

# The Perils and pitfalls of Pause and Resume recording.

How it's hindering your agents, your CX, and your bottom line.

## Call recording and payment card data – the facts.

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

Organizations in many industries record customer calls for a wide range of reasons including training, analytics, caller sentiment, quality control, regulatory, and legal purposes. Having a full and complete call recording of customer phone interactions can:



Provide evidence that contact centers comply with regulatory or best practice guidelines



Provide an effective way to train and coach agents to handle customer inquiries more effectively



Enable calls to be reviewed for quality control purposes



Assess and improve agent performance



Ensure dispute resolution is processed quickly and easily



Protect organizations and agents from costly dishonest claims

If your contact center takes card payments over the phone, you will also need to comply with the Payment Card Industry Data Security Standards (PCI DSS), 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? On top of that, how do you juggle staying compliant while protecting your organization and ensuring your agents are delivering the CX your customers expect?

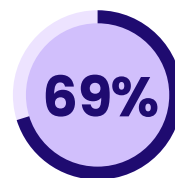
At first glance, Pause and Resume recording systems appear to offer the ideal quick fix to the PCI DSS compliance challenge, enabling calls to be paused at the point of payment and resumed once payment is complete.

However, Pause and Resume is an inadequate approach that exposes organizations to considerable risk in terms of compliance and security, and it can have a negative impact on CX.

Contact center PCI DSS compliance involves a whopping **438 security controls**. Pause and resume addresses **just ONE element** (call recordings), leaving the rest of your contact center—and your organization—vulnerable

## Pause and Resume: a risky approach for your organization – and customer loyalty.

Although Pause and Resume has become a widely used contact center practice, it doesn't guarantee PCI DSS compliance, and doesn't safeguard your organization from costly data breaches. Further, data breaches could cost you even more in customer loyalty and retention.



In a recent survey of 6,000 consumers, **69% said they would avoid doing business with a company that had suffered a data breach**, even if it offered a better deal than competitors

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 organizations having to undertake a review on how to address compliance of the entire contact center estate, costing more precious time, money, and resources.

A properly implemented Pause and Resume solution can help reduce the applicability of PCI DSS by taking the call-recording and storage systems out of scope – but it's important to know that the technology does not reduce PCI DSS applicability to the agent, the agent desktop environment, or any other systems in the telephone environment.

Pause and resume leaves your organization vulnerable to expensive data breaches: the average **global cost in 2023 was \$4.45 million USD – a 15% increase over 3 years!**

✉ nasales@sycurio.com

✉ emeasales@sycurio.com

☎ +1 888-267-5723

☎ +44 (0)845 543 0822



**Sycurio.**

## Manual Pause and Resume: the costly consequences.

- ✘ **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
- ✘ **Frustrated customers** – not only could this result in difficulties with dispute resolution, non-compliance with mandated data retention requirements and sensitive payment data being stored on the recording, it also puts you at risk of receiving lower customer satisfaction scores (CSAT) from frustrated customers who have to repeat their information to be recaptured or corrected by agents
- ✘ **Deliberate agent 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. This is especially important to note if you have agents that work from home
- ✘ **Increased risk of insider fraud** – Remote locations and homes are almost impossible to effectively secure – shared living spaces and housemates present unpredictable security problems when sensitive payment data is entering your organization – and ultimately your agents' homes. If you use Pause and Resume, agents can still see and hear the customer's payment card details being relayed verbally (and it can be overheard by others) noting these down for their own malicious use and increasing your organization's risk of insider fraud and data breaches

9.6% ↑

Attacks initiated by malicious insiders cost organizations on average \$4.90m – that's **9.6% higher** than the global average cost of data breach!

## Automated Pause and Resume: a step up, but still risky.

Following the publication of the [PCI SSC guidance for Protecting Telephone-Based Payment Card Data](#) some organizations moved to automated Pause and Resume.

What's the difference between manual and automated Pause and Resume? Automated Pause and Resume solutions instinctively stop and restart 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 foolproof approach to safeguard your organization from costly data breaches, reductions in operational inefficiency, and the risk of lost customer loyalty and retention.

- ✘ **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 the array of systems working in unison
- ✘ **Increased AHT and decreased CSAT** – this workaround process typically results in a longer average call handling time (AHT). Further, if any ability exists for the agent to bypass the integrated process, the Pause and Resume technology could be circumvented and rendered ineffective. Additionally, customers that struggle when transferred to a separate payment process may abandon the call – and may not ring back, especially in debt collection scenarios
- ✘ **Organization & agent exposure to payment data** – at best, automated Pause and Resume excludes only the call recording from PCI DSS compliance scope. Your contact center and your agents are both still exposed to sensitive payment data entering your organization
- ✘ **Increased risk of data breaches** – with payment data flowing through your contact center environment and systems and your agents still able to see and hear customer card details, your organization is vulnerable to brand damaging and costly data breaches
- ✘ **Risk management** – omitting the payment section of a call complicates fraud investigation and dispute resolution

Expensive to implement and complex to deploy, automated Pause and Resume is a quick fix that only resolves a small part of the overall PCI DSS compliance issue, while also hindering agent productivity, your CX efforts, and your bottom line.

