

Are truncated Primary Account Numbers (PAN) required to be protected in accordance with PCI DSS?

PCI SSC FAQ | Article 1117 | September 2021

Systems that store, process, or transmit only truncated PANs (where a segment of PAN data has been permanently removed) may be considered out of scope for PCI DSS if those systems are adequately segmented from the cardholder data environment, and do not otherwise store, process, or transmit cardholder data or sensitive authentication data. This applies to any truncation that meets the acceptable PAN truncation formats specified in FAQ 1091.

However, the system performing the truncation of the PANs, as well as any connected systems and networks, would be in scope for PCI DSS.

Some entities use solutions that combine truncation with tokenization or encryption to create format-preserving values that can be passed through legacy payment systems. For example, the BIN and the last four digits of the PAN are retained in accordance with FAQ 1091 while the remaining digits are replaced with values generated via a tokenization or encryption operation. Whether such format-preserving values may be considered out of scope for PCI DSS is dependent on a variety of factors and can only be determined in respect of an entity's specific implementation by an Assessor. However, the systems performing encryption or tokenization of the PAN segment and those performing key management for the encrypted or tokenized PANs would be in scope for PCI DSS.

For solutions that combine truncation with tokenization or encryption, factors that indicate the resulting truncation result would be in scope for PCI DSS, include, but are not limited to the following:

-

The tokenization or encryption of the PAN segment can be reversed in the environment in which the segment resides.

-

The encrypted or tokenized PAN segment is not isolated from related key management processes.

-

The encrypted or tokenized PAN segment is present on a system or media that also contains the decryption key.

-

The encrypted or tokenized PAN segment is present in the same environment as the decryption key.

-

The encrypted or tokenized PAN segment is accessible to an entity that also has access to the decryption key.

Note that access to different truncation formats of the same PAN greatly increases the ability to reconstruct full PAN, and the security value provided by an individual truncated PAN is significantly reduced. If the same PAN is truncated using more than one truncation format (for example, different truncation formats are used on different systems), additional controls should be in place to ensure that the truncated versions cannot be correlated to reconstruct additional digits of the original PAN. To consider the truncated PAN out of scope, the additional controls must be verified to confirm that correlation is not possible, and that the different truncation formats do not result in more than the maximum allowable digits being present in the environment. If a PAN is truncated using different truncation formats, and this results in more than the allowable number of PAN digits being present in an environment, then that environment would be in scope for PCI DSS.

See also the following FAQs:

FAQ 1091: What are acceptable formats for truncation of primary account numbers?

FAQ 1146: What is the difference between masking and truncation?

Source: <https://www.pcisecuritystandards.org/faqs/1117/>