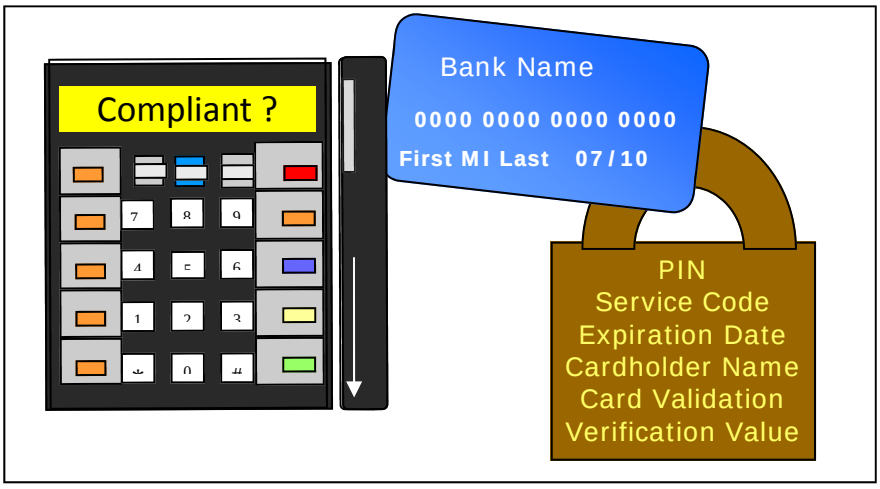
Cyber Security:

Secure Credit Card Payment Process

Payment Card Industry Standard Compliance

A Non-Technical Guide
Essential for
Business Managers
Office Managers
Operations Managers



Multi-State Information Sharing and Analysis Center

NYS Office of Cyber Security

This appendix is a supplement to the Cyber *Security: Getting Started Guide,* a non-technical reference essential for business managers, office managers, and operations managers. This appendix is one of many which is being produced in conjunction with the *Guide* to help those in small business and agencies to further their knowledge and awareness regarding cyber security. For more information, visit: http://www.dhses.ny.gov/ocs/.

Introduction

The use of credit cards as a method of payment allows organizations to receive payments from customers quickly and easily. However, the acceptance of credit cards comes with risks. Hundreds of millions of U.S. records have been involved in data loss incidents and that number keeps growing.

Could a breach happen at your organization? If you receive credit card payments either in person or online -- and your systems are not secure -- you could have a breach of data that is stored on a server, on paper, or on a computer. It could take many months for this breach to be discovered. In the meantime, the stolen information could have been sold and customers' credit cards used to commit fraud by purchasing items and opening new credit card accounts. Ask yourself, can it happen? Yes it can!

This guide outlines the controls an organization needs to implement when accepting credit card payments and provides examples of what organization managers need to know to protect data and specific information about how to secure credit card processing.

What You Need to Know Organization managers need to know about mandatory industry standards for the protection of credit cardholder data.

The Payment Card Industry (PCI) The world's major credit card companies (payment brands) have taken steps to protect their customers' personal information and protect the credit card payment process. In 2004 Visa and MasterCard collaborated to create the Data Security Standards (PCI-DSS), common industry security requirements. In 2006 the five major payment brands -- American Express, Discover, JCB, MasterCard and Visa -- formed the Payment Card Industry Security Standards Council (PCI-SSC) to manage the PCI-DSS. The PCI-SSC performs the following:

- manages three separate standards to ensure payment security:
  - The PCI Data Security Standard (PCI-DSS) - a set of 12 requirements designed to build a strong payment security foundation.
  - The Payment Application Data Security Standard (PA-DSS) – which establishes protocols and a testing procedure for software running on Point-of-Sales (POS) devices and electronic shopping carts.
  - The PIN Transaction Security Standard (PTS) – which defines the physical and logical security of devices involved in swiping credit card transactions, PIN entry devices and unattended payment terminals, like those at gas stations and parking facilities.
- creates helpful documents and tools for use in working toward payment security
- sets the standards for cardholder security but does not oversee compliance--each credit card company has its own set of rules for meeting compliance
- vets, trains and maintains lists of assessors (qualified individuals who perform PCI data security assessments and/ or scanning)
- tests and provides lists of Approved Scanning Vendors (ASVs), part of the compliance requirements for some merchants
- tests and maintains lists of approved software and hardware for securely conducting payment transactions
- maintains all PCI-SCC issued documents **-- it is important to check the website frequently to stay current**

Below are details regarding PCI Data Security Standard (PCI-DSS), PCI Payment Application Data Security Standard (PA-DSS) and PIN Transaction Security (PTS).

