PCI Payment Terms Explained

SOURCE: PCI SECURITY STANDARDS COUNCIL
Payment Terms

Definitions

WHAT DO THESE TERMS MEAN?

A PAYMENT TERMINAL is the device used to take customer card payments via swipe, dip, insert, tap, or manual entry of the card number. Point-of-sale (or POS) terminal, credit card machine, PDQ terminal, or EMV/Chip-enabled terminal are also names used to describe these devices.

An ELECTRONIC CASH REGISTER (or till) registers and calculates transactions, and may print out receipts, but it does not accept customer card payments.

An INTEGRATED PAYMENT TERMINAL is a payment terminal and electronic cash register in one, meaning it takes payments, registers and calculates transactions, and prints receipts.

A MERCHANT BANK is a bank or financial institution that processes credit and/or debit card payments on behalf of merchants. Acquirer, acquiring bank, and card or payment processor are also terms for this entity.

ENCRYPTION is a process that cryptographically protects data via a mathematical formula that renders the data unreadable to people without special knowledge (called a key). Cryptography can be applied to stored data as well as data transmitted over a network. While your payment terminal may encrypt card data, unless it is part of a PCI-listed P2PE solution, you don't know the quality of that encryption. With a PCI-listed P2PE solution, card data is always entered directly into a PCI-approved payment terminal with secure reading and exchange of data (SRED) enabled. This approach minimizes exposure of clear-text card data, and protects merchants against payment terminal exploits such as "memory scraping" malware. Any encryption that is not done within a PCI-listed P2PE should be discussed with your vendor.

A PAYMENT SYSTEM encompasses the entire process for accepting card payments in a retail location, and may include a payment terminal, an electronic cash register, other devices or systems connected to a payment terminal (for example, Wi-Fi for connectivity or a PC used for inventory), and the connections out to a merchant bank.

https://www.pcisecuritystandards.org/pci_security/small_merchant_tool/payment-terms-explained.html
Dial-up payment terminal

Type 1

Payments sent via phone line.

https://www.pcisecuritystandards.org/pci_security/small_merchant_tool/type-1.html
Dial-up payment terminal and internet-connected electronic cash register

Type 2
Payments sent via phone line.

https://www.pcisecuritystandards.org/pci_security/small_merchant_tool/type-2.html
Payment terminal and electronic cash register separately connected to the internet

Type 3
Payments sent via internet by payment terminal.

Payment terminal and electronic cash register share non-card data

Type 4

Payments sent via internet by payment terminal.

https://www.pcisecuritystandards.org/pci_security/small_merchant_tool/type-4.html
Payment terminal connected to electronic cash register

Type 5

Payments sent via internet by electronic cash register.

Integrated payment terminal and payment middleware share card data

**Type 6**

Payments sent via internet.

Payment terminal and electronic cash register combined
Card is swiped by a staff member; diagram is not applicable for chip cards
No separate PIN entry device
No other equipment connected to merchant payment system

Encrypting card data reduces your risk. If your payment terminal encrypts card data, ask your terminal vendor how (e.g., does it use PCI’s Secure Reading and Exchange of Data (SRED) to encrypt).

Wireless payment terminal ("pay-at-table") with integrated payment terminal and payment middleware

Type 7

Payments sent via internet.

Payment terminal connects to electronic cash register with additional connected equipment

Type 8

Payments sent via internet.

E-commerce merchant with fully outsourced payment page/form

Type 9

Payments sent by PCI DSS compliant third-party service provider.

E-commerce merchant fully or partially presents payment to customers

Type 10

Payments sent from customer browser direct to PCI DSS compliant third-party service provider.

https://www.pcisecuritystandards.org/pci_security/small_merchant_tool/type-10.html
E-commerce merchant accepts card data using payment page presented to customers from own website.

Type 11 Payments sent via the merchant website.

PCI-listed encrypting secure card reader and mobile payment terminal

Type 12

Payments sent via cellular network only.

PCI-listed encrypting secure card reader and mobile payment terminal

Type 13

Payments sent via cellular network or Wi-Fi.

Virtual payment terminal accessed via merchant internet browser

Type 14

Payments sent via internet.

A "virtual terminal" is a web page accessed by the merchant, for example, with a computer or a tablet. Merchant manually enters card data via their web browser into the virtual terminal.

For merchants without a traditional payment terminal. They manually enter transactions one at a time and usually have low payment transaction volume (for example, those doing sales from home).

Note that there is greater risk if mobile payment acceptance is done over unprotected public Wi-Fi since criminals can steal your card data via that unsecured network.

Payment terminal encrypts card data via a PCI-listed Point to Point encryption solution

Type 15 Payments sent to PCI-listed P2PE Solution Provider.