

How can an entity meet PCI DSS requirements for PAN masking and truncation if it has migrated to 8-digit BINs?

PCI SSC FAQ | Article 1492 | April 2024

There are two PCI DSS requirements that may be affected when considering 8-digit BINs.

Requirement 3.4.1 pertains to masking (concealing) digits of the PAN so that the full PAN is not displayed, and Requirement 3.5.1 is for rendering PAN unreadable when stored. These requirements are different and distinct and therefore it is important to understand each requirement and how it pertains to the entity's implementation.

PCI DSS Requirement 3.4.1 requires that no more than the BIN and last four digits of the PAN are displayed on computer screens, reports, etc. unless there is a documented business justification for seeing more digits. The documented business justification should explain why that person (or role) needs to see more digits of PAN, be approved by management, and available for an assessor to review as part of the PCI DSS assessment.

PCI DSS Requirement 3.5.1 applies when PAN is stored (i.e., data at rest). This requirement specifies four acceptable methods for rendering PAN unreadable when stored. One of the techniques is truncation, which permanently removes the middle digits of the PAN, leaving the rest of the PAN to be stored in the clear. FAQ #1091 What are acceptable formats for truncation of primary account numbers? (https://www.pcisecuritystandards.org/faq/articles/Frequently_Asked_Question/What-a-re-acceptable-formats-for-truncation-of-primary-account-numbers) provides information about acceptable truncation formats for each payment brand based on the length of PAN/BIN. Because each payment brand has different PAN/BIN lengths and different requirements, questions about payment brand truncation requirements should be directed to the applicable payment brands. Contact details for the payment brands are provided in FAQ #1142 How do I contact the payment card brands? (https://www.pcisecuritystandards.org/faq/articles/Frequently_Asked_Question/How-d-o-I-contact-the-payment-card-brands)

Please note that truncation is only one acceptable method for rendering PAN unreadable during storage; other options include encrypting the entire PAN, using index tokens, or using one-way hashes. All hashes generated after 31 March 2025 must be keyed cryptographic hashes according to PCI DSS Requirement 3.5.1.1.

Source: <https://www.pcisecuritystandards.org/faqs/1492/>