

For PCI DSS, can sensitive account data be stored before authorization?

PCI SSC FAQ | Article 1154 | July 2025

For PCI DSS, account data consists of cardholder data (CHD) and sensitive authentication data (SAD). With respect to SAD, PCI DSS Requirement 3.3.1 prohibits storage of SAD after authorization, even if encrypted. Note that there are no specific rules in PCI DSS regarding how long SAD can be stored before authorization, but such data would need to be protected according to PCI DSS. Use of PCI approved PTS devices and PCI-validated payment software can support PCI DSS compliance for the protection of data prior to authorization.

The individual payment brands determine whether SAD is permitted to be stored before authorization, including any related usage and protection requirements. Additionally, several payment brands have specific rules that prohibit any storage of SAD and do not make any exceptions. To determine payment brand requirements, please contact the individual payment brands directly. Contact information for the payment brands can be found in FAQ 1142 How do I contact the payment card brands?

(https://www.pcisecuritystandards.org/faq/articles/Frequently_Asked_Question/How-do-I-contact-the-payment-card-brands)

Source: <https://www.pcisecuritystandards.org/faqs/1154/>