FIS Merchant Solutions

Payment Card Industry

(PCI) Compliance and EMV Payments

The information in this document includes summaries of certain requirements imposed by FIS, the Card Associations and applicable law relating to merchant acceptance and processing of credit and debit card transactions.

This document is not meant to be a detailed description or a complete listing of all these requirements or of your obligations. We urge you to read your Merchant Agreement, the rules and regulations of the Card Associations, the Payment Card Industry Data Security Standards and applicable law in order to understand fully all of your obligations as a merchant accepting card transactions and, if appropriate, consult with your own legal advisor. We also note that these requirements may change over time, and that you will be responsible for complying with any such changes as they come into effect.

Fidelity Information Services, LLC is a registered ISO of Wells Fargo Bank, N.A., Concord, CA
Fidelity Information Services, LLC is a registered ISO of ICBA Bancard, Washington, DC

Table of Contents

Payment Card Industry (PCI) Compliance.......4

Payment Card Industry Data Security Standard.......4

Requirements for Protecting Transaction Data.......4

Compliance Validation.......6

Network Scans.......6

Frequently Asked PCI Questions.......7

Where can I get information on the published PCI DSS or individual Card Brands' security programs?.......7

Do I need to upgrade equipment, software or networks to become PCI DSS compliant?.......7

How is an IP-based Point-Of-Sale (POS) environment defined?.......7

How is transaction volume that determines a merchant's compliance level measured?.......7

Can my compliance requirements change?.......8

If I change the way I process transactions, including storage or transmission of cardholder data, do I have to recertify my compliance?8

How is cardholder data defined?.......8

When is it acceptable to store chip or magnetic stripe data?.......8

What if my business does not comply with PCI DSS?.......8

What is a network security scan?.......9

Is there a cost for qualified security assessor (QSA) or approved scanning vendor (ASV)?.......9

How can I find a list of approved security assessors and scanning vendors?.......9

I use a PCI DSS-compliant terminal/gateway. Do I need to certify PCI DSS compliance?.......9

I currently use a PCI-compliant (and validated) service provider. Why do I need to certify I am PCI DSS compliant?.......9

What should I do if I suspect a breach has occurred and cardholder data may have been compromised?.......9

EMV – Europay Mastercard Visa.......10

What is EMV?.......10

What is "Liability Shift"?.......10

Where can I find additional information related to EMV?.......10

Payment Card Industry (PCI) Compliance

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

Please be advised that all merchants accepting cards must be PCI compliant. FIS™ Merchant Solutions provides the Merchant Intelligence Center (MIC) tool at: https://www.merchantintel.com/mic. This website allows you to take a Self-Assessment Questionnaire (SAQ) to validate your compliance status.

Please complete the SAQ in MIC within 60 days of receipt of this package to avoid being billed a non-compliance surcharge. If you need assistance in completing the questionnaire, contact your Merchant Relationship Team for guidance.

Payment Card Industry Data Security Standard

Requirements for Protecting Transaction Data

The Payment Card Industry Data Security Standard (PCI DSS) is a set of comprehensive requirements for enhancing the security of payment account data – essentially to reduce card data theft and the resulting fraud. It specifically applies to all merchants that take credit and debit cards, regardless of size or transaction volume, as well as any business involved in the storage, processing or transmission of cardholder data.

The PCI DSS was developed by the founding payment brands of the PCI Security Standards Council (American Express, Discover Financial Services, JCB International, Mastercard Worldwide and Visa Inc.) to help facilitate the global adoption of consistent data security measures. PCI DSS compliance does not guarantee that a security breach will never occur; but, it does greatly minimize the chance of a successful breach occurring. If your business is validated as compliant at the time of a breach, the payment networks may give you Safe Harbor from fines.

FIS requires merchants, small or large, that process, store or transmit card data to validate PCI DSS compliance by adhering to the following requirements:

1. **Install and maintain a firewall configuration to protect data.** Firewalls are computer software devices that control traffic in the company's network. This includes unauthorized access from the Internet, as well as access to sensitive areas from the company's internal network.

2. **Avoid vendor-supplied defaults for system passwords.** Hackers attempt to identify passwords and settings and use them to compromise systems. Always change these defaults before installing a system on the network.

3. **Protect stored transaction data.** Keep transaction storage to a minimum and never store sensitive authentication data after authorization. Take precautions to make stored transaction data unreadable through encryption or some other secure and robust approach.

4. **Encrypt transaction data when transferred over networks.** Sensitive information should always be encrypted during transmission over wireless networks or the Internet, as it is often easy to divert or intercept data while in transit. Never send any transaction data via email.

5. **Utilize anti-virus software or programs.** Install these mechanisms on all systems that can be affected by viruses, and ensure that these systems are current, running and capable of generating audit logs.

