

Are digital images containing cardholder data and/or sensitive authentication data included in the scope of the PCI DSS?

PCI SSC FAQ | Article 1070 | August 2022

Yes, forms and images containing cardholder data are subject to PCI DSS. PCI DSS Requirement 3 requires that all cardholder data be rendered unreadable. It does not differentiate between how the data is stored or managed. PCI DSS requires that the image and/or paper form must be rendered unreadable (or protected with appropriate compensating controls). In addition, PCI DSS Requirement 3 prohibits the storage of sensitive authentication data after authorization. If the entity collects any sensitive authentication data, they must remove or obfuscate such data before they image it, not storing scanned images with prohibited data.

Note: The specific sub requirement number(s) and terminology may vary depending on the version of the standard being used.

Refer to the definition of "sensitive authentication data" in the applicable glossary for the version of the standard being used.

Source: <https://www.pcisecuritystandards.org/faqs/1070/>