Contact Centre
PCI DSS Compliance

semafone
securing data · protecting reputations

cardprotect

The Perils and Pitfalls of Pause and Resume Recording

Call Recording and Payment Card Data – The Facts

Gaining and maintaining compliance with industry rules and best practice guidelines is a top priority, especially for highly regulated industries such as financial services where call recording in contact centres is standard practice, and may even be a mandated requirement.

In the UK for example, organisations regulated by the Financial Conduct Authority (FCA) are required to record all telephone conversations that involve client orders.

Organisations from a variety of industries record customer calls for a number of reasons including regulatory, legal, training, analytics and caller mood, or quality control. Indeed, having a full and complete call recording of customer phone interactions can:

- Make dispute resolution quicker and easier
- Provide an effective way to train and coach staff to handle customer enquiries effectively
- Enable calls to be reviewed for quality control purposes to ensure contact centre teams comply with regulatory or good practice guidelines
- Help discourage the provision of fraudulent or incorrect information to callers
- Protect agents from dishonest claims, and protect organisations from dishonest agents!

Putting call recording practices in place requires a careful evaluation of any laws and rules governing privacy and the recording or monitoring of telephone calls.

However, if your contact centre takes card payments over the telephone you will also need to comply with PCI DSS (Payment Card Industry Data Security Standard) regulations, which stipulate that sensitive authentication data such as three or four-digit security codes (CID, CVC2, CVV2 or CAV2) must be protected – and cannot be recorded or stored.

This creates a dilemma: how do you record calls, keeping sufficient evidence of transactions, without recording sensitive payment card details?

At first glance, Pause and Resume recording systems appear to offer the ideal quick fix to the PCI DSS compliance challenge, enabling calls to be paused at the point of payment and resumed once payment is complete.

But, as we'll see, Pause and Resume is an inadequate security approach that exposes organisations to considerable risk in terms of compliancy and fraud.

Let's find out why.

Pause and Resume – A Risky Enterprise

Although Pause and Resume has become a widely used contact centre practice, it does not necessarily deliver guaranteed or robust PCI DSS compliance. In 2018 the PCI SSC updated the guidance for Protecting Telephone-Based Payment Card Data to address this.

Manual or automated Pause and Resume solutions often cause more problems than they solve – and these flaws can result in systemic governance failures. As a result, it's not unusual for organisations having to undertake a 'rethink' on how to address compliance of the entire contact centre estate.

Manual Pause and Resume

This places day-to-day compliance responsibilities in the hands of front line personnel, an approach that has several disadvantages:

- **Human error** – busy agents can forget to pause and subsequently resume a call at precisely the point when important details are being discussed with a customer. As well as making dispute resolution difficult, this could result in non-compliance with mandated data retention requirements
- **Deliberate abuse** – agents have the ability to pause recordings whenever they want during a call to say something off the record, offer unethical advice or upsell to hit personal targets. From a compliance standpoint, unmonitored conversations represent a big problem
- **Insider fraud** – agents can still see and hear the customer's payment card details being relayed verbally, noting these down for their own malicious use
- **Accidental card data capture** – agents can forget to start the pause at the point of payment, resulting in sensitive cardholder data being stored in the recording
- **Agent initiated Pause and Resume is not PCI DSS compliant** – PCI DSS regulations unequivocally state that sensitive card authentication data must be removed from recordings automatically, with no manual intervention by staff

Source: PCI SSC Information Supplement: Protecting Telephone-based Payment Card Data

This explains why, to address PCI DSS compliance, many organisations have instead looked to automated Pause and Resume technology.

Automated Pause and Resume

Integrated into contact centre technologies used by agents, automated Pause and Resume solutions automatically stop and re-start recordings without agent intervention, as part of the business process workflow. In some instances, systems are set up to monitor which applications the agent is using to trigger automated pause and resume functions.

While more reliable than manual call recording methods, automated Pause and Resume isn't a fool proof approach:

- **Risk management** – omitting the payment section of a call complicates fraud investigation and dispute resolution
- **Non-compliance** – pausing call recording will conflict with the compliance requirements of regulatory bodies that mandate all calls must be recorded in their entirety
- **Technical complexity** – dependent on the "seamless" integration of call recording, agent desktop and call management systems, automated Pause and Resume may result in the introduction of 'workaround' processes to get everything working in concert and typically results in a longer average call handling time (AHT).

  If any ability exists for the agent to bypass the integrated process, the pause-and-resume technology could be circumvented and rendered ineffective.
- **Secure deletions** – recordings that contain CHD and SAD should be securely deleted. The contact centre should only allow call recordings to be retrieved or listened to by an authorised senior manager. In addition, multi-factor authentication controls need to be added to call recording solutions, as well as storage and search tools.

