PAUSE & RESUME CALL RECORDING

Time to Calculate the Risk

Contents

Executive Summary

One of the primary challenges inherent in managing contact centers is ensuring compliance with data security regulations.

With recent security breaches attracting fines of multiple millions of dollars and recent legislation exposing businesses to state as well as individual suits (the recent example of Massachusetts vs. Equifax being one example), the penalties for non-compliance increase dramatically with the introduction of General Data Protection Regulation (GDPR) as of May 2018.

Although Pause & Resume call recording has long been used to mitigate the risks inherent in contact center payments, the 'solution' is not the failsafe it is often seen as, and does not ensure PCI DSS compliance. In fact, using outdated compensating controls such as Pause & Resume call recording has the potential to leave your business vulnerable to expensive security breaches. The average breach costs $3.62 million. Could your business afford this bill?

This whitepaper discusses why businesses need to utilize technology that protects against data breaches caused by:

- Hackers
- Employees
- Illegal data storage

Compliant call recording technology offers the following:

- Faster calls
- Accessible data
- Cost-effective solutions
- Increased customer service
- Quick deployment

To identify Pause & Resume problems and solutions, these important questions will be addressed:

1. Why is pause & resume call recording so widely used?
2. Is pause & resume call recording PCI DSS compliant?
3. What is the potential cost of a data breach?
4. Why do businesses use old call recording technology?
5. What is DTMF technology? Is it PCI DSS compliant?
6. Is the Agent Assist solution PCI DSS compliant?

Are businesses allowed to record calls?

Your business is permitted to record calls without notifying employees in the following circumstances:

To Protect National Security

If there are serious security risks nationwide, your recordings could prevent national attacks. Government bodies would have access to the data.

To Prevent or Detect Crime

Smaller attacks - those aimed at your business - can also be recorded. If customers commit acts such as fraud, stored recordings would increase your chance of getting justice.

To Document Business Transactions

Agents can try their best, but you can't please everyone. When unhappy customers start dispute resolution, recordings could prove all business transactions and help your case.

To Ensure Compliance

If regulatory bodies need proof of your compliance, recordings will prove your business has followed the law and treated customers fairly.

To Maintain Quality Control

The best way to improve customer services is through real life experience. Customer recordings can deliver more effective training and role-play using real-world examples to enable teams to train for unpredictable situations.

To Prevent Unauthorized Access

Malicious parties could intercept your telecommunications systems and cause serious damage to your business reputation. Recordings help to investigate where the breach is, so your security team can secure your system.

If call recordings are well-protected by the law, why is Pause & Resume so risky? Before we answer that, let's clarify what Pause & Resume is and how it became a prominent technology choice.

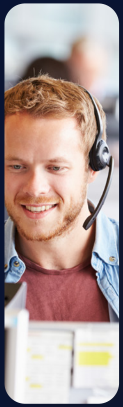
What is Pause & Resume Call Recording?

When customers call your business, an agent answers. The agent and caller eventually reach a point where the caller makes a payment. To adhere to laws and regulations, the agent pauses the call recording so sensitive financial data isn't stored in the system. Once payment has cleared, the agent resumes the recording so the remaining call is documented for legal purposes.

Why is Pause & Resume Call Recording so Widely Used?

In 2006, the Payment Card Industry Security Standards Council (PCI SSC) was formed by the biggest payment card providers: American Express, Discover Financial Services, JCB International, MasterCard, and Visa.

The PCI SSC outlined how to keep data secure e.g. encrypting stored data. The key stipulation relevant to call recording was to never store sensitive cardholder data.



Pause & Resume call recording became popular because of the wrongful belief that it complied with the PCI SSC's advice. Businesses had been instructed not to record sensitive data. By pausing recordings when necessary, agents believed they were fulfilling this security requirement.

Never recording calls isn't a realistic option as it may be a legal requirement to record data, especially if the authorities need access to it. From dispute resolution, claim investigation, fraud prevention and training, recordings can play an important role in the call center and, as a result, quickly became seen as a suitable compromise.

Reducing the need to store sensitive data while still being able to access information in the moment - however, relying on Pause & Resume today can cause more problems than it solves, resulting in systemic governance failures, breaches and loss of business.

