

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

PCI SSC FAQ | Article 1085 | August 2025

---

No. PCI DSS Requirement 4.2.2. prohibits the sending of unprotected primary account numbers (PANs) via end-user messaging technologies, whether sent internally or over public networks. E-mail, instant messaging, SMS, and chat are all considered end-user messaging technologies and thus required to meet PCI DSS Requirement 4.2.2. Per PCI DSS Requirement 4.2.1, strong cryptography and security protocols must be used when cardholder data is sent over open, public networks.

Also refer to the following FAQs:

FAQ 1310: Are entities allowed to request that cardholder data be provided over end-user messaging technologies?  
([https://www.pcisecuritystandards.org/faq/articles/Frequently\\_Asked\\_Question/are-entities-allowed-to-request-that-cardholder-data-be-provided-over-end-user-messaging-technologies/](https://www.pcisecuritystandards.org/faq/articles/Frequently_Asked_Question/are-entities-allowed-to-request-that-cardholder-data-be-provided-over-end-user-messaging-technologies/))

FAQ #1157: What should a merchant do if cardholder data is accidentally received via an unintended channel?  
([https://www.pcisecuritystandards.org/faq/articles/Frequently\\_Asked\\_Question/what-should-a-merchant-do-if-cardholder-data-is-accidentally-received-via-an-unintended-channel/](https://www.pcisecuritystandards.org/faq/articles/Frequently_Asked_Question/what-should-a-merchant-do-if-cardholder-data-is-accidentally-received-via-an-unintended-channel/))

Source: <https://www.pcisecuritystandards.org/faqs/1085/>