6. **Develop and maintain secure systems and applications.** As a participating merchant or service provider, you must ensure that all components have the latest vendor security and software patches to protect against external hackers and viruses. Develop standard system development processes and secure coding techniques.

7. **Restrict access to data.** Limit access to resources and cardholder information to employees who need access to the information to do their jobs - and limit access only to what is needed. Establish a mechanism for systems that restrict access based on an individual's need to know.

8. **Assign a unique user name and password to each person with computer access to transaction data.** This allows for all actions taken on the system to be identified and tracked. Take necessary precautions to protect user identification, and immediately revoke access for terminated users.

9. **Restrict physical access to transaction data. Use appropriate facility entry controls and monitor access.** Develop procedures to help personnel easily distinguish between employees and others. Destroy media containing transaction information when it is no longer needed.

10. **Track and monitor access to network resources and transaction data.** Logging mechanisms and tracking user activity are critical to uncovering unauthorized and illegal activity.

11. **Regularly test security systems and processes.** New vulnerabilities are continually being discovered. Consistent testing ensures security maintenance.
12. **Maintain an information security policy.** A strong security policy sets the security tone for the entire company.

13. **Use only PCI Qualified Integrated Resellers (QIR) for POS application and terminal installations and integrations.** Level 4 merchants must use only PCI-Certified QIR professionals for the installation and integration of their POS systems. Annual validation of PCI DSS compliance is required, or participate in the Technology Innovation Program (TIP).

Some of the standards above may not be applicable to all environments.

Compliance Validation

FIS requires all merchants to validate their PCI DSS compliance, and the PCI Compliance section of MIC (www.merchantintel.com/mic) makes fulfilling this responsibility simple and convenient. To validate compliance, merchants must take the following steps:

- Complete and pass an annual PCI DSS Self-Assessment Questionnaire (SAQ) appropriate for your merchant processing environment.
- If you are storing or processing cardholder data on or through an Internet-facing environment, you must also pass quarterly vulnerability scans of your network. Additional certification requirements may apply based on your processing environment and the number of transactions you process annually.

Log into MIC at anytime to easily access the tools that help you maintain compliance. If you choose not to take advantage of the MIC access that is automatically provided to you, including the compliance tools, we recommend that you engage a qualified security assessor (QSA) to assist you through this process.

Network Scans

The PCI DSS requires that all merchants with external-facing IP addresses perform quarterly network scans to achieve compliance. Scans identify vulnerabilities in operating systems, services, and devices that could be used by hackers to target the company’s private network. A current list of qualified scanning vendors can be found at the PCI Security Standards Council website, www.pcisecuritystandards.org.

Frequently Asked PCI Questions

Where can I get information on the published PCI DSS or individual Card Brands' security programs?

PCI DSS is managed by PCI Security Standards Council (SSC). Information can be found at: PCI SSC www.pcisecuritystandards.org

The Card Brands each have their own programs that help businesses enforce compliance with the PCI DSS. The PCI SSC was founded in 2006 to oversee the standard itself; but, each of the Card Brands issue fines, fees and schedule deadlines through their own enforcement programs.

- Visa Cardholder Information Security Program (CISP)
  www.visa.com/cisp
- Mastercard Site Data Protection (SDP)
  www.Mastercard.com/sdp
- Discover Information Security and Compliance (DISC)
  www.discovernetwork.com/disc
- American Express Data Security Operating Policy (DSOP)
  www.americanexpress.com/datasecurity

Do I need to upgrade equipment, software or networks to become PCI DSS compliant?

In order to become compliant, you may be required to upgrade your equipment or software to a PA-DSS version. You may also need to address vulnerabilities within your networks. You will need to contact your equipment and/or software vendors to discuss options available and costs associated with an upgrade. The costs associated with any equipment and/or software upgrade are your responsibility.

How is an IP-based Point-Of-Sale (POS) environment defined?

An IP-based POS environment is one in which transactions are stored, processed or transmitted using an Internet-facing Internet Protocol (IP) address. POS software that is visible from the Internet increases risk to the cardholder data environment. PCI DSS requires vulnerability scanning of all Internet-facing system components owned or utilized by a merchant that are part of the cardholder data environment, as well as any externally-facing system that provides a path to the cardholder environment.

How is transaction volume that determines a merchant's compliance level measured?

The number of transactions will be determined based on the gross number of Visa, Mastercard, American Express and Discover Network transactions processed by a merchant outlet or a chain of stores. In those cases where a corporation owns several chains, each chain will qualify independently.

Can my compliance requirements change?

Yes, as your transaction volume changes, and as card association (such as Visa, Mastercard, American Express and Discover) rules change, compliance requirements may change. It is your responsibility to be aware of the data security requirements that currently apply to you.

If I change the way I process transactions, including storage or transmission of cardholder data, do I have to recertify my compliance?

