

Does PCI DSS apply to "hot cards," expired, cancelled or invalid payment account numbers?

PCI SSC FAQ | Article 1038 | December 2022

PCI DSS applies to any primary account number (PAN), including active, expired, or cancelled PAN, except where the organization can provide documentation which confirms that the PAN is inactive or otherwise disabled and no longer poses a fraud risk to the payment system. However, if the PAN is later reactivated, PCI DSS will again apply.

When payment account numbers expire, the same account number is often reused on the new card with a different expiry date. The PAN must therefore be verified as not being valid before expired payment account numbers are excluded from PCI DSS scope.

Entities should retain PAN based on business/legal needs, as defined in their data retention policy (PCI DSS Requirement 3). Remember: If you don't need it, don't store it.

Source: <https://www.pcisecuritystandards.org/faqs/1038/>