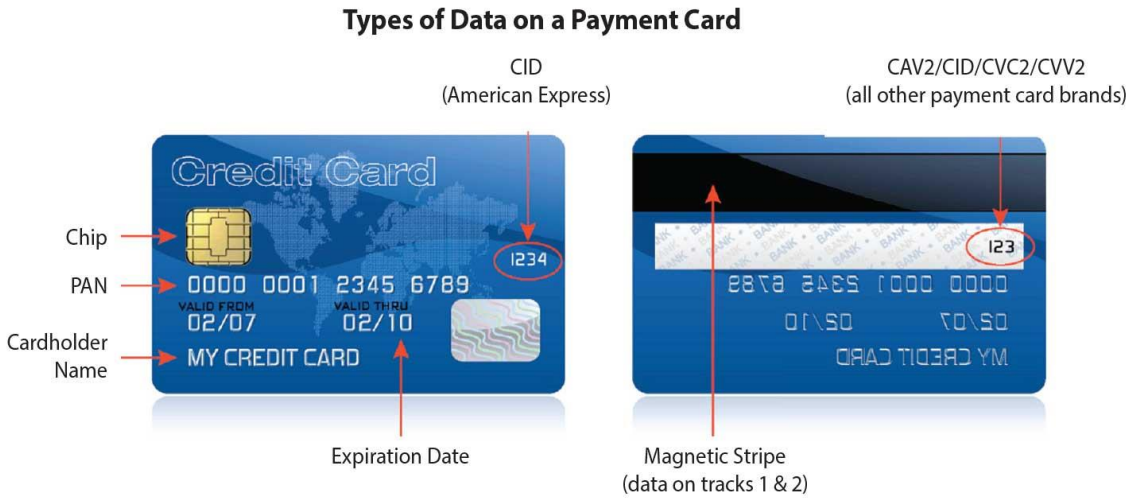
What data thieves are after

Cybercriminals are always chasing cardholder information. When they retrieve the Primary Account Number (most commonly known as card number) or other sensitive data, they can actually manage to impersonate the cardholder, use his card and steal the identity of the person.

As you can see below, all the information at the end of the red arrows is sensitive, meaning it is vulnerable to be stolen and the merchant must absolutely take all necessary steps to protect this data.



Source: [PCI Security Standards Council]

Where thieves steal

Sensitive cardholder data can be stolen from many places:

- Compromised card reader.
- Paper records stored in a filing cabinet.
- Data in a payment system database.
- Hidden camera recording entry of authentication data such as PIN at an ATM or a Point Of Sale merchant terminal.
- Secretly tap into your agency's wireless or wired network.

What needs to be secure

It is essential to not store any cardholder data in the below list of systems, card reading terminals and filing systems:

- Point Of Sale terminals and their card readers (magnetic stripe of chip).
- An Agent’s Branch networks & wireless access routers.
- Data storage and transmission.
- Paper-based records.
- Online payment applications and shopping carts.