Is Pause & Resume Call Recording Compliant?

Manual Pause & Resume call recording relies on the customer service agent to implement at the right moment. The concerns and challenges inherent in this approach include human error. It's all too easy for an agent to forget to pause the call - particularly in busy or high-volume periods. This means they'll record sensitive information and store it illegally. Alternatively, agents could be rushed through the call by a customer - missing important information that might be useful in the event of a later dispute.

As a result, many call centers opt for automated call recording however this too comes with risks. No technology works perfectly 100% of the time, however, this would be unacceptable if there was an investigation by regulatory bodies. They would expect full recordings and failing to assist them could lead to bad publicity and reputational damage if missed recordings became public knowledge.

Ultimately, neither manual or automatic call recording solutions can prevent one of the most prevalent and potentially damaging risks associated with CNP (Card Not Present) payments. Neither can they prevent an unhappy employee from sabotaging your business.

Businesses go to great lengths to protect themselves from external threats while overlooking the very real threat of breaches originated within the confines of the business.

Keeping Data Safe from Agents

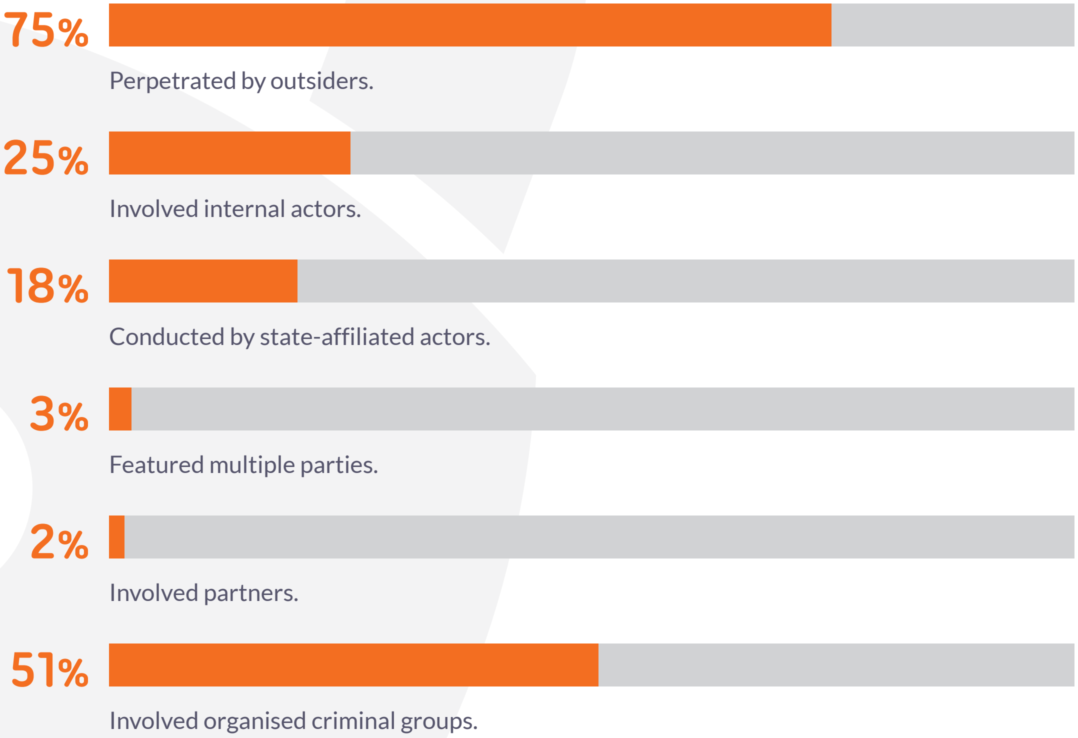
Verizon's 2015 Data Breach Investigations Report revealed that 50% of security breaches are caused by insiders. 20% are considered misuse events which sees employees stealing and/or profiting from company-owned or protected information. With automatic recording, the agent simply writes down the information by asking the customer to repeat financial data just to confirm it's been entered correctly. With manual recording, an agent could stop your business's recording and start their own. Once they pause the recording, your business has no record of criminal behavior and can't help the authorities. Failing to assist in the justice process would anger customers whose details were exploited.

