

Are audio/voice recordings containing cardholder data and/or sensitive authentication data included in the scope of the PCI DSS?

This response is for call centers that record cardholder data in audio recordings, and applies only to the storage of card validation codes and values (referred to as CAV2, CVC2, CVV2 or CID by the payment brands). This response is intended to provide clarification for call centers regarding their potential storage of card validation codes and values, and their compliance with the PCI DSS. It is a violation of PCI DSS requirement 3.2 to store any sensitive authentication data, including card validation codes and values, after transaction authorization. Call centers may find themselves in the position of receiving cardholder data which includes sensitive authentication data, and they may be unable to delete this sensitive data since individual elements cannot easily be deleted from an audio recording. To clarify, these call centers and all cardholder data are IN SCOPE for PCI DSS. However, if the storage of card validation codes and values meets the unique circumstances described in this response AND these values are protected according to all applicable PCI DSS requirements, those card validation codes and values may be stored. If commercially reasonable technology exists to delete these data elements, then these elements should be deleted. If the individual data elements within an audio file can never be queried, then only the physical and logical protections defined in PCI DSS version 1.1 must be applied to these audio files. Additionally, if these audio files that can never be queried are copied to magnetic tape media, that media must also be protected in accordance with PCI DSS. However, if card validation codes and values stored on audio files are subject to technology that allows for the capture and transposition of the speech/audio data into a format that can be queried (for example digital or other file formats), then the sensitive authentication data, including card validation codes and values, must not be stored and must be deleted immediately after authorization. Again, this response applies only to call centers and card validation codes and values. All other cardholder data captured by call centers must be protected in accordance with the PCI DSS, including PCI DSS requirement 3.4. In addition, this response does not apply to any other entity besides call centers, and all other entities must protect all cardholder data in accordance with PCI DSS, including requirements 3.2 and 3.4.