Training Bulletin Guidance—
Payment Cards and Your Employees

Trainer Notes

This bulletin raises awareness about handling payment card data and the PCI DSS. The Payment Card Industry Data Security Standard is a data protection standard developed by the Payment Card Industry for all businesses who handle payment card information. If your organization accepts or processes payment cards, your organization must comply with PCI DSS!

Noncompliance fees range from $5,000 to $100,000 every month until compliance issues are addressed. Even if you are compliant but experience a data breach, you can still be fined up to about $100 per cardholder whose data was compromised. That quickly adds up!

Talking Points

- Remind employees that cybersecurity is a team effort. Every employee counts, and participation is needed to maintain a good security posture.
- Hackers want your payment card data because they can sell it on the black market.
- Cardholder data should be secured from where it is captured at the point of sale and as it flows into the payment system. The best step is to not store any cardholder data!
- Remind employees that PCI DSS compliance is important, and that protecting payment card data should be a top priority in your cybersecurity program.

CYBERSECURITY TRAINING BULLETIN

Payment Card Guidance for Employees

What is PCI DSS?

The **P**ayment **C**ard **I**ndustry **D**ata **S**ecurity **S**tandard is a data protection standard developed by the Payment Card Industry for businesses who handle payment card information. If your organization accepts or processes payment cards, your organization must comply with PCI DSS.

What steps can I take to maintain PCI DSS compliance?

- Where possible, try to limit payment card transactions to in-person “swipe” purchases using validated payment card processing equipment.
- If you take cardholder data over the phone, type the number directly into your point-of-sale (POS) system. Do not repeat the information if you could be overheard.
- Generally, refrain from writing cardholder data on paper. If you must, then:
  - protect the written information from unauthorized disclosure;
  - process the transaction as soon as possible; and
  - render the information unusable - destroy it in a shredder or use a permanent marker to black-out sensitive information.
- Never use cardholder data in email transactions.
- Do not allow unknown people to inspect, configure, repair or replace your POS equipment or computers.
- Inspect your POS equipment regularly for signs of tampering.
- Immediately report signs of potential POS compromise.

What are signs of potential POS compromise?

- New, unidentifiable equipment in POS area
- Open filing cabinet/drawer/safe used to store CHD
- Unusual/Unexplained transactions
- Lost keys or codes

Where can I learn more about PCI DSS?

Your organization should have policies, procedures and training that provide greater detail into expected practices.

The official website for PCI DSS is: http://www.pcisecuritystandards.org/

Remember, YOU are the first line of defense against payment card fraud!