The Impact on Customer Experience

Non-compliance isn't the only way Pause & Resume risks causing customer dissatisfaction. When businesses struggle to make Pause & Resume more compliant, they try changing their system e.g. transferring callers to a separate payment provider.

Transferring callers can result in dropped calls, frustrated would-be customers, and ultimately, lost sales.

Who’s behind the breaches?



[1] Maggie Overfelt, “World's oldest hacking profession doesn't rely on internet” CNBC. Published May 13th 2016. Retrieved September 2nd 2017 from https://www.cnbc.com/2016/05/13/a-surprising-source-of-hackers-and-costly-data-breaches.html

[2] Sarah Ingrams, “Does your energy company keep you waiting?” Which? Published November 17th 2016. Retrieved September 2nd 2017 from http://www.which.co.uk/news/2016/11/does-your-energy-company-keep-you-waiting-456805/

What is the Potential Cost of a Data Breach?

Many businesses wrongly believe that Pause & Resume is secure from malicious parties. They discover the hard way that non-compliance leads to massive fines that could put them out of business altogether. But a 'massive' fine can mean different things to different businesses.

What do Security Breaches Cost?

IBM's 2017 Cost of Data Breach Study, independently conducted by the Ponemon Institute, revealed a mixture of good and bad news. The number of security breaches dropped, but the breaches grew larger by 1.8% to more than 24,000 records. One unhappy customer is bad publicity. 24,000 could put you out of business.

Despite the cost of security breaches dropping by 10%, the average cost in the U.S. is still vast: $3.62 million, around $141 per record lost or stolen. With the advent of recent legislation changes spurred on by high-profile Equifax and Transunion cases, as well as the inception of Europe's GDP regulations, these costs are set to skyrocket.

What Could a Security Breach Cost Your Business?

Vitrium, a security and analytics software provider, shared a "guesstimate" of the potential cost to your business. Assuming the worst, a security breach could financially impact your business in the following ways:

- $1,000,000s: At least a 30-50% loss in direct customer revenue.
- $100,000 to repair your business reputation.
- $100,000 for damage control.
- $100,000 to find out who breached your security.
- $100,000 to take legal action.

You'll also need to pay for infrastructure upgrades to prevent another breach. Additionally, any intellectual property may have also been leaked, eroding competitive edge.

Smaller businesses don't have millions to spend after a security breach. As we've seen in the past twelve months, larger corporations can outlast the downturn, but their damaged reputation and lost customers will cut profits long-term.

In May 2018 a new data protection law, the GDPR, came into force. The ICO has the power to fine companies up to 4% of their global turnover or €20 million (whichever is higher). That will be in addition to the millions of pounds and dollars spent recovering from security breaches.

If Pause & Resume could put companies out of business, why is this outdated technology still in use by so many organizations?

A “guesstimate” cost to your business

$1,000,000s

At least a 30-50% loss in direct customer revenue.

$100,000

To repair your business reputation.

$100,000

For damage control.

$100,000

To find out who breached your security.

$100,000

to take legal action

[3] IBM Security, “2017 Ponemon Cost of Data Breach Study”IBM. Retrieved September 2nd 2017 from https://www.ibm.com/security/data-breach/

[4] Ibid.

[5] ICO, “Private health firm fined £200,000 after IVF patients’ confidential conversations revealed online” Information Commissioner’s Office. Published February 28th 2017 Retrieved September 2nd 2017 from https://ico.org.uk/about the-ico/news-and-events/news-and-blogs/2017/02/private health-firm-fined-200-000-after-ivf-patients-confidential conversations-revealed-online/

[6] Vitrium, “How Much Does a Data Breach Cost? A Quick Worksheet” Vitrium. Published July 2nd 2015. Retrieved September 2nd 2017 from http://blog.vitrium.com/document security-protection-drm-blog/how-much-does-a-data-breach cost-a-quick-worksheet

Why do Businesses Use Old Call Recording Technology?

