

# Are audio/voice recordings permitted to contain sensitive authentication data?

PCI SSC FAQ | Article 1210 | June 2025

---

PCI DSS Requirement 3.3.1 prohibits storage of sensitive authentication data (SAD), including card validation codes and values, after authorization even if the data is encrypted. Storage of card validation codes or values (referred to as CAV2, CVC2, CVV2 or CID) in any form of digital audio recording—for example, .wav or .mp3 files—after authorization is therefore a violation of this requirement.

If SAD is collected during a call, every effort must be made to prevent the data from being recorded. Where technology exists to suppress or redact audio during data entry, it should be enabled.

If it is not possible to prevent SAD from being recorded, the data should be securely deleted immediately upon authorization of the transaction. If secure deletion is not possible due to legitimate technical or business constraints, compensating controls should be implemented to mitigate the risk associated with storing the data. At a minimum, the compensating control process should include:

- Comprehensive risk assessments, annually and upon significant changes to the environment.
- Securing SAD in accordance with applicable PCI DSS requirements.
- Controls preventing SAD access and call recording queries
- Documentation of controls, detailed justifications, risk assessment results, and evidence of compliance

These controls are validated during annual PCI DSS assessments and shared with acquirers/payment brands as needed.

PCI DSS does not override local or regional audio retention laws. Refer to the Information Supplement: Protecting Telephone-Based Payment Card Data for further guidance.

Source: <https://www.pcisecuritystandards.org/faqs/1210/>