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 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.

For example in the US, FINRA (Financial Industry Regulatory Authority) mandates recording telephone conversations between their registered persons and existing/potential customers regarding trading activities and in the UK, organizations regulated by the Financial Conduct Authority (FCA) are required to record all telephone conversations that involve client orders.

Organizations from a variety of industries record customer calls for a wide range of reasons including regulatory, legal, training, analytics, caller sentiment and quality control. Indeed, having a full and complete call recording of customer phone interactions can:

- Ensure dispute resolution is processed quickly and easily
- Provide an effective way to train and coach staff to handle customer enquiries effectively
- Enable calls to be reviewed for quality control purposes
- Provide evidence that contact centers comply with regulatory or good practice guidelines
- Protect organizations and agents from dishonest claims
- Understand agent performance

Non-compliance: pausing call recordings will conflict with the compliance requirements of regulatory bodies that mandate all calls must be recorded in their entirety

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.

If your contact center takes card payments over the telephone 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?

Only **27.9 %** of organizations are **fully compliant** with the PCI DSS according to Verizon's Payment Security Report.

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 security approach that exposes organizations to considerable risk in terms of compliance and fraud.

Limited scope: Pause and Resume ONLY addresses a single element (call recordings) neglecting other critical contact center systems and environments... and your agents

Pause and Resume – a risky approach.

Although Pause and Resume has become a widely used contact center practice, it does not necessarily deliver guaranteed or robust PCI DSS compliance. The PCI SSC's Information Supplement on Protecting Telephone-Based Payment Card Data addresses 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 organizations having to undertake a review on how to address compliance of the entire contact center estate.

Whilst 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, **the technology does not reduce PCI DSS applicability to the agent, the agent desktop environment, or any other systems in the telephone environment.**

Manual Pause and Resume.

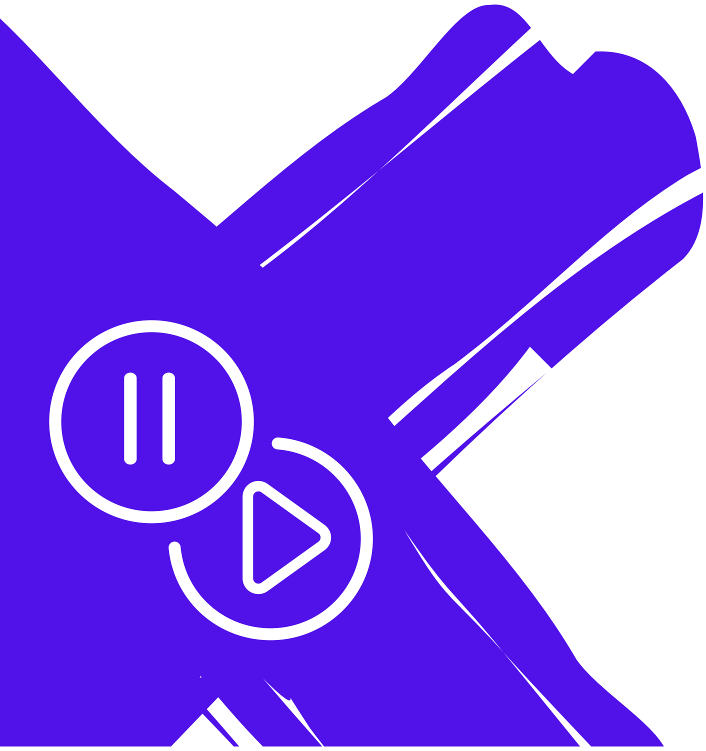
This places day-to-day compliance responsibilities in the hands of front-line personnel, an approach that has several disadvantages:

- ✖ **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

$4.90m

Attacks initiated by malicious insiders cost organizations on average $4.90m that's **9.6% higher** than the global average cost of data breach[1]

- ✖ **Accidental card data capture** – agents can forget to start pausing the call recording at the point of payment, resulting in sensitive cardholder data being stored on 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



Automated Pause and Resume.

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

Integrated into contact center technologies used by agents, automated Pause and Resume solutions instinctively 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 completely dependable approach:

- ✖ **Risk management** – omitting the payment section of a call complicates fraud investigation and dispute resolution
- ✖ **Non-compliance** – pausing call recordings 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 the array of systems working in unison. Something that 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 cardholder data (CHD) and sensitive authentication data (SAD) should be securely deleted. The contact center should only allow call recordings to be retrieved or listened to by an authorized senior manager. In addition, multi-factor authentication controls need to be added to call recording solutions, as well as storage and search tools
- ✖ **Customer experience** – 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 see and hear customer card details – putting these at risk of compromise – and any personal card data held in contact center systems is vulnerable to cyber-attack

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. Critically, it only addresses a single element in relation to providing contact center security. PCI DSS states that a cardholder's full primary account number (PAN) cannot be kept without further protection measures, as this potentially exposes cardholder data to further unnecessary risk.

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

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

With Sycurio.Voice, protecting contact center customers from fraud while complying with PCI DSS becomes straightforward and easy to implement. Using a patented payment method, Sycurio.Voice securely captures credit and debit card data taken over the phone and reduces the scope of compliance requirements significantly.

Even better, with Sycurio all calls, and call recordings can continue as normal, with minimal disruption to customers or contact center operations.

Sycurio.Voice

Sycurio.Voice - 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 Sycurio's patented data capture technology can help. It is a proven and award-winning PCI DSS compliance solution that prevents payment card data from entering your entire contact center environment, Sycurio makes it possible for organizations to achieve PCI DSS compliance while recording calls in their entirety.

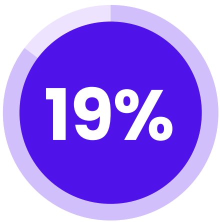
So, how does it work?

Customers simply enter their card number directly into the telephone keypad or by using the integrated Speech Recognition feature. These numbers are sent straight to the Payment Service Provider, 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 reduce their PCI DSS burden plus initial and on-going compliance costs, while recording calls in their entirety:

- ✓ **Agents are no longer exposed to cardholder data** – protecting organizations against the risk of opportunistic agent fraud and associated reputational damage
- ✓ **Payment card details never enter the contact center 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



Internal actors (employees, contractors and interns) are responsible for **19% of data breaches**[2]

- ✓ **Cyber-insurance premium costs** can be lowered for de-scoped organizations, compared to those that are simply compliant
- ✓ **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 center significantly simplifies PCI DSS compliance** – removing sensitive authentication data (SAD) before it hits the call recorder and the contact center infrastructure and taking the contact center out of scope for any PCI DSS audit
- ✓ **Contact centers gain new operational flexibility** – there's no requirement to implement the inflexible measures associated with operating 'clean rooms'
- ✓ **Reduce the time and cost 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**

Pause & Resume:
438
controls

Sycurio.Voice:
6
controls

✉ nasales@sycurio.com
☎ +1 888-267-5723

✉ emeasales@sycurio.com
☎ +44 (0)845 543 0822

Sycurio.

[1] IBM costs of data breach 2023 | [2] Verizon Data Breach Investigations Report 2023