Yes. Changes to your payment processes or environment may increase your vulnerability to a security breach and may require recertification. Please contact your Merchant Relationship Team as soon as possible to discuss the changes and next steps.

How is cardholder data defined?

Cardholder data is any personally identifiable data associated with a card-holder. This could be an account number, expiration date, name, address or Social Security number. The account number is the critical component that makes the PCI DSS applicable. All personally identifiable information associated with the cardholder that is stored, processed or transmitted is also considered cardholder data. However, PCI DSS applies even if the only data stored, processed or transmitted is account numbers.

When is it acceptable to store chip or magnetic stripe data?

It is never acceptable for acquirers, merchants or service providers to retain chip or magnetic stripe data, including the card verification value or code (CVV2/CVC/CID). American Express, Visa, Mastercard and Discover Network operating regulations prohibit storage of the contents of the chip or magnetic stripe data. The CVV2/CVC/CID is a three-digit code located on the back of a card, inside the signature panel area. The three-digit code helps merchants ensure that the card is in the owner’s possession.

What if my business does not comply with PCI DSS?

According to the payment networks, the penalties and fines for failure to comply with requirements or to rectify a security issue can be severe and can range from $10,000 to more than $500,000 per incident. If a security breach occurs in your environment, you will be liable for the cost of the required forensic investigations, as well as covering the costs of fraudulent purchases. You will also be liable for the costs of re-issuing stolen cards. Beyond fines, your business may lose card acceptance privileges, at least for a period of time. You may also experience loss of customer confidence as customers find out you are not doing as much as others to protect their private information.

What is a network security scan?

A network security scan uses an automated tool that checks a merchant or service provider’s system for vulnerabilities. The tool conducts a nonintrusive scan to remotely review networks and Web applications based on the IP addresses provided by the merchant or service provider. The scan identifies vulnerabilities in operating systems, services and devices that could be used by hackers to target the company’s network – private or public (for example, the Internet). A qualified scan vendor will provide a tool that will not require the merchant or service provider to install any software on their systems.
No denial-of-service attacks will be performed.

Is there a cost for qualified security assessor (QSA) or approved scanning vendor (ASV)?

Yes, there is a cost to using a QSA or ASV to ensure compliance. The specific cost will vary depending on your level, the number of IP addresses to be scanned, the frequency of the scans and the chosen scan vendor.

How can I find a list of approved security assessors and scanning vendors?

A list of approved QSAs and ASVs can be found on the PCI SSC Web site at www.pcisecuritystandards.org.

I use a PCI DSS-compliant terminal/gateway. Do I need to certify PCI DSS compliance?

Yes, you must certify you are PCI DSS compliant. Use of a terminal/payment application/gateway that is Payment Application–Data Security Standard (PA-DSS) certified by the PCI SSC is only one of many components that are evaluated in the PCI DSS compliance assessment.

I currently use a PCI-compliant (and validated) service provider. Why do I need to certify I am PCI DSS compliant?

How you utilize the validated service provider determines the PCI DSS requirements and SAQ you must complete. If you utilize a validated service provider and process card transactions from your merchant environment, you are required to complete the SAQ and quarterly scan of your external network environment.

What should I do if I suspect a breach has occurred and cardholder data may have been compromised?

In the event of a security incident, contact Merchant Support immediately.

For step-by-step guidelines to address a security incident, visit Visa (www.visa.com/cisp) to review the “What to Do If Compromised” guide.

EMV – Europay Mastercard Visa

What is EMV?

The term EMV is an acronym for Europay, Mastercard and Visa, and it represents the use of chip card technology in payment transactions. A chip card transaction is only possible when both the card being used by the customer has a chip, and the terminal being provided by the merchant is chip-enabled.

“Chip technology is touted for its ability to combat counterfeit fraud for card-present transactions. Each time a debit or credit card is used at an EMV terminal, it produces a unique code that is not created by conventional magnetic-striped cards.”

What is “Liability Shift”?

“Liability Shift” refers to the party responsible for fraudulent transactions. Prior to EMV, the card issuer was primarily responsible for the costs associated with counterfeit fraudulent transactions. As of October 2015, the liability shifted to the participant who is least compliant in a given transaction.

For example, if a merchant’s terminal is not certified for chip card acceptance, the merchant’s acquirer may be liable for counterfeit fraudulent transaction. Likewise, if a counterfeit magnetic stripe card is presented at a chip enabled terminal, the card issuer may be liable for the counterfeit fraudulent transactions.

Where can I find additional information related to EMV?

Please visit our website at www.fisglobal.com/emv for additional information and resources.

Fidelity Information Services, LLC is a registered ISO of Wells Fargo Bank, N.A., Concord, CA
Fidelity Information Services, LLC is a registered ISO of ICBA Bancard, Washington, D.C.