Data Security Standards for PayPort Clerks

Overview

American Express, Discover, MasterCard and VISA developed Payment Card Industry Data Security Standards (PCI-DSS) to reduce security vulnerabilities and help protect cardholder data.

As someone who takes credit/debit card payments over the counter or phone, you are responsible for protecting cardholder data. This document explains what cardholder data is and how to protect it under your control.

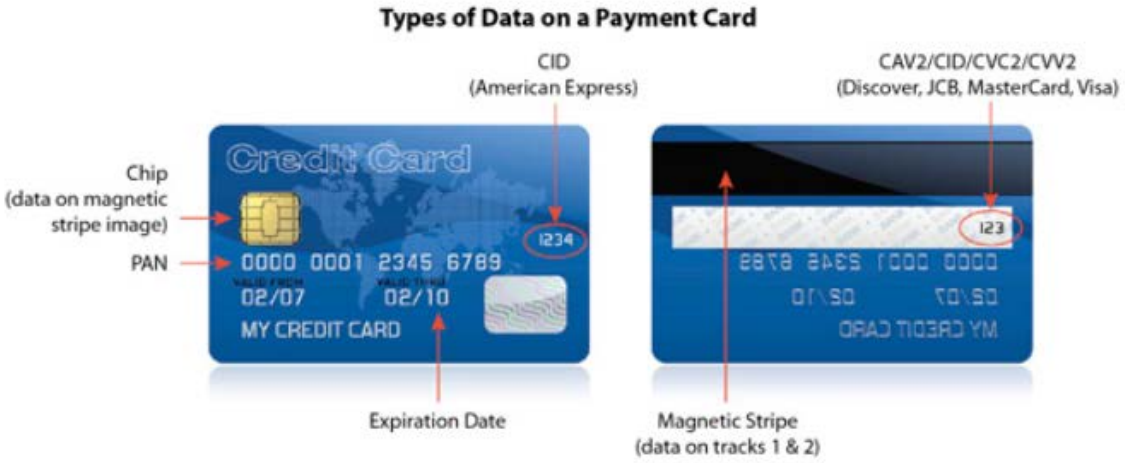
What Thieves Want

The object of desire is cardholder data. By obtaining the Primary Account Number (PAN) and sensitive authentication data, a thief can impersonate the cardholder, use the card, and steal the cardholder's identity.

Sensitive cardholder data can be stolen from many places, including:

- Compromised swipe card readers
- Documents stored in a filing cabinet
- Data in a payment system database
- Hidden camera (phone) recording entry of authentication data
- Secret tap into your wireless or wired network
- Employee fraud through collecting card holder data (skimming, writing, picture taking, etc.)

Key information highlighted by the red arrows below is targeted by criminals and must never be stored/copied/recorded.



Quick steps to security!

- Never store any sensitive cardholder data (on computers, paper, etc.). If a customer faxes, calls or mails in card data, securely destroy the data as soon as possible.
- Use a firewall on your network and PCs.
- Make sure your wireless router is password-protected and uses encryption.
- Use “strong” passwords. Be sure to change default passwords on hardware and software—most are unsafe!
- Regularly check computers for rogue software or “skimming” devices.
- Create an office culture of protecting cardholder data.

Questions?

Contact Rich Steckler or Leslie Vitagliano at Access Idaho: Boise area—332-0102, or toll free—1-877-443-3468.

5/2015