Payment Card Industry–Data Security Standard (PCI-DSS): is a global data security standard that governs any business, ***or organization***, that accepts payment cards and stores, processes and/or transmits cardholder data

- focused on protecting cardholder payment data and increasing consumer confidence
- mirrors best security practices for the protection of sensitive information
- requires twelve basic steps for protecting credit card information
- applies to internally developed or "homegrown" applications that are not sold to a third party

Payment Application Data Security Standard (PA-DSS): helps software vendors and others minimize vulnerabilities in payment applications (e.g., when a customer adds items to "a cart" while "shopping" on an organization's website).

- addresses Point–of-Sale (POS) software, e-commerce shopping carts and payment kiosks
- applies to payment applications that are sold, distributed or licensed to third parties

A list of certified payment applications is available at
https://www.pcisecuritystandards.org/approved_companies_providers/vpa_agreement.php

PIN Transaction Security (PTS): applies to companies which make devices that accept personal identification number (PIN) entry for all PIN-based transactions. Organizations are required to use a certified PIN entry device (PED or a POS swipe machine). Examples of use include:

- a PIN pad, where a customer enters a PIN to complete a transaction while a clerk is present.
- unattended payment terminals such as parking kiosks
- libraries, where a patron uses a credit card to make copies

A list of approved devices is provided on the PCI Security Standards Council website at
https://www.pcisecuritystandards.org/approved_companies_providers/approved_pin_transaction_security.php

Organizations should use certified PTS devices and check with their acquiring financial institution to understand requirements and associated timeframes for compliance.[1]

Do These Standards Apply to Your Organization? If your organization accepts, stores, processes and/or transmits credit card payments, including debit cards or pre-payments you are considered a merchant and these standards apply to your organization. Credit cards may be used to pay for taxes and fees, such as those for building permits, vital statistics documents, recreation programs, community center facility use, planning board review, court, civil service exams and business application fees (just to name a few). If your organization is required by law to handle payments directly and not through a third party, compliance may require more work. However, be aware that using a third party for your credit card processing does not absolve your responsibility for compliance. Even if you contracted out for these services, the PCI-DSS still applies to your organization. You must have a written agreement from your service provider verifying that they will be compliant with the requirements of PCI.

Your organization may be using multiple methods to accept payments in various departments. You must address each of these payment methods appropriately.

Not only is *electronic* credit card information covered by the PCI-DSS but *so are paper copies* and files. To ensure compliance, you need to follow the workflow of the payment process from the time it is initiated (submitted in person to an organization employee or online or by other means, such as by fax or by telephone) to the final storage of the transaction information, whether in a file cabinet or on a server or computer.

[1] Payment Card Industry Security Standards, PCI Standards Council

The Primary Account Number (PAN) is the defining factor in the applicability of PCI-DSS requirements and PA-DSS. If the PAN is stored, processed, or transmitted, PCI-DSS and PA-DSS apply. The following table highlights the do's and don'ts for storage.

Basic PCI Data Storage Guidelines for Merchants

Hhttps://www.pcisecuritystandards.org/pdfs/pci_fs_data_storage.pdf

Data Do's	Data Don'ts
Do understand where payment card data flows for the entire transaction process.	Do not store cardholder data unless it's absolutely necessary.
Do verify that your payment card terminals comply with the PCI personal identification number (PIN) entry device (PED) security requirements.	Do not store sensitive authentication data contained in the payment card's storage chip or full magnetic stripe, including the printed 3-4 digit card validation code on the front or back of the payment card, after authorization.
Do verify that your payment applications comply with the Payment Application Data Security Standard (PA-DSS).	Do not have PED terminals print out personally identifiable payment card data; printouts should be truncated or masked.
Do retain (if you have a legitimate business need) cardholder data only if authorized, and ensure its protected.	Do not store any payment card data in payment card terminals or other unprotected endpoint devices, such as PCs, laptops or smart phones.
Do use strong cryptography to render unreadable cardholder data that you store, and use other layered security technologies to minimize the risk of exploits by criminals.	Do not locate servers or other payment card system storage devices outside of a locked, fully secured and access-controlled room.
Do ensure that third parties who process your customers' payment cards comply with PCI DSS, PED and/or PA-DSS as applicable. Have clear access and password protection policies.	Do not permit any unauthorized individuals to access stored cardholder data.

For example, if a customer sends a PAN via email for a renewal or payment, the PAN is not secure and therefore not compliant.

Why Take Action? Many organizations store credit card numbers, card expiration dates, and customer data from the magnetic stripe on the card. See the chart below to determine what can be stored and what cannot be stored as this information can be used to steal the identity of card owners and compromise your system.