The decision to stay with the status quo is driven by three widely held but incorrect beliefs:

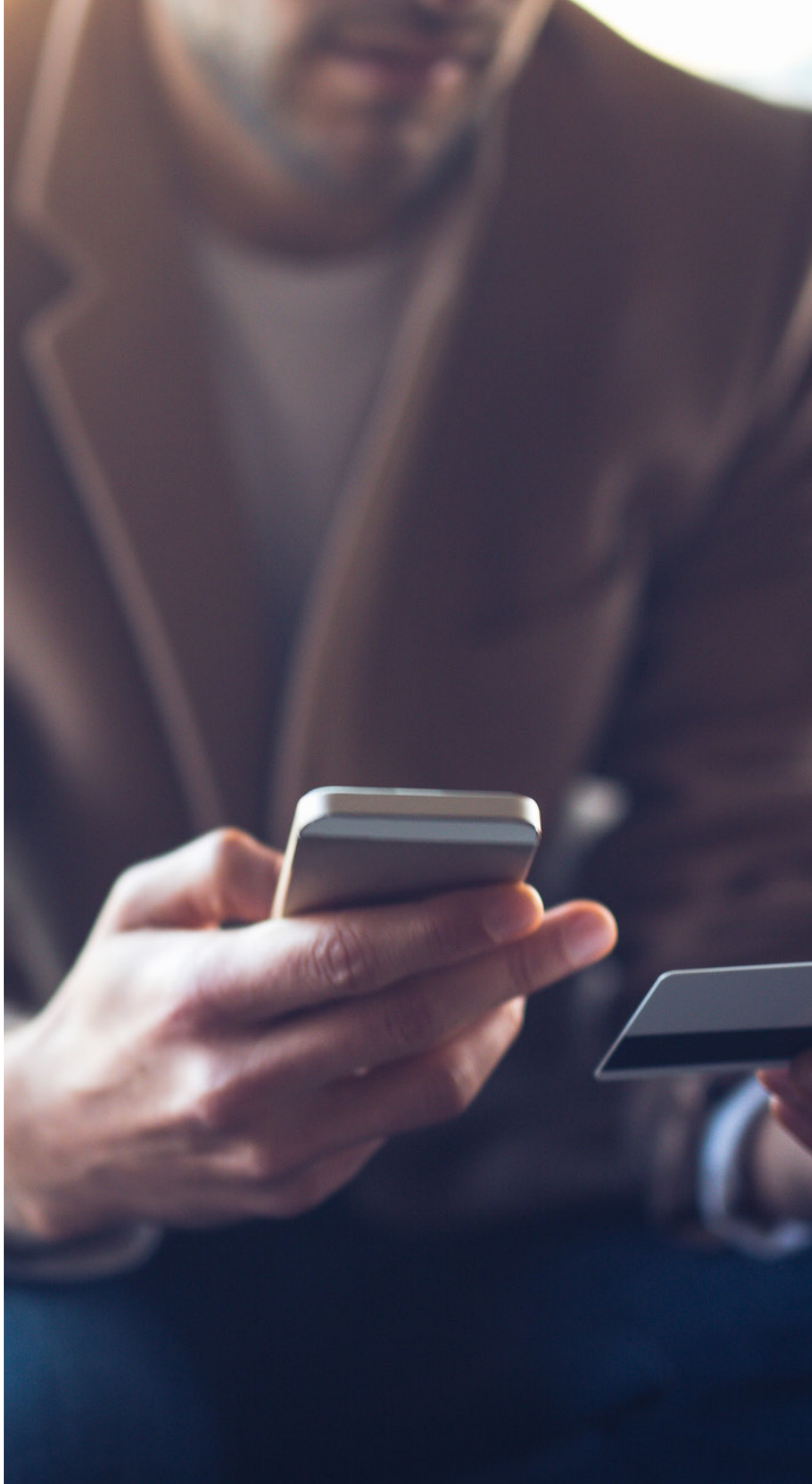
1. It's time and cost-efficient

Short-termism and a lack of planning leaves businesses thinking the smart decision is to delay spending on call recording technology. Short term savings will be heavily outweighed by long-term penalties and reputational impacts caused by security breaches. Data breaches have led to six-figure fines, lost customers, and damaged business relationships. An expensive breach greatly exceeds the short-term cost of upgrading to Payment Card Industry Data Security Standards (PCI DSS) compliant technology. In addition, agents are happier knowing updated technology makes their job easier, quicker and less stressful.

