

Does PCI DSS allow faxing of payment card numbers?

PCI SSC FAQ | Article 1139 | August 2025

Any cardholder data that is stored, processed, or transmitted must be protected in accordance with PCI DSS. If faxes are sent or received via modem over a traditional PSTN phone line, these are not considered to be traversing a public network. On the other hand, if a fax is sent or received via the Internet, it is traversing a public network and must be encrypted per PCI DSS Requirement 4.2.1. Any systems, such as fax servers or workstations, that cardholder data passes through must be secured according to PCI DSS. Additionally, any cardholder data on the fax that is stored electronically must be rendered unreadable in accordance with PCI DSS Requirement 3.5.1. If the fax system is combined with an email system (for example, via a fax-to-email gateway), any emails would also be subject to Requirement 4.2.2.

Furthermore, Requirement 3.3 prohibits the storage of sensitive authentication data (full track, card verification codes/values, and PIN block data) after authorization. If sensitive authentication data is received on a fax (for fax transmissions this would only be the 3- or 4- digit card verification codes/values printed on the front or back of payment cards), the data should be blacked-out or removed prior to retaining the fax in paper form. The original fax transmission should be securely deleted from the system in a manner which ensures the data is non-recoverable. Entities should also protect paper documents that contain cardholder data in accordance with PCI DSS Requirements 9.4.

Also refer to the following FAQ:

FAQ 1085: Can unencrypted PANs be sent over e-mail, instant messaging, SMS, or chat?

(https://www.pcisecuritystandards.org/faq/articles/Frequently_Asked_Question/can-un-encrypted-pans-be-sent-over-e-mail-instant-messaging-sms-or-chat/)

Source: <https://www.pcisecuritystandards.org/faqs/1139/>