What information needs to be protected?

- Not all information related to a credit card transaction need to be protected.
- There is cardholder data and payment data.
- Payment data should be kept for auditing purposes.
- Cardholder data should not be stored.

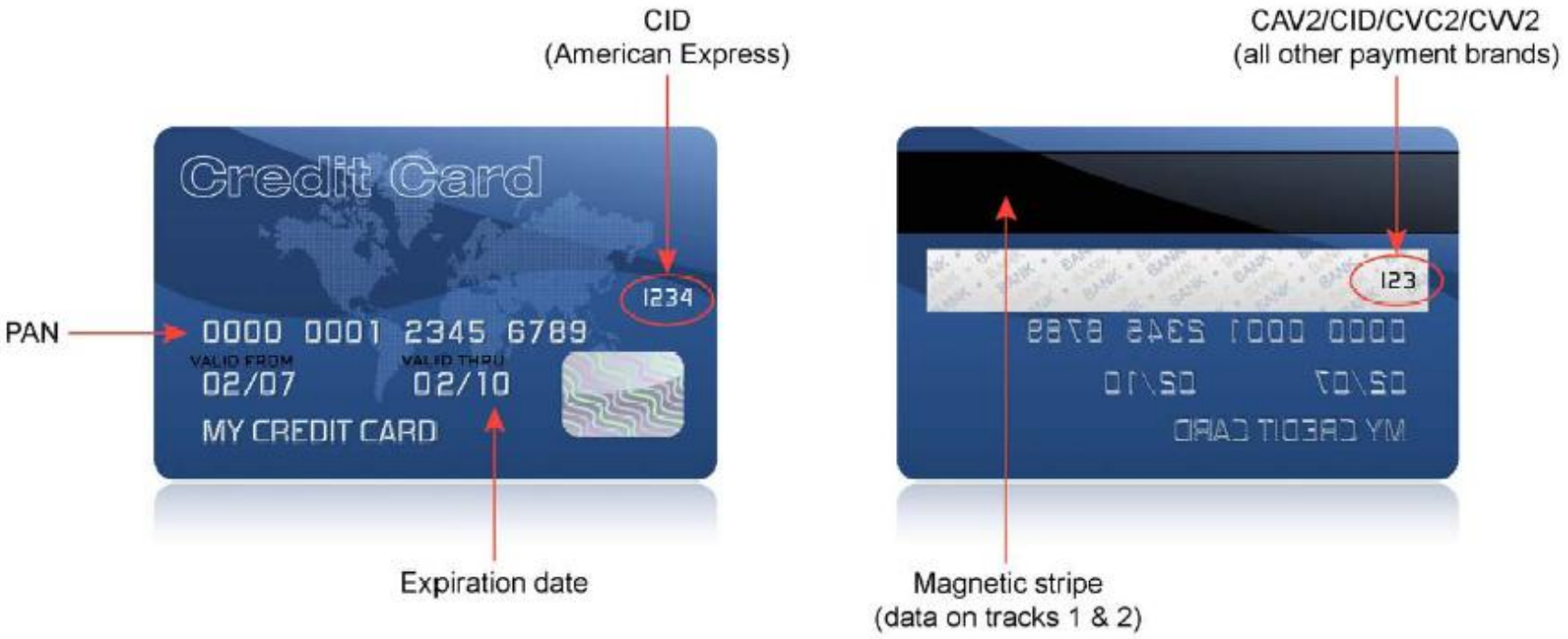
Cardholder Data vs Payment Data

- Payment data includes
  - Cardholder name
  - Transaction date
  - Last 4 Digits of credit card number
  - Authorization code
  - Card type
  - Amount

This information should be stored for 3 years per the record retention schedule.

Cardholder Data vs Payment Data

Cardholder Data – Should NOT be stored.



CVV2 – 3 or 4 digit code

NEVER store CVV2 data (3 or 4 digit code found on the back of a card)

- If you have this stored somewhere – DESTROY IT.
- If it is stored in old records, you need to go back and DESTORY IT.

In the event of a compromise, if you have this information, the severity of the compromise greatly increases.

*If your terminal asks for this code and you would rather not be responsible for it, let me know and we can have your terminal reprogrammed to not ask for this code.

Cardholder Data vs Payment Data

- Cardholder data – You do not need it, SO DON'T STORE IT.

- Misconception - I need to keep the credit card number.
  - Process refund – There are other ways to do this.
    - Ask the cardholder for their card number.
    - You can get the credit card number off of the processorsonline reporting website.
    - If you are using an approved service providers website, you do not need to cardholder data to process a refund.
    - You can call the processors helpdesk for assistance.
  - Any other reasons you need cardholder data?

*Think about whether the storage of cardholder data and the business purpose it supports are worth the risk of having data compromised.

Cardholder Data

Take inventory of all the places you store cardholder data and **destroy it** especially if you have the CVV2 (3 or 4 digit code).