2. SAQ is Sufficient

Some businesses assume they are compliant because they passed Self-Assessment Questionnaires (SAQs), meeting certain PCI DSS requirements. If the assessment is passed, an Attestation of Compliance certification is issued. However, compliance and secure are not necessarily the same thing. In January of this year, PCI DSS 3.2 was introduced to build a culture of constant preparation as opposed to exam compliance cramming.

Many companies struggle to ensure continuous compliance - data taken from a 2017 report found that at the time of data compromise the average merchant is not compliant with almost half (47%) of current PCI DSS requirements. Of those that do pass compliance checks, almost a third are



not compliant just 12 months later, according to Verizon's PCI DSS Compliance report.

Ultimately, being "compliant with PCI DSS at one point in time does not prevent things from changing in your environment, which - if the proper controls are not implemented - could impact your security."

3. They Believe They're Already Compliant

Some businesses take security seriously, but their data protection methods are still not quite PCI DSS compliant. For example, a popular but non-compliant way of protecting data is through encryption.

The PCI SSC outlines acceptable encryption and access protection, but how many businesses take the time to confirm that their encryption is compliant? Instead they trust their security provider, not realizing they aren't compliant until it is potentially too late. Encryption also misleads businesses by encouraging them to store encrypted data. Compliance means certain data is not permitted to be stored under any circumstances, even when encrypted.

The PCI SSC allows the following to be stored if they're protected:

- Primary Account Number (PAN)
- Cardholder Name
- Expiration Date

The problem is the storing of sensitive data, such as:

- CAV2
- CVC2
- CVV2
- CID

The PCI SSC states the following: "It is a violation of PCI DSS requirement 3.2 to store any sensitive authentication data, including card validation codes and values, after authorization even if encrypted". Using Pause & Resume without 100% accuracy means businesses record and store this sensitive information by accident. Storing sensitive data means hackers can use data to steal money and identities.

If Pause & Resume technology is non-compliant, what is the alternative?

[7] PCI Security Standards Council, "PCI DSS Self-Assessment Questionnaire Instructions and Guidelines, v3.2" PCI Security Standards Council, LLC. Published May 2016. Downloaded September 1st 2017 from https://www.pcisecuritystandards.org/documents/SAQ-InstrGuidelines-v3_2.pdf, page 5

[8] The Direct Marketing Association, "PCI DSS Compliance as it relates to Call Recording" The Direct Marketing Association (UK) Ltd 2011. First Edition. Downloaded September 1st 2017 from https://dma.org.uk/uploads/PCI%20Guidance%20Notes_542ec328e8176.pdf, page 4

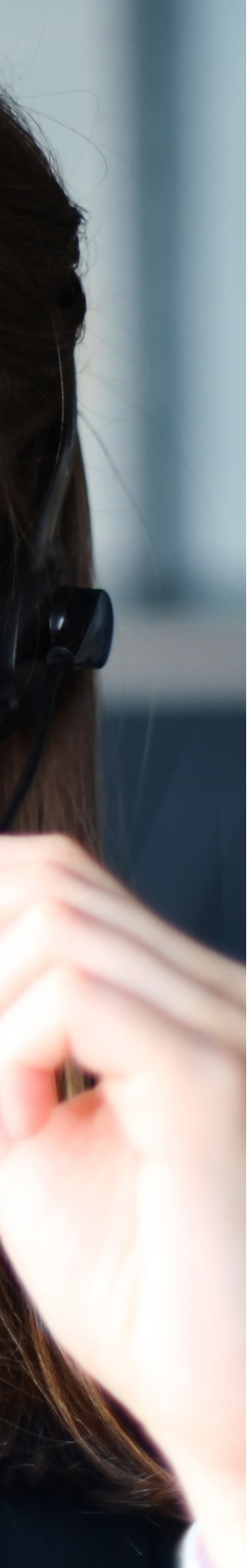
[9] Ibid, page 5

DTMF Technology:
Is it PCI DSS Compliant?

