PCI Compliance FAQ

If you accept credit cards as payment you should be aware of PCI compliance and how it affects your business.

What is PCI Compliance?

The Payment Card Industry Data Security Standard (PCI DSS) is a set of security standards designed to ensure that ALL companies that accept, process, store or transmit credit card information maintain a secure environment.

What is PCI Compliance?

The Payment Card Industry Data Security Standard (PCI DSS) is a set of security standards designed to ensure that ALL companies that accept, process, store or transmit credit card information maintain a secure environment.

What is defined as Cardholder Data?

What is PCI Compliance?

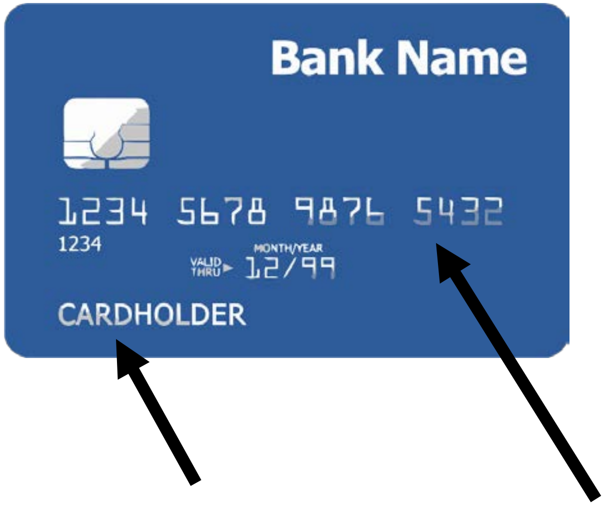
The Payment Card Industry Data Security Standard (PCI DSS) is a set of security standards designed to ensure that ALL companies that accept, process, store or transmit credit card information maintain a secure environment.

What is defined as Cardholder Data?

The PCI Security Standards Council (SSC) defines “cardholder data” as the full Primary Account Number (PAN) or the full PAN along with any of the following elements:

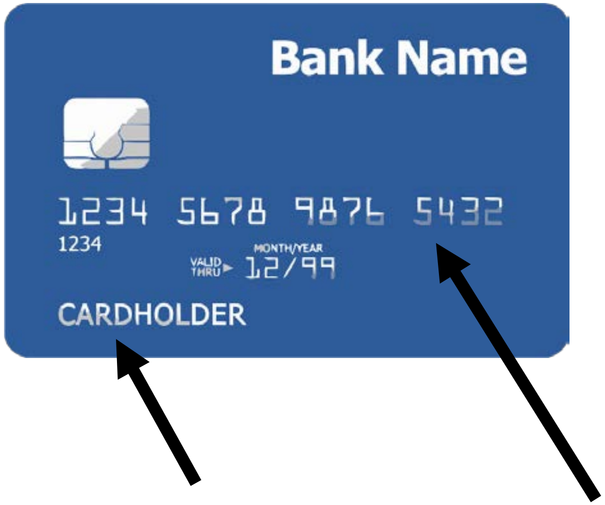
Cardholder Name
Expiration Date
Service Code (CVV or CVC)

Cardholder information to protect

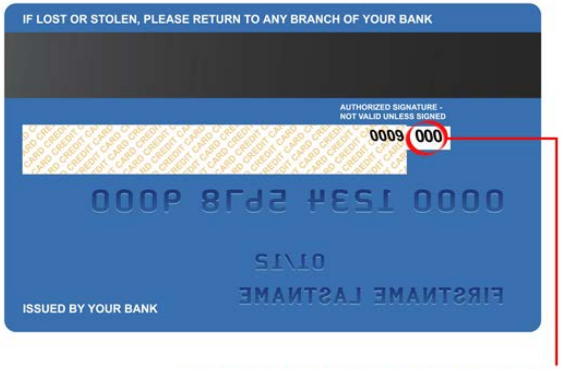


Cardholder Name and Number

Cardholder information to protect



Cardholder Name and Number


IF LOST OR STOLEN, PLEASE RETURN TO ANY BRANCH OF YOUR BANK
AUTHORIZED SIGNATURE - NOT VALID UNLESS SIGNED
0009
000
ISSUED BY YOUR BANK

On your card you can find your **CVV/CVC** code here.

Never share or copy any cardholder information!

How do I know if I am PCI compliant?

If you have concerns about your PCI compliance ask your current processing provider the following questions:

- Does your gateway provider have a PCI Approved Scanning Vendor (ASV) conduct quarterly scans of their system?
- Does your current provider have a certificate to authenticate their PCI Compliance? And to what level are they compliant?
- Does my provider require me to fill out a Self Assessment Questionnaire (SAQ) to validate my compliance?

Simple Do’s and Don’ts of PCI Compliance

PCI compliance is essentially many common sense practices. Listed are a few key things you should do and also not do to ensure you are compliant with PCI’s standards.

PCI compliance: DO's

- Change the default password on your county computer to a complex password.
- Supervise all visitors & personnel in areas where credit card information is stored.
- Ensure all cardholder data is unreadable, no matter where it is stored electronically.
- Cross-cut shred handwritten credit card information immediately after use.
- Store documents or media with credit card information in a locked drawer of a filing cabinet accessible only by authorized personnel.
- Report immediately to your customer and processing provider if you suspect credit card information has been lost, stolen, exposed, or otherwise misused.
- Make sure your processing company has a quarterly scan report, completed by an Approved Scanning Vendor (also called an ASV).
- Maintain a copy of PCI compliance policies and procedures for any clerk accepting credit card payments.

DON'T

- **NEVER** physically write down any credit card information unless you are explicitly required to do so as part of your business processes.
- **NEVER** acquire or disclose any cardholder's credit card information without the cardholder's consent, including but not limited to:

  The partial sixteen (16) digit card number
  The CVV/CVC (3 or 4 digit code on back)
  The PIN (personal identification number)

- **NEVER** store any sensitive authentication data on a county computer, server, or on paper, including:

  The card's storage chip or magnetic stripe
  The CVV/CVC code on the back of the card

- **NEVER** use an imprint machine to process credit card payments
- **NEVER** leave unsettled batches in terminals at the end of a business day. Ask your processing provider about auto-settle programming.
- **NEVER** share the password to your computer or any computer you access.
- **NEVER** leave sensitive information unattended on any desk, screen, or in any public area.

Other Points to Consider

- Establish a training session with your departments regarding the safety and security of cardholder data.

- Develop internal procedures on how credit card data should be handled.

- Check any credit card equipment to see if it has been tampered with or if anything has been added to the connected equipment

Questions:

Cathy Lunsford, Midland County Treasurer
clunsford@co.midland.mi.us

Or Graphite Municipalities (who helped provide this information)

Ray Dolman ray@graphitepayments.com
586-246-9598

Rich Carlisi rich@graphitepayments.com
586-746-7219