

Can card verification codes be stored for card-on-file or recurring transactions?

PCI SSC FAQ | Article 1280 | October 2023

No. It is not permitted to retain card verification codes once the specific purchase or transaction for which it was collected has been authorized. 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.

A card verification code (also referred to as CAV2, CVC2, CVN2, CVV2, or CID, depending on the payment brand) is the 3- or 4- digit number printed on the front or back of a payment card. —These values are considered sensitive authentication data (SAD), which, in accordance with PCI DSS Requirement 3, cannot be stored after authorization*.

Card verification codes are not needed for card-on-file or recurring transactions (for example, for a recurring gym membership payment), and PCI DSS prohibits storage for these purposes. PCI DSS also prohibits storage of card validation codes for concierge-style services, where cardholder details are retained by an entity to facilitate potential future transactions on behalf of a consumer (for example, for making restaurant reservations or purchasing theatre tickets).

All card verification codes must be completely removed from the entity's systems to comply with Requirement 3. The requirement that prohibits retaining sensitive authentication data after authorization applies even if that data is encrypted. Any service or process that claims to "remove" card verification codes from storage, yet is able to retrieve them for future authorization, would need to be assessed (for example, by a QSA or ISA), to confirm that all card verification codes have been truly removed from the entity's systems and are not being stored in any way, shape, or form.

It should also be noted that 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.

Merchants and their service providers should contact organizations that manage compliance programs, such as their acquirer (merchant bank), the payment brands, or other entity directly, as applicable, for guidance on how to process recurring or card-on-file transactions without requiring transmission or storage of the card verification codes. 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 1574: 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?

FAQ1533: 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?

* Only issuers or those companies supporting issuing services with a legitimate issuing business need may store SAD after transaction authorization.

Source: <https://www.pcisecuritystandards.org/faqs/1280/>