What is DTMF Technology?

PCI compliance is crucial. Being PCI compliant shows consumers, businesses and legislators that you took steps to protect your customers' data - potentially reducing fines and the potential for civil or criminal action.

Compliance also shows customers that your business takes security seriously, so they're less likely to blame you if there is a breach.
That's why Dual Tone Multi Frequency (DTMF) technology is important for PCI DSS compliance.



Is DTMF Technology PCI DSS Compliant?

DTMF technology works by removing any need for the agent to see, hear or store sensitive payment data in three steps:

1. When payment is required, the customer uses the phone's keypad to enter private financial information.
2. The information is hidden on-screen so agents can't see it. Audio plays so they can't hear the keypad's tone. Whenever the customer speaks, their voice is audible so the agent can provide assistance.
3. When the customer is finished, the agent submits the information to the payment provider. It is processed by the provider, not the agent's business.

Here are three ways DTMF call recording meets PCI DSS compliance:

1. Removes Manual Intervention

PCI compliance means there should be no manual intervention. DTMF technology is compliant because agents don't stop and start recordings. All the data that customers enter is hidden so recordings are continuous. This means disgruntled employees can't record and sell financial information illegally.

2. Eliminates Missing Audio

Businesses may be required to provide full recordings e.g. showing proof of transactions to the Financial Conduct Authority. Because DTMF technology removes the need for manual intervention, employees can't mistakenly stop recording. If the authorities need proof for an investigation, complete DTMF recordings without interruptions would be compliant unlike incomplete Pause & Resume recordings.

3. Eliminates Illegal Data Storage

As DTMF removes manual intervention so there's no illegal recording of sensitive financial information like magnetic stripe data. Customers submit their details without revealing this data openly, so it can't be stored. By sending the transaction to the payment provider, the burden of legal data storage is transferred to them.

In addition to PCI DSS compliance and simplicity, DTMF call recording has the following benefits:

Quicker Calls

Instead of customers struggling to speak over loud call centers, they just input numbers into their keypad. This means calls are processed faster, which cuts waiting times for other customers. Those customers are less likely to hang up because they've been waiting for so long.

More Privacy

When customers need assistance in a public setting e.g. at work, they can use the keypad instead of sharing private information aloud. They have more control over when they share financial information and who they share it with.

Is PCI Pal's Agent Assist PCI DSS Compliant?

PCI DSS compliance involves meeting certain requirements. Let's see how PCI Pal's Agent Assist DTMF solution is compliant from start to finish.

No Manual Intervention

The agent opens Agent Assist's desktop application so the customer has privacy while they enter sensitive information. The application never gives agents access to the recording software, so they can't pause call recordings. No manually administered recordings are PCI DSS compliant.

Payment Information Hidden

Payment information is hidden by the desktop application. It replaces numbers entered with asterisks. The application also hides information by masking the keypad's tone with a monotone beep. This means agents and third parties can't decipher the data by using the keypad tones.

No Sensitive Data Stored

The customer enters their information into the keypad. Once they've finished, the agent submits the details straight to the payment provider, meaning no sensitive data is stored.

Are There Additional Agent Assist Benefits?

Businesses need more than just PCI DSS compliance to operate a secure and efficient contact center. The Agent Assist solution also offers the following business-friendly options:

Flexible Payments

Whether your business is an international brand or a small business, Agent Assist suits your budget. This DTMF call recording service is available with various pricing options.

Maximum Sales Opportunities

Some customers are so loyal to their favorite payment provider, they won't do business if it isn't available. Fortunately, Agent Assist can be integrated with any payment providers. By offering integration with every payment provider, you'll maximize profit instead of turning away customers who might never come back.

