

How can hashing be used to protect Primary Account Numbers (PAN) and in what circumstances can hashed PANs be considered out of scope for PCI DSS?

PCI SSC FAQ | Article 1089 | March 2026

One-way hashing is a method that can be used to render PAN unreadable in storage. The hashing process and results, as well as the system(s) that perform the hashing, are in scope for a PCI DSS assessment to assure that the process meets applicable PCI DSS requirements.

If the hashing result is transferred and stored within a separate environment, the hashed PAN in that separate environment would no longer be considered cardholder data and would be out of scope for additional PCI DSS requirements. However, if the hashed PAN is stored on the same system or in the same environment that performed the hashing, that system or environment is considered to be storing cardholder data and remains within PCI DSS scope.

PCI DSS requires that hashing be of the entire PAN and be based on strong cryptography. This means that collisions would not occur frequently, and the PAN cannot be recovered or easily determined during an attack. Additionally, PCI DSS v4.x includes Requirement 3.5.1.1 to use keyed cryptographic hashing for hashes used to render PAN unreadable.

Since hashing is used when there is no need to recover the PAN, a recommended practice is to remove the PAN rather than allowing the possibility of a compromise cracking the hash and revealing the original PAN. If the entity intends to recover and use the PAN, then hashing is not an option and an alternative method for rendering the PAN unreadable should be considered.

Source: <https://www.pcisecuritystandards.org/faqs/1089/>