Four ways to make call recordings PCI DSS compliant

PCI DSS is becoming an accepted regulatory necessity for businesses taking payments by phone and recording their calls. But differing interpretations of the guidelines are causing confusion to businesses seeking to become PCI DSS compliant. There is no single approved method for making call recordings compliant. In fact, there are several PCI DSS compliant methods, and you need to choose the best option for your business.

One of our core values is to make call recording technology accessible and easy to understand, and in our opinion, the confusion around PCI DSS is unnecessary. With the objective of informing instead of confusing, here is a reliable overview of which methods, when properly implemented, will make call recordings PCI DSS compliant:

These methods can work:

1. Pause and resume

The "pause and resume" method records the entire call apart from the sensitive authentication data. It is technically difficult to set up and tricky to maintain during future changes within your organisation.

2. Turn off your call recording

Literally, switch off your call recorder. You will lose all the benefits associated with call recording such as training, customer service and compliance. This method cannot be used by businesses operating in some regulated financial sectors.

3. Transfer to an IVR

Transfer calls to an automated payment card processing solutions such as an IVR. IVRs are not particular favourites with customers and they do require significant integration with back-end IT and telephony.

4. CallGuard

CallGuard automatically detects and blocks DTMF tones and therefore the payment card data from call recordings. Call recording continues as usual and no sensitive data is captured or stored in any format. It works with any call recording system.

Compare these methods in more detail here.

These methods don't work:

These methods are non-PCI DSS compliant:

- Manual pause and resume. The PCI DSS guidelines state that card data should be removed from calls automatically, not manually.
- Encryption only. The PCI DSS guidelines bar the storage of sensitive authentication data in any format, even if it has been encrypted.
- Use speech recognition for removal after the recording has been made. It is tricky to detect and remove payment information (essentially numbers) without compromising other parts of the recording. Ifsome of the payment information is missed, the recording is not PCI DSS compliant.