then sends confirmation to the operator's desktop that the payment is authorised, and the operator communicates this to the customer.

This type of solution can integrate with the operator's desktop environment to prevent SAD being captured or displayed on the operator's screen. Asterisks appear on the operator's screen as the customer enters digits. The customer and operator can speak with each other if they are having trouble at any time, which improves customer satisfaction and ensures more orders are successfully completed. DTMF blocking allows the operator to have voice contact with the customer throughout the entire telephone transaction.



Standard Central DTMF Blocking Call and work flow

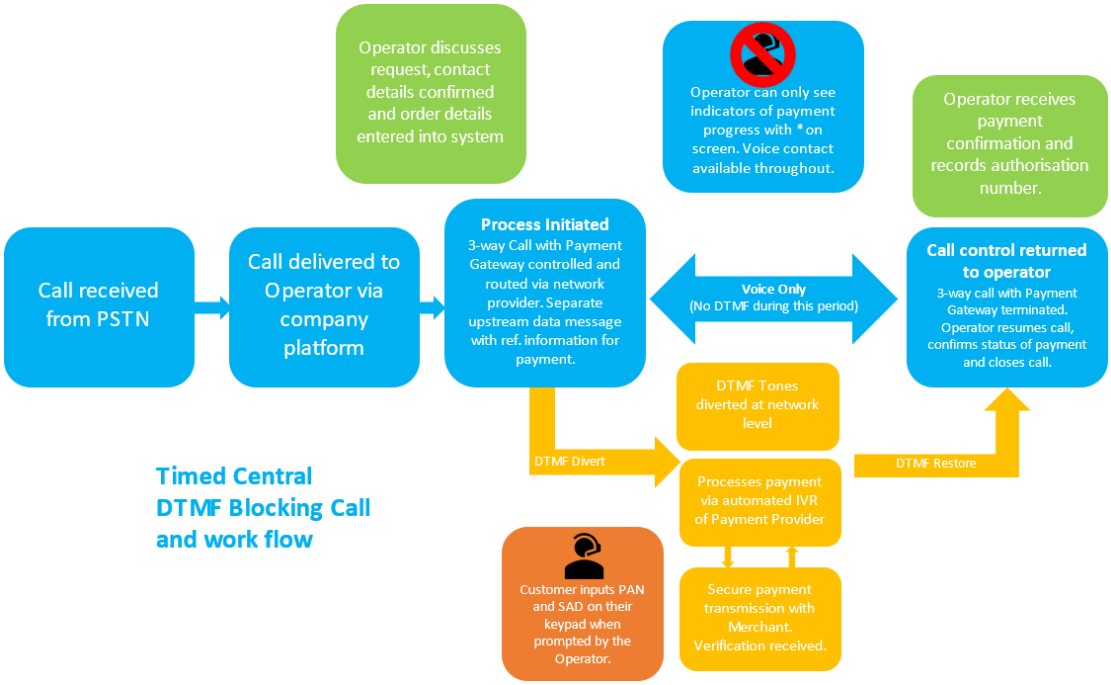
Standard Central DTMF Blocking

Additional Pros and Cons

From the start and throughout the whole call, the service/payment provider maintains the connection with the automated payment system and IVR which separates the DTMF from the voice and masks the DTMF to the organisation.

DTMF tones and the sensitive data never enters your organisation.

When the service provider is not also the network provider there is less control of this external voice network and potentially open to attack.



Timed Central DTMF Blocking

Additional Pros and Cons

The calls enter your organisation and are answered by the operator as normal. At the point where the customer needs to provide the secure card details the operator initiates a secure 3-way scenario by conferencing in the offsite IVR. The connection to the Payment Provider and blocking occurs only when needed.

The DTMF tones are instantly diverted at the network level so the DTMF tones holding the sensitive card data never enter your business environment.

The network provider manages the call routing for the business and the service provider so as all parts of the call are within the same network there is greater control and security.

The Best of All Worlds?

