www.veritape.com/callguard info@veritape.com Contact us on 0845 899 5500

What are the options available to ensure PCI compliance for call recording?

The Payment Card Industry Data Security Standards (PCI DSS) state that sensitive payment card data may not be retained once a transaction has been authorised. This means contact centres cannot store card data in call recordings.

Failure to comply may result in fines from card issuers (Visa, Mastercard, etc) of up to $50,000 per month and leave you open to potential internal or external fraud risks.

This document aims to outline the key questions that should be asked by companies before investing in a PCI compliant solution for their call recordings, and discusses the benefits and disadvantages of all 5 methods currently on the market.

What are the key questions to ask before selecting a PCI compliant solution?

- How quickly can the solution be implemented?
- How much integration work is required?
- What changes will need to be made to our business/back office processes?
- Does it require any changes to agent behaviour?
- Are there any interruptions to the conversation between the agent and the customer?
- Can the solution be scaled in line with company growth?
- Will it still work if system changes are made in the future?
- Does it work for cloud/virtual/network recording?
- Can it bring PCI compliance to our screen recording?
- Will it mean we are compatible with FSA regulations?
- Can we stop our agents seeing the card data to further reduce the chance of fraud?

There are 5 options currently available to companies looking for a PCI compliant solution for call recording

Option 1 - Turn off recording

This is as really quick and simple solution that gives instant compliance and may be the best approach for you.

However, you will obviously lose all the benefits associated with recording your calls, including use in staff training, customer complaint handling and the other business information the calls provide.

In a regulated environment, this really isn't a viable option.

Option 2 - External IVR

With an external IVR solution, the customer is transferred to a 'robot' where they enter their card details using their phone keypad. However, there are a number of disadvantages associated with this option:

- This route really changes the way your customers interact with you at present and interrupts the conversation between the Agent and the customer. You are also providing the customer with an opportunity to abandon the call if they are hesitant to proceed.
- An external IVR solution requires significant integration with back-end IT and telephony systems, which limits your flexibility around future purchasing decisions.
- Changes will need to be made to the working processes for your staff. For example, what does an Agent do when the caller is 'away' entering card details into the IVR? Nothing, or take another call (in which case the next part of the call needs to be handled by a different Agent, thus confusing the customer)?
- Your average call handling time is increased, which will result in an increase in telephone costs. In addition, telephony costs are automatically higher because you need

an additional outbound call in order to transfer customers to the IVR.

- You may also incur an increase in card processing costs as the acquirer being used by the IVR provider may grant worse rates than those currently in place directly.

Option 3 - Pause the recording

With this option, the recording is automatically 'bleeped' or paused, based on 'triggers' from screen information or agent behaviour.

Unlike Option 2, pausing the recording requires no changes to the Agent or customer behaviour. The potential problems with this route are:

- It is very difficult to integrate the Agent desktop payment processes with the recording system and requires both a very high level of IT programming skill and a long period of integration.
- If any future changes are made to the payment process, the 'triggers' will need to be reconfigured, increasing reliance on your IT teams (internal or external). Until reconfiguration is complete, you will not meet the PCI compliance standards.
- This potentially costly option could limit your options for future business development. In fact, it isn't an option at all if you are an FSA regulated organisation as manual pausing of calls isn't compliant with their guidelines.

Option 4 - Single-location DTMF blocking

With this option, the customer enters the payment card details using their phone handset. The DTMF tones generated by the presses are detected and filtered out of the call recording system, so no card data ever reaches it. At the same time, the customer's card details are entered into the relevant fields on the Agent's screen. Options exist to obscure card data on screen, for increased security.

This method can be delivered on a customer's premises, or through a hosted/cloud service.

- Unlike the IVR option, this route ensures a live, uninterrupted call between customer and Agent.
- Some DTMF tones need to be let through (so the internal IVR will work, for example) and some blocked, so there are two distinct 'modes'. In order to switch modes, it's necessary to detect when the agent is about to take payment information. One option to change modes requires complex integration to 'map' between lines, extensions, agent desktop and payment applications. An alternative approach is for the call centre agent to enter a unique code into their telephone keypad, thus extending call handling time and introducing a further point for potential error.
- A concern with this solution is that it has a single point of failure. If the system falls over, all calls into the centre stop.

Option 5 - Dual-location DTMF blocking

Like Option 4, CallGuard accepts DTMF tones generated when the customer enters the card details via the phone handset. CallGuard automatically filters credit card details from call recordings, live, and stops agents seeing card data on screen.

CallGuard's technology comprises two separate hardware components – the Decoder and Filter.

- The CallGuard Filter is a hardware device which sits in line with your existing call recorder. It listens for customers' DTMF tones, and stops them from getting through to your recorder. Consequently, your call recordings will not contain any card data.
- The CallGuard Decoder automatically enters the customer's card details into the relevant fields on the Agent's screen, again disguised for security.
- Adding CallGuard DataShield software at your Agent desktop PCs enables you to completely isolate your agents from any customer card data. With DataShield, card data is obscured on screen with asterisks (or similar), eliminating the opportunity for card data theft.

CallGuard is a plug and play solution that works in any existing – or future - IT/telephony environment. Critically, there is no need to make any changes to your existing payment system, or payment provider, and consequently, there are no costly integration charges.

If, however, you choose to do so in the future, CallGuard will continue to work.

For more information

To see how CallGuard can make your call recorder PCI compliant, go to www.veritape.com/callguard or call +44 (0) 845 899 5500.

Veritape and PCI DSS

Veritape is a trusted voice on PCI DSS compliance issues. Veritape is the only call recording company accredited as a PCI DSS Participating Organisation.

PCI Security Standards Council™
PARTICIPATING ORGANIZATION

Veritape Ltd, Alkrington Hall, Alkrington, Manchester, M24 1WD, UK
Tel 0845 899 5500 Fax 0845 899 5511