

How does PCI DSS apply to VoIP?

PCI SSC FAQ | Article 1153 | October 2012

PCI DSS requirements apply wherever payment card account data is stored, processed, or transmitted. While PCI DSS does not explicitly reference the use of VoIP, VoIP traffic that contains payment card account data is in scope for applicable PCI DSS controls, just as other IP network traffic containing payment card account data would be.

VoIP transmissions originating from an external source and sent to an entity's environment are not considered within the entity's PCI DSS scope until the traffic reaches the entity's infrastructure. This is because an entity cannot control the method of inbound phone calls that their customers and other parties may make, including whether any payment card account data sent over that transmission is being adequately protected by the caller.

An entity is considered to have control over the transmission, storage and processing of VoIP traffic within their own network and up to the external perimeter of their infrastructure. The following guidance is intended to assist with PCI DSS scoping for VoIP in different scenarios.

Internal transmissions: VoIP traffic containing payment card account data is in scope for applicable PCI DSS controls wherever that traffic is stored, processed or transmitted internally over an entity's network.

External transmissions to other business entities (business-to-business): Where an entity uses VoIP for transmission of payment card account data to another business—for example, a service provider or payment processor—the entity's systems and networks used for those transmissions are in scope. Where an entity has end-to-end control over the VoIP connection, the transmission is also in scope for applicable PCI DSS controls. Where an entity cannot control the entire connection—for example, where the transmission passes through multiple telephone carriers between the two entities—the VoIP transmission is within the entity's scope only while the transmission is under control of the entity's infrastructure. This is because the entity does not control how the VoIP traffic will be routed outside of the entity's infrastructure or if all the telephone carriers can support secure connections.

External transmissions to/from cardholders: Where VoIP is used for transmissions of payment card account data between a cardholder and an entity, the entity's systems and networks used for those transmissions are in scope. Securing the VoIP transmission outside of the entity's infrastructure is not considered within the entity's scope, as the entity cannot control the methods used by the cardholder to make and receive phone calls. This applies regardless of whether the transmissions are initiated by the entity or the cardholder.

PCI SSC has published an Information Supplement titled "Protecting Telephone-Based Payment Card Data", which provides additional guidance for protecting payment card account data that is received via voice communications. This Information Supplement

is available for download from the Guidance Documents section in the PCI SSC Document Library.

Source: <https://www.pcisecuritystandards.org/faqs/1153/>