

# **For PCI DSS, why is storage of sensitive authentication data (SAD) after authorization not permitted even when there are no primary account numbers (PANs) in an environment?**

PCI SSC FAQ | Article 1533 | July 2021

---

In the PCI DSS Applicability Information section of the standard, it is stated that sensitive authentication data must not be stored after authorization even if encrypted, and that this applies even for environments where there is no PAN present.

Sensitive authentication data (SAD) is used by the issuer of a card to authenticate the card and the cardholder, specifically the card verification code and the PIN/PIN block.

The card verification codes that are found in the track data, the track data equivalent in the chip or, for an e-commerce transaction, that are printed on the front or back of a payment card, are validated by the issuer during authorization to give them confidence that the card they issued is being used for the transaction.

The PIN or PIN block is validated by the issuer during authorization to give them confidence that the cardholder is making the transaction.

If an entity stores sensitive authentication data even where there is no PAN in the entity's environment, there is the risk that the SAD could be compromised by an attacker and subsequently correlated with other data to give an attacker the PAN and SAD together, which would reduce an issuer's ability to determine whether a transaction was genuine or fraudulent. For example, a customer is often identified by its email address; criminals may use correlation databases to correlate a PAN and email address stolen from one merchant with a card verification code and the same email address stolen from a second merchant.

Similarly, if a merchant stores a card verification code alongside a token that can be used to make a payment transaction, the merchant (or an attacker with access to the merchant's environment) is misrepresenting to the card issuer that the cardholder provided the card verification code during the transaction, limiting the issuer's ability to protect their cardholder from fraud. Transactions that use stored cardholder data with the cardholder's permission (referred to as account on file, card on file, and credential on file), including recurring transactions and additional charges in the travel industry, do not require the merchant to provide the card verification code. For more information on card-on-file or recurring transactions, see FAQ #1280 Can card verification codes/values be stored for card-on-file or recurring transactions?

Source: <https://www.pcisecuritystandards.org/faqs/1533/>