## When it comes to secure payment solutions, Pause and Resume isn't the answer.

As we've highlighted, Pause and Resume is a tactical approach that leaves agents and the contact center infrastructure exposed to sensitive payment data. This results in a risk to customer retention and loyalty, as well as your bottom line.

With Sycurio.Voice, protecting organizations from costly fraud and data breaches while staying compliant and ensuring happier customers becomes straightforward and easy to implement. Sycurio's patented payment method using DTMF masking securely captures credit and debit card data taken over the phone, **without sensitive data ever entering your organization.**

Even better: with Sycurio, all calls and call recordings can continue as normal, with little disruption to customers or contact center operations. The solution integrates seamlessly with contact center systems & payment service providers (PSPs) and training and onboarding is simple – so agents can be up and running in no time!

✉ nasales@sycurio.com

✉ emeasales@sycurio.com

☎ +1 888-267-5723

☎ +44 (0)845 543 0822



**Sycurio.**

# Sycurio.Voice

## Sycurio.Voice – the better choice.

To safeguard your organization from data breaches, achieve PCI DSS compliance, and improve your operational efficiency, customer satisfaction, and bottom line, you need to prevent payment data from flowing through your call recordings, agents, desktops, IT systems, the physical environment, and telephony network.



That's where Sycurio can help – offering a proven and award-winning PCI DSS compliance solution that prevents sensitive data from ever entering your entire organization.

## So, how does it work?

Customers simply enter their card number directly into the telephone keypad or by using the integrated Secure Speech Recognition feature. These numbers are sent straight to the PSP, so sensitive card details never enter the contact center 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 recognize numbers or reverse engineer any card data from the call recording itself.

Sycurio's approach allows organizations to significantly ease their PCI DSS burden, lower compliance costs, reduce the risk of data breaches, improve CX, and protect their bottom line – all while recording calls in their entirety:

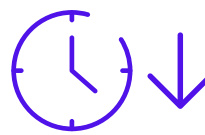
- ✓ **Agents are no longer exposed to cardholder data** – protecting organizations against the risk of opportunistic agent fraud, insider data breaches, and associated reputational damage

19%

Internal actors (employees, contractors, and interns) are responsible for **19% of data breaches**<sup>2</sup>

- ✓ **Payment card details never enter the contact center infrastructure** – significantly reducing the risk of costly data breaches
- ✓ **Fully enables a flexible agent workforce** – whether on-site, remote, hybrid, or outsourced, Sycurio is the single payments solution for all your agents, wherever they're located. Providing your staff with a flexible working environment can boost retention rates and opens up new recruitment opportunities

- ✓ **Minimal agent intervention is required** – the system automatically hides card entries and blocks DTMF tones from being recorded, freeing up agents' time to focus on the job in hand. This extra time enables agents to carry out wrap up activities during the call while customers type in their card numbers
- ✓ **Seamless CX** – customer stay on the phone with agents while payment is being taken, creating better call outcomes and reduced AHT... and improving CSAT scores by keeping agents engaged with customers throughout the entire interaction – instead of agents starting/stopping recording or reading back payment details



Sycurio reduces AHT by

**7–30 seconds**

- ✓ **Operational flexibility and improved bottom lines** – reducing opportunities for error through providing a single point of numerical entry, improving first time resolution (FTR) by automatically carrying out early verification BIN and Luhn checks during the call, and eliminating the requirement to implement the inflexible measures associated with operating 'clean rooms' are just a few ways using Sycurio can help boost productivity and reduce costs
- ✓ **Lowered cyber insurance premium costs** – organizations with de-scoped compliance can enjoy lower cyber insurance premiums compared to those that are simply compliant
- ✓ **Reduced time and cost investment of PCI DSS compliance** – using Pause & Resume requires a SAQ- D, the most comprehensive, costly, onerous, and complex SAQ involving around **438 controls**. **Sycurio.Voice requires SAQ-A – a much simpler, cost effective SAQ and reduces scope to just 6 controls.**

✉ nasales@sycurio.com

✉ emeasales@sycurio.com

☎ +1 888-267-5723

☎ +44 (0)845 543 0822



**Sycurio.**