This document is intended to provide simple and quick information security steps for small to mid-size merchants that accept credit and/or debit cards as a form of payment for the products and services provided to their customers. Such payments are accepted in either a card present or card-not-present environment using third party hosted payment software. The merchant does not store or transmit cardholder data. This document is intended as a “Best Practice Guide for Security and Compliance” but alone does not necessarily make a merchant PCI compliant.
What is PCI Compliance?

In response to a growing number of data security breaches, the major payment card brands (Visa, MasterCard, Discover, etc.) came together in 2006 to form the Payment Card Industry Security Standards Council (PCI SSC). The PCI SSC developed a set of security requirements for all businesses that handle payment cards, including merchants and software developers of applications that handle payment card data. This set of requirements is known as the Payment Card Industry Data Security Standard (PCI DSS). PCI compliance applies to any merchant, bank or processor who handles payment card information.

What are the PCI DSS Requirements?

**Build and Maintain a Secure Network**
- Requirement 1: Install and maintain a firewall configuration to protect cardholder data
- Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters

**Protect Cardholder Data**
- Requirement 3: Protect stored cardholder data
- Requirement 4: Encrypt transmission of cardholder data across open, public networks

**Maintain a Vulnerability Management Program**
- Requirement 5: Use and regularly update anti-virus software
- Requirement 6: Develop and maintain secure systems and applications

**Implement Strong Access Control Measures**
- Requirement 7: Restrict access to cardholder data by business need-to-know
- Requirement 8: Assign a unique ID to each person with computer access
- Requirement 9: Restrict physical access to cardholder data

**Regularly Monitor and Test Networks**
- Requirement 10: Track and monitor all access to network resources and cardholder data
- Requirement 11: Regularly test security systems and processes

**Maintain an Information Security Policy**
- Requirement 12: Maintain a policy that addresses information security
The Key to Achieving PCI Compliance

It is important to remember that PCI compliance is not just an annual assessment of a businesses cardholder data environment, but rather a practice of secure measures on a 24/7/365 basis. Understanding and implementing the twelve requirements of PCI DSS can seem daunting, especially for merchants without a large security or IT department. However, the PCI DSS standard mostly calls for good, basic security practices which are outlined in this document. This document is intended as a “Best Practice Guide for Security and Compliance” to help merchants implement and maintain a secure payment processing environment.

Even if there was no requirement for PCI compliance, the best practices for security contained in the standard are steps that every business would want to take to protect their customers’ sensitive data and continuity of operations.

The Shocking Statistics

Credit card breaches cost businesses $5.7 million* per incident in expenses which include detection, notification, legal fees, loss of customers, and brand damages.

The average cost per compromised record, whether it was a stored credit card number or harvested by thieves while in transit is an average of $188**.

In 2013, 64.4% of organizations failed to restrict each account with access to cardholder data to just one user — limiting traceability and increasing risk.***

Payment card data remains one of the easiest types of data to convert to cash, and therefore the preferred choice of criminals. 74% of attacks on retail, accommodation, and food services companies target payment card information.***

---

* 2012 Payment Card Threat Report, Security Metrics
** Ponemon Institute 2013 Cost of a Data Breach Study: Global Analysis
*** Verizon 2014 PCI Compliance Report
Laws and Mandates Governing Securing Customer Data

Merchants should be aware of the laws and mandates applicable to their acceptance of credit and debit card payments.

Federal Laws
The Gramm-Leach-Bliley Act ("GLBA") and the Health Insurance Portability and Accountability Act ("HIPAA") require that financial and health care providers take steps to ensure that personal information is secure. Consult an attorney to determine if you are covered by these laws, as the government considers many small businesses “financial institutions” or “health care providers” even when the business might not consider itself to be involved in financial services or health care.

- **Summary of federal state data breach and privacy statutes** http://www.occ.treas.gov/consumer/Customernoticeguidance.pdf

State Laws
A majority of the states have passed laws requiring small businesses to implement procedures to prevent customer information from being disclosed or improperly used. Some states specifically require that small businesses encrypt personal information that is sent over the Internet. Unlike federal laws, these state laws apply to all small businesses — not just those that are financial institutions or a health care provider. Additionally, 47 states have passed legislation requiring disclosure of any incident involving the loss of consumer information.

- **Links to state data breach notification statutes:** http://www.ncsl.org/Default.aspx?TabId=13489
- **www.consumersunion.org/campaigns/financial-privacynow/002215indiv.html**

Contractual Requirements ("PCI")
Small businesses that accept credit and debit card payments are contractually required to take certain steps to secure the credit and debit card information they collect – referred to as the PCI standards. Contact the company that manages your payment card processing for details or visit https://www.pcisecuritystandards.org/ for more details on the PCI requirements for protecting payment card data.
Securing Your Customers Data - PCI Requirements Addressed with Simple Steps

Given all the things I need to juggle to run my business, why should I make securing my customer data a priority?

As hard as you’ve worked to earn your customers’ trust in you and your business, it can take just one trigger to break that trust. Your ability to keep your customers’ sensitive data secure is one of those make-it-or-break-it triggers. Customers expect that every business — large or small — that collects their sensitive personal information will protect it. Beyond customer expectations, there’s the law. Depending on your type of business and the states in which your customers reside, you may be legally required to protect the personal information you collect.

This feels overwhelming. How do I even start this process?

It will be less overwhelming if you approach this piece by piece. First — determine what makes sense for your type of business by completing five (5) core steps.

1. Inventory all your data and its various types and forms.
2. Inventory all the different sites/places where you store data.
3. Inventory potential sources for customer information leaks.
4. Implement the Securing Data “Do’s” and address the “Don’ts”.
5. Write this all down, and you’ll have just created the foundation of your written security policy.
What are five (5) minimum security actions a small business should implement?