Technical Guidelines for PCI Data Storage
(See glossary for definitions)

	Data Element	Storage Permitted	Protection Required	PCI DSS Req. 3, 4
Cardholder Data	**Primary Account Number (PAN)**	**Yes**	**Yes**	**Yes**
	Cardholder Name [1]	**Yes**	**Yes [1]**	**No**
	Service Code [1]	**Yes**	**Yes [1]**	**No**
	Expiration Date [1]	**Yes**	**Yes [1]**	**No**
Sensitive Authentication Data [2]	**Full Magnetic Stripe Data [3]**	**No**	**N/A**	**N/A**
	CAV2/CVC2/CVV2/CID	**No**	**N/A**	**N/A**
	PIN/PIN Block	**No**	**N/A**	**N/A**

[1] These data elements must be protected if stored in conjunction with the PAN. This protection should be per PCI-DSS requirements for general protection of the cardholder data environment. Additionally, other legislation (e.g., related to consumer personal data protection, privacy, identity theft, or data security) may require specific protection of this data, or proper disclosure of a company's practices if consumer related personal data is being collected during the course of business. PCI-DSS, however, does not apply if PANs are not stored, processed, or transmitted.

[2] Sensitive authentication data must not be stored after authorization (even if encrypted).

[3] Full track data from the magnetic stripe, magnetic stripe image on the chip, or elsewhere.

More information on the previous two charts may be found at: https://www.pcisecuritystandards.org/pdfs/pci_fs_data_storage.pdf

If your system is compromised, you could:

- lose the ability to process credit cards
- be required to scan your system more frequently than otherwise required
- cause a negative impact on other stakeholders
- suffer loss of public confidence

The cost of a credit card breach can include fines and fees for which you are accountable and which may vary in severity depending on 1) the number of card numbers stolen; 2) if magnetic stripe (track) data was stored or not; 3) the timeliness of reporting the incident and 4) the circumstances surrounding the incident. Fines may be assessed by each of the credit card companies involved. There may also be extra costs for breach notification, forensic investigations and annual on-site security audits. Organizations are **not** exempt from these fees and fines.

But what will it cost to comply? *Less than if a breach occurs.* There will likely be costs for upgrading your payment systems and implementing security controls on your network(s) if none are currently in place. Vulnerability scanning and maintaining compliance will be ongoing costs, as threats and vulnerabilities continue to change. Costs may be minimal if your organization is already following the PCI-DSS and other best practices for securing information.

How can you secure the credit card data your organization processes? As a business manager, you should talk with the person responsible for your information security and IT Manager (if you have one) to determine how your organization needs to address compliance. The PCI-DSS Prioritized Approach is a great tool available from the PCI Security Standards Council to expedite your efforts towards payment security. Like other business programs, security begins with managing risk – where compliance is a byproduct of security. Implementing these six strategies can reduce the highest risk to cardholder data as early as possible in the journey to compliance:

1. **If you don't need it, don't store it** (in particular, credit card numbers and other sensitive data items at highest risk).
2. **Secure the perimeter** (use a network diagram to determine all access points—external, internal, and wireless networks — and segment the network to limit what you need to secure).
3. **Secure payment cards applications** (including application processes and servers).
4. **Control access to your systems** (know the who, what, when and how for people accessing your network).
5. **Protect stored cardholder data** (if your organization must store sensitive card information).
6. **Finalize remaining compliance efforts, and ensure all controls are in place** (complete the remaining PCI-DSS requirements, implement policy, procedures and processes).

The PCI-DSS Prioritized Approach is available at the PCI Security Standards Council website to assist your organization in organizing these strategies. Other tools and best practices continue to be added to the website at https://www.pcisecuritystandards.org/security_standards/documents.php

Additionally your organization should have policies and procedures for staff on how to handle card transactions and associated data. These procedures should address day-to-day operations, secure storage of paper records, and printouts. Your policies and procedures should reflect the PCI requirements (e.g., only saving the last four digits of the credit card number.)

Who are the players? The chart below contains the roles of various organizations involved in a credit card transaction.

Payment Brands	Processing organization MasterCard, ISA, American Express etc.) that licenses members and merchants to issue and accept credit cards
Issuers	Financial Institutions that issue credit cards to cardholders (name of institution on the card)
Acquirers	Financial institutions that support merchants by providing services for processing payment card transactions (accepts credit card transactions from the merchant)
Merchants	Any business owners, agencies or governments authorized to accept credit card transactions in exchange for goods and services
Service Providers	Organizations that process, store, or transmit cardholder data on behalf of members, merchants, or other service providers. (They may pass Information onto the bank or hold onto the information. Paypal and AuthorizeNet are examples of service providers.)

If you use a service provider, you will need to determine if the service provider is PCI compliant. A list of compliant service providers is available on each payment brand website.

Achieving Compliance

This section contains more specifics about securing the credit card process in your organization. Not only will the IT Manager need to be aware of the process but so will anyone involved with credit card transactions of any kind, including paper transactions which may be stored in file cabinet. Additional charts and information are found on the PCI and payment brands (e.g. Visa, MasterCard etc.) websites.