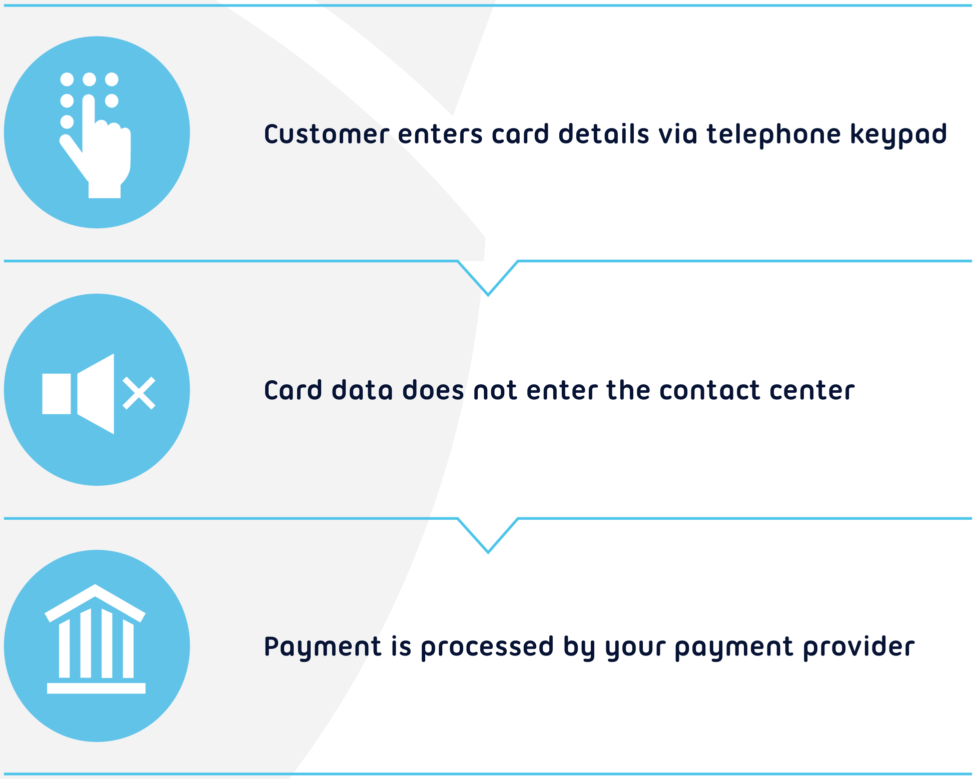
Fast DTMF Integration

Agent Assist could be deployed within weeks. If integration is required, there are various options. Fully hosted integration involves connecting your call traffic to Agent Assist's secure cloud (99.999% uptime). Payments are still processed by DTMF technology, so PCI compliance is continuous. With on demand integration, your business controls calls while Agent Assist manages the payment stage. Financial data is transmitted via DTMF to ensure PCI compliance.

A Compliant Provider

Call recording companies should take data security very seriously. We demonstrate how seriously we take security by ensuring our entire business is PCI DSS compliant, not just our contact center services.

There are various security levels for service providers. Our company adheres to Level 1, which is the highest level of security required by the leading card companies. We maintain our compliance by adhering to the latest Payment Card Industry Data Security Standards.



Customer enters card details via telephone keypad

Card data does not enter the contact center

Payment is processed by your payment provider

Conclusions

Pause & Resume processes urgently need replacement. They greatly increase the risk of data breaches and loss of data that could lead to six-figure fines, lost customers and the breakdown of business connections. The financial cost could be much higher with the General Data Protection Regulation law in place as of May 2018.

Businesses who replace old Pause & Resume systems with modern DTMF technology enjoy many benefits. DTMF users cut the risk of legal action, have full PCI DSS compliance and reduce the chance of security breaches.

When your business is ready for these benefits, get in contact with a reputable DTMF provider to upgrade your call recording technology. Within weeks, you could be fully compliant with data security regulations, easing the workload for your agents, and increasing customer satisfaction.

Thank you

We hope you found this eBook useful. If you have any further questions about PCI compliance or would like to find out how PCI Pal can help secure your contact center, please get in touch with our expert consultants today.

Keep an eye out for the next guide in our series on PCI compliant contact centers, coming soon.

GET IN TOUCH

☎ U.S. +1 866 645 2903

☎ U.K. +44 207 030 3770

✉ info@pcipal.com

U.S. 615 South College Street, Floor 9, Charlotte, NC 28202, USA

U.K. 1 Cornhill, London EC3V 3ND

www.pcipal.com

Secure contact center technology
from contact center people.