

# What should a merchant do if cardholder data is accidentally received via an unintended channel?

PCI SSC FAQ | Article 1157 | October 2012

---

Merchants sometimes find themselves in a situation where a customer provides their cardholder data unsolicited via an insecure communication channel that was not intended for the purpose of capturing sensitive data.

In this situation, the merchant can choose to either include the channel into the scope of their cardholder data environment (CDE) and secure it according to PCI DSS, or implement measures to prevent the channel from being used for cardholder data.

Some suggestions for merchants to prevent any further capture of cardholder data via unsecured methods include:

- Implementing controls to prevent acceptance of cardholder data via unsecured channels
- Responding to customers in a manner which does not propagate any further unsecured transmissions of cardholder data
- Implementing best practices and customer communications to proactively prevent customer use of unsecured channels for cardholder data

Cardholder data received via an unintended channel should be either immediately removed or secured according to PCI DSS and incorporated into the merchant's CDE. If a merchant does not wish to bring a communication channel and its supporting systems into the scope of their CDE, controls should be in place to prevent the capture of cardholder data and/or to securely delete cardholder data from this channel before the data can be further stored, processed or transmitted.

If unsolicited cardholder data is received via an insecure method, the merchant should take immediate steps to minimize the security impact and prevent further exposure of that data. For example, if a merchant receives cardholder data in an email from a customer, the merchant's personnel should be trained to not 'reply' using the same email that contains the cardholder data. Instead, the merchant's personnel should respond in a manner that does not further propagate the unsecured transmission of cardholder data. This may be accomplished by removing all sensitive data from the email response before replying or by contacting the customer via an alternative communication channel to complete the transaction.

Merchants are encouraged to communicate with their customers on the risks of sending cardholder data through insecure channels, and to ensure their customers are aware of the merchant's secure methods for submitting payment information. By proactively encouraging their customers to use only secure payment methods, merchants can reduce the amount of cardholder data received via unsolicited or insecure channels.