- **Customer satisfaction** – customers that struggle when transferred to a separate payment process may abandon the call – and may not ring back, especially in debt collection scenarios
- **Agents and other internal systems are still exposed to card data** – at best, automated Pause and Resume excludes only the call recording from PCI DSS compliance scope. Agents can still hear customer card details – putting these at risk of compromise – and any personal card data held in contact centre systems is vulnerable to cyber-attack

Expensive to implement and complex to deploy, automated Pause and Resume is a quick fix that addresses a small part of the overall PCI DSS compliance issue. AND it only addresses a single element in relation to providing contact centre security.

That's important, because PCI DSS also states that a cardholder's full primary account number (PAN) cannot be kept without further protection measures, as this potentially exposes cardholder data to unnecessary risk.

A Better Way

To reduce the risk of fraud – and achieve PCI DSS compliance – you need to prevent card holder data flowing through your call recordings, agents, desktops, IT systems, the physical environment and telephony network.

And that's where Semafone's patented data capture technology can help.

A proven and award winning PCI DSS compliance solution that prevents payment card data from entering the contact centre in the first place, Semafone makes it possible for organisations to achieve PCI DSS compliance while recording calls in their entirety.

So, how does it work?
Customers simply enter their card number directly into the telephone keypad rather than saying them out loud. These numbers are sent straight to the card provider, so sensitive card details never enter the contact centre infrastructure.

And while the call recording captures all voice communications, all DTMF tones are masked so only a flat tone is recorded – making it impossible for agents to recognise numbers or reverse engineer any card data from the call recording itself.

Semafone's approach allows organisations to significantly reduce their PCI DSS burden and initial and ongoing compliance costs, while recording calls in their entirety:

- **Agents** are no longer exposed to cardholder data – protecting organisations against the risk of opportunistic agent fraud and associated reputational damage
- **Payment card details** never enter the contact centre infrastructure – reducing the risk resulting from any data breaches
- **Fully enables a flexible agent workforce** – the solution works with outsourcers and home or remote workers – all your customer service representatives can now take payments securely, **wherever they are located**
- **Cyber-insurance premium costs** are lower for de-scoped organisations, compared to those that are simply compliant

semafone®
securing data · protecting reputations

- **Minimal agent intervention** is required – the system automatically hides card entries and blocks DTMF tones from being recorded, leaving agents to focus on the job in hand
- **Customers can stay on the phone** with agents while payment is taken – giving them a faster, more streamlined experience and reduced AHT
- **Call recordings can continue** without interruption – there's no need to use Pause and Resume and risk non-compliance with other regulatory or industry requirements
- **Eliminating card information** from the contact centre significantly simplifies PCI DSS compliance – removing Sensitive Authentication Data (SAD) before it hits the call recorder and the contact centre infrastructure and taking the contact centre out of scope for any PCI DSS audit
- **Contact centres gain** new operational flexibility – there's no requirement to operate the draconian measures associated with clean rooms

Semafone – The Leader in Contact Centre PCI DSS Compliance

When it comes to assuring PCI DSS compliance, Pause and Resume isn't the answer.

As we've seen, it's a tactical 'sticking plaster' approach that leaves agents – and the contact centre infrastructure – exposed to sensitive card data.

But with Semafone, protecting contact centre customers from fraud while complying with PCI DSS becomes easy. Using patented technology, Semafone securely captures credit and debit card data taken over the phone and reduces the number of PCI requirements significantly.

Even better, with Semafone all calls and call recordings can continue as normal, with minimal disruption to customers or contact centre operations. Contact us now on **0845 543 0822** or **emeasales@semafone.com** and we'll show you how.

The Facts

- The average size and cost of a data breach is growing and depending on geographical region, can be **as high as $11m**.
  Source: The Ponemon Institute 2018 Cost of Data Breach Study reports the global average cost of a data breach is up 6.4 percent over the previous year to $3.86 million.
- Card Not Present Fraud is now 81 percent more likely than point of sale fraud.
  Source: Annual 2018 Identity Fraud Study by Javelin Stategy & Research.
- The Kroll Global Fraud & Risk Report 2018, shows how fraud continues to climb and of those reporting a fraud incident, 81% cited one or more insiders as perpetrators.
- **Survey reveals 10 top U.S. insurers ask for verbal confirmation of payment card details.**
  Source: Semafone research 2017
- Using Cardprotect from Semafone significantly reduces the number of PCI DSS requirements

New PCI SSC Guidance for Securing Telephone-Based Payment Card Data

The updated guidance catches up with technology for the first time since 2011. QSA's now have clear guidelines regarding call recordings and the capture of sensitive card details. If a contact centre is using either manual or automated Pause and Resume, QSA's can demand extensive evidence of measures to protect sensitive data, and are empowered to conduct invasive auditing to ensure that additional controls have been effectively put in place.

To find out more about the **updated guidance**, please take a look at our handy fact sheet, which outlines the main changes.

The updated PCI DSS guidance can be found **here**.

cardprotect