

Does PCI DSS apply to bank account data?

PCI SSC FAQ | Article 1335 | June 2023

PCI DSS applies for the protection of cardholder data (primary account number (PAN), cardholder name, service code and expiration date) and sensitive authentication data (full track data from the magnetic stripe or equivalent data on the chip, CAV2/CVC2/CVV2/CID/CVN2, and PIN/PIN block), from a payment card representing a PCI SSC Participating Payment Brand (American Express, Discover, JCB, Mastercard, UnionPay, or Visa).

Bank account data, such as branch identification numbers, bank account numbers, sort codes, routing numbers, etc., are not considered payment card data, and PCI DSS does not apply to this information. However, if a bank account number is also a PAN or contains the PAN, then PCI DSS applies.

It should also be noted that some bank account numbers may contain PAN digits. If the number of included PAN digits is in excess of the truncation formats defined by the particular payment brand (see FAQ 1091), then PCI DSS applies.

Even if PCI DSS does not apply to a particular account number containing elements of PAN, it is strongly recommended that the account number be protected to avoid unauthorized persons from being able to derive the full PAN from the account number.

Refer to FAQ 1091 for more information on truncation formats: What are acceptable formats for truncation of primary account numbers?

Source: <https://www.pcisecuritystandards.org/faqs/1335/>