Organizations which process credit card payments are considered "merchants." Your merchant level is generally determined by how many credit card transactions your organization processes each year. However, payment brands may change your level if a breach occurs or at their discretion.

Note that each "payment brand' may use different parameters for establishing your merchant level and have different requirements at each level. You must comply with all payment brands' requirements for those payment brands in use. For example, one payment brand may categorize an organization as a level 1 while another brand categorizes the same organization as a level 2. In general, the more restrictive categorization would apply and the organization would need to validate at a level 1. Smaller numbers of transactions may result in fewer requirements. A merchant level chart is included at the end of this Guide; however check with your payment brand company for current merchant level definitions and validation requirements.

Start by writing and implementing information security policies and procedures, as required by the Data Security Standards. The previous Getting Started Guide and its companion guides located at http://www.dhses.ny.gov/ocs/resources/ are a good place to look for help with building policies.

If your wireless network is segmented from your credit card process, it does not need to be included in the planning. Any wireless network that may be involved with or connected to the credit card processor must be included in the compliance process.

The **PCI Standard** requirements are presented in the chart below:

PCI-DSS Overview Fact Sheet

(https://www.pcisecuritystandards.org/pdfs/pcissc_getting_started_with_pcidss.pdf)

Goals	General Requirements
Build and Maintain a Secure Network	**1)** Install and maintain a firewall configuration to protect cardholder data
	2) Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	**3)** Protect stored cardholder data
	4) Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	**5)** Use and regularly update anti-virus software or programs
	6) Develop and maintain secure systems and applications
Implement Strong Access Control Measures	**7)** Restrict access to cardholder data by business need-to-know
	8) Assign a unique ID to each person with computer access
	9) Restrict physical access to cardholder data
Regularly Monitor and Test Networks	**10)** Track and monitor all access to network resources and cardholder data
	11) Regularly test security systems and processes
Maintain an Information Security Policy	**12)** Maintain a policy that addresses information security for employees and contractors

Goal 1: Build and Maintain a Secure Network. PCI-DSS applies to the entire cardholder environment, i.e., the segment of the network, systems and equipment that transmits or stores cardholder data.

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

Organizations must secure all system components (network components, including wireless, servers, applications) that are connected to the segment containing the credit card information. Adequate segmentation and/or isolation of the cardholder environment reduce your scope of compliance.

Goal 2: Protect Cardholder Data

Requirement 3: Protect stored cardholder data

Requirement 4: Encrypt transmission of cardholder data across open, public networks

If you don't need it, don't store it. If you must store the primary account number (PAN), it must be unreadable through the use of strong encryption especially in the case of a wireless network or be truncated using only the first six or last four digits. Full magnetic stripe data must **NEVER** be stored after a transaction is authorized. The information on the card stripe contains the following sensitive information:

- Cardholder Name
- Service Code
- Expiration Date
- PIN – must never be stored
- CVV – Card Validation/Verification Value must never be stored

Technical Guidelines for PCI Data Storage
(See glossary for definitions)

	Data Element	Storage Permitted	Protection Required	PCI DSS Req. 3, 4
Cardholder Data	Primary Account Number (PAN)	Yes	Yes	Yes
	Cardholder Name [1]	Yes	Yes [1]	No
	Service Code [1]	Yes	Yes [1]	No
	Expiration Date [1]	Yes	Yes [1]	No
Sensitive Authentication Data [2]	Full Magnetic Stripe Data [3]	No	N/A	N/A
	CAV2/CVC2/CVV2/CID	No	N/A	N/A
	PIN/PIN Block	No	N/A	N/A

[1] These data elements must be protected if stored in conjunction with the PAN. This protection should be per PCI-DSS requirements for general protection of the cardholder data environment. Additionally, other legislation (e.g., related to consumer personal data protection, privacy, identity theft, or data security) may require specific protection of this data, or proper disclosure of a company's practices if consumer related personal data is being collected during the course of business. PCI-DSS, however, does not apply if PANs are not stored, processed, or transmitted.

[2] Sensitive authentication data must not be stored after authorization (even if encrypted).

[3] Full track data from the magnetic stripe, magnetic stripe image on the chip, or elsewhere.

More information on the previous two charts may be found at: https://www.pcisecuritystandards.org/pdfs/pci_fs_data_storage.pdf

Goal 3: Maintain a Vulnerability Management Program

Requirement 5: Use and regularly update anti-virus software

Requirement 6: Develop and maintain secure systems and applications

Anti-virus software, updated and maintained through software license renewals, is required on all operating systems to defend against malicious software. Additionally all computer systems must be patched to reduce software vulnerabilities. Organization applications accessed over