

# **If an organization provides software or functionality that runs on a consumer's device (for example, smartphones, tablets, or laptops) and is used to accept payment account data, can the organization store card verification codes for those consumers?**

PCI SSC FAQ | Article 1574 | October 2023

---

No. PCI DSS prohibits storage of card verification codes, for example, after transaction authorization or to facilitate potential future transactions.

There are four common scenarios where organizations may want to, or think it is necessary to, store card verification codes for consumers, due to software or functionality on a consumer's device:

- 

Applications that facilitate consumers' online purchases and where the merchant or service provider stores card verification codes for use on behalf of consumers. Examples include merchant online store applications, gaming applications, and web browsers for auto fill of payment transactions.

- 

Functionality where a service provider stores card verification codes on behalf of consumers, including password vaults.

- 

Issuing functions that provision a consumer's account data into a consumer's device (which may include card verification codes). Not the subject of this FAQ. Only issuers or companies supporting issuing services with a legitimate issuing business need may store SAD after transaction authorization.

- 

Consumers that enter their own payment account data into their device (which may include card verification codes). Not the subject of this FAQ. In this case, the device is treated similarly to a consumer's payment card.

This FAQ applies only to the first two bullets above.

Card verification codes are typically used for authorization in card-not-present transactions.— PCI DSS does not prohibit the collection of card verification codes prior to authorization of a specific purchase or transaction. However, it is not permitted to retain card verification codes once the specific purchase or transaction for which it was collected has been authorized.

It is not permissible to store card verification codes regardless of any permission the entity may have received from their customer to store the sensitive authentication data on their behalf. A customer's request or approval for an entity to retain a card verification code has no validity for PCI DSS and does not constitute an allowance to

store the data.

Generally, PCI DSS is intended for all entities that store, process, or transmit cardholder data (CHD) and/or sensitive authentication data (SAD) or could impact the security of the cardholder data environment (CDE). This includes all entities involved in payment card account processing—including merchants, processors, acquirers, issuers, and other service providers.

Note that whether such an entity is required to undergo a PCI DSS assessment is determined by organizations that manage compliance programs, such as acquirers (merchant banks), payment brands, or other entities. Entities should contact these organizations directly for information about any such requirements. Contact details for the payment brands can be found in FAQ #1142 'How do I contact the payment card brands'?

See also the following related FAQs:

FAQ 1280: Can card verification codes/values be stored for card-on-file or recurring transactions?

FAQ 1283: How do PCI standards apply to organizations that develop software that runs on a consumer's device (for example, a smartphone, tablet, or laptop) and is used to accept payment card data?

FAQ 1533: 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?

Source: <https://www.pcisecuritystandards.org/faqs/1574/>