Finally, returning to our aim of trying to solve the dilemma of providing a good customer experience for the operator to take card payments without exposing them to the actual card data itself; we offer this mapping analysis of the two important requirements of customer satisfaction and security.



Auto Pause and Resume	1	On Site DTMF Blocking	4
Automated IVR on Premise	2	Central DTMF Blocking - Standard	5
Automated IVR in Cloud	3	Central DTMF Blocking - Timed	6

With the growing complexities illustrated in this paper the temptation for companies is to place the highest weighting on factors that help descope themselves from the equation and seek a secure solution that minimises the management effort for them. What we have illustrated is that there are compliant solutions that can reduce risk and the onus of managing every aspect of the compliance, but not at the expense of a customer friendly service, where contact and control throughout the call guarantees a greater success rate for completed transactions.

PCI DSS Compliance Resources - The Basics

The key PCI document referenced in the white paper can be found here.
https://www.pcisecuritystandards.org/document_library

Most businesses fall under the scope of compliance for the Payment Card Industry's Data Security Standard (PCI DSS). PCI DSS is an industry standard designed to help protect consumers' payment card information. It is a set of requirements that organizations must follow to accept, process and transmit cardholder data as securely and safely as possible, with the aim of preventing fraud and reducing data breaches. The PCI DSS was set up by some of the major payment card brands and currently covers all payment cards from American Express, Discover, JCB, MasterCard, and Visa International.

Who Has to Comply?

Any merchant that accepts payments must be compliant with the PCI DSS, regardless of merchant level. This includes companies that accept payments and perform card-not-present (CNP) transactions over the phone, through digital channels such as online forms and web chats.

PCI Compliance Level 1
If over 6 million Visa/Mastercard transactions are processed per year.

PCI Compliance Level 2
If over 1 million to 6 million Visa/Mastercard transactions are processed per year.

PCI Compliance Level 3
If over 20,000 to 1 million Visa/Mastercard e-commerce transactions are processed per year.

PCI Compliance Level 4
If less than 20,000 Visa/Mastercard e-commerce transactions are processed per year as well as other companies that process up to 1 million Visa/Mastercard transactions per year.

Companies that meet the level 1 requirement must have yearly on-site reviews by an internal auditor as well as a required network scan. This should be completed by an approved scanning vendor. Companies that meet levels 2, 3 and 4 are obliged to annually complete the PCI DSS Self-Assessment questionnaire. Alongside this, they also need to undergo quarterly network scans accompanied with an approved scanning vendor.

If a data breach occurs and the merchant is found noncompliant, the payment card brands can impose financial penalties on the merchant's acquiring bank. The bank passes those costs along to the merchant. Fines can range anywhere from £3, 500 to £250,000. For repeat offenses, the payment card brands can even revoke the rights of the merchant to process transactions using their cards.

PCI DSS Requirements

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. 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. There are 12 broad requirements.

Goal	PCI DSS Requirement
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. Use 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. Assign a unique ID to each person with computer access. 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 – and ensure that all personnel are aware of it.

Non-Compliant PCI Coaching

Audio Masking

An audio tone is inserted over the section of the call when the payment is being processed. The sensitive data is still being retained and therefore does not adhere to regulations.

Encryption

Encrypt the recordings this does not comply with PCI DSS. Clarification states that it is only the Primary Account Number (PAN) that can be retained in an encrypted format. Sensitive Authentication data such as the CVV / CV2 number cannot be stored in any

©TalkOne 2021 All rights reserved
You may copy the content to individual third parties for individual use, but only if you acknowledge the source of the material as www.talkone.co.uk.

TalkOne

TalkOne provide fully hosted, cloud-based, VoIP telephony platforms for small and medium sized businesses. We tailor the configuration of each PBX to the specific customer needs and offer an easy pathway to enable integration to the Customer's primary business systems whether they are standard "off-the-shelf" platforms such as Salesforce.com, Zendesk, Zoho etc. or in house custom solutions.

If you would like more information on our telephony solutions, please get in touch using the contact details below.

Tel: 0330 880 4444

Email: info@contactone.net

www.talkone.co.uk