worldpay

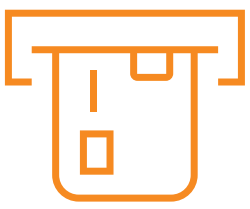
Tokenization and encryption

Two key components of card data security

Encryption

Protects sensitive payment data by transforming it into a non-readable code that requires an encryption key to decipher. Encryption is designed to prevent hackers from stealing cardholder data "in transit," such as from the POS to the payment processor.

Customer uses their card to make a purchase

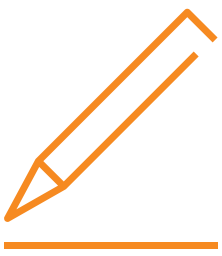


Card information is encrypted at the point of entry and sent to Worldpay's secure data center

Encrypted data is meaningless to hackers

Tokenization

Protects sensitive payment data by replacing it with a unique "token" that has no intrinsic value and is worthless if stolen. Tokenization is designed to protect cardholder data "at rest" that is stored for future transactions.



Tokens can also be used for transaction reporting and analysis

Tokens can be used for recurring billing, tip adjustment, and other secure post-authorization transactions

Card information is replaced with a token at Worldpay's secure data center, which is returned to the merchant

WIP146 11.18