Destroy information when it is no longer needed...and destroy it responsibly. Do enter customer card numbers and information directly into only a PCI compliant payment application. If you must write down card information prior to entry (due to systems being down), cross-shred the information immediately after entering into your payment application when it becomes available. If you must store credit and debit card numbers for back up purposes, ensure all files are encrypted techniques with strong passwords and stored in a secure location. Utilize tokenization technology to securely store cardholder data offsite at a PCI DSS compliant service provider. Using this technology, merchants can perform card-on-file billing and scheduled payments without the risk and liability associated with storing cardholder data. Make sure to use a PCI compliant payment processing solution.

- **DO NOT**....keep information that you don’t absolutely need (review and purge historical data and files).
- **DO NOT**....write down customer card numbers and/or other card information that can be entered directly into your payment application.
- **DO NOT**....store sensitive information, particularly credit and debit card numbers in: excel spreadsheets clear text, never store credit/debit card magnetic stripe data.
- **DO NOT**....use a payment application that stores or transmits sensitive cardholder data in the clear.
“Restrict & Limit Access”

Limit the number of sites/locations where sensitive information is stored. If it is unavoidable to store sensitive information on portable devices for back up purposes, make sure the information is encrypted and maintained in a secure location. Seek a more secure hosted option for backup. If paper records are business necessary, keep paper records in a locked cabinet, preferably offsite, or in a room that stays locked when not in use. Limit employees’ physical and logical access to data to only those that need the information to do their job. Encrypt sensitive electronic information in every area it is stored. If you have a business that electronically stores a great deal of sensitive information, invest in higher-level security software to provide advanced encryption software for desktops, laptops, and removable storage devices. Force computer lock (screensaver password protected) after 15 minutes of inactivity (to prevent unauthorized used or a rogue employee accessing sensitive data). Transmit data over the internet using secure connections (e.g., using a Secure Sockets Layer or “SSL” technology). There are several companies that offer relatively inexpensive web-based sites, known as FTP sites, which can transfer data with a secure connection.

• **DO NOT**....lock sensitive information in a file drawer and/or cabinet that is easily accessible to your building entrances or unauthorized employees.
• **DO NOT**....store sensitive information on portable devices (e.g., USB drives, laptops, smart phones, external hard drives, etc.) as these devices are frequently lost or stolen.
• **DO NOT**....keep paper records (if possible).
• **DO NOT**....make physical keys and computer passwords accessible to all employees.
• **DO NOT**....store sensitive data unencrypted allowing easy access to customer information.
• **DO NOT**....allow computers to remain on without screensaver passwords enabled.
• **DO NOT**....perform payment and/or banking functions using internet connectivity in public areas (with common/ shared logon and passwords, i.e., Wi-Fi at restaurants, airports, hotels).
“Use Effective Passwords”

Every employee with computer access should be assigned a unique ID and use a robust password with a minimum of eight (8) characters (e.g., mix of letters, numbers, and symbols) so you can control access by user. Make sure to change passwords regularly – every 45-60 days.

- **DO NOT**....share passwords.
- **DO NOT**....use the default password that may be provided by another company or service provider.
- **DO NOT**....use obvious passwords such as your name, your business name, your merchant ID, address, date of birth, SSN, any family member’s name, “12345,” “ABCDE,” “password” or your user name.

“Block Potential Intruders”

Restrict computer use to business-only purposes. Malware and viruses can sneak onto business machines when employees use them to download software or visit social networking and other personal web sites. Protect your IT systems from viruses, malware and spyware by using up-to-date antivirus protection and firewalls. Most operating systems and antivirus programs contain an automatic update feature that updates the software as new viruses and spyware become known. Antivirus protection is not enough. Consider supplementing your anti-virus protection and firewalls with other specialized protection tools, such as intrusion prevention and anti-spam technologies. Set computers and applications to automatic Windows or MAC updates to protect from known vulnerabilities/exploits. Limit use of remote access applications to only those you trust and authorize to access your environment.

- **DO NOT**....use a general purpose computer for your POS payments.
- **DO NOT**....allow anti-virus, malware and spyware software subscriptions to expire without renewal.
- **DO NOT**....connect directly to the internet without proper and updated firewalls installed on your computer or a router between your computer and the internet connection.
- **DO NOT**....use system software and application versions with known security vulnerabilities.
- **DO NOT**....leave remote access applications (typically used by your IT servicer as “remote desktop” to view your computer) in an “always on” mode.
“Test & Monitor Systems”

Regularly monitor and test networks/systems that are connected to and/or used to conduct payments. This can be accomplished by performing vulnerability scans regularly, at least quarterly per PCI mandates, against your internet connection.

- **DO NOT....**ignore the PCI rules that require internet-connected payment systems from having a quarterly vulnerability scan.

---

**About Element**

Headquartered in Chandler, Arizona, Element Payment Services, Inc., a Vantiv Company (NYSE: VNTV), is an industry leading software company that develops PCI DSS compliant technology designed to secure the processing, transmitting, and storing of payment card related data. Element’s technology is deployed through partnerships with point of entry hardware vendors and business management software providers. Engineered using service-oriented architecture, Element’s Express Processing Interface allows for easy integration and supports advanced technologies including tokenization and point-to-point encryption (P2PE).

Written by Susan Kohl, President & CEO of ThoughtKey. ThoughtKey provides personalized risk management, portfolio strategy guidance and strategy consulting services to the payment card industry. Please visit www.thoughtkeyinc.com for more information.