

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?

PCI SSC FAQ | Article 1283 | October 2023

If the consumer is also the cardholder and is using the device solely for their own cardholder data entry, and the software is only used by that cardholder using his own credentials, then the device is treated similarly to a cardholder's payment card. The consumer's environment in which the software runs is not in scope for the organization's PCI DSS assessment.

Even though the consumer's environment is outside of the organization's PCI DSS scope, the development of the software is in scope, as the software is being developed for the purpose of facilitating a merchant's payment acceptance process. The software should therefore be developed in accordance with industry best practices and applicable PCI DSS requirements — for example, those included in Requirement 6. Additionally, if the software developer stores, processes, or transmits payment account data on the consumer's behalf, then PCI DSS will apply to the developer's environment.

It is recommended that software be developed using the Software Security Framework (SSF) standards (the Secure Software Standard and Secure SLC Standard) as a baseline for the protection of payment account data. Sources of industry guidance for developing mobile applications include ENISA and OWASP, as well as the PCI Mobile Payment Acceptance Security Guidelines for Developers.

For information about whether software that runs on a consumer's device is eligible for listing as Validated Payment Software according to the PCI Secure Software Standard, or whether the software vendors are eligible for listing as a Secure SLC-Qualified Vendor according to the PCI Secure SLC Standard, refer to the Secure Software Program Guide or the Secure SLC Program Guide, respectively, on the PCI SSC website.

Note that, while PCI DSS does not require the use of Validated Payment Software or a Secure SLC-Qualified Vendor, some payment brands may have specific requirements. Entities should contact organizations that manage compliance programs, such as their acquirer (merchant bank) the payment brands, or other entity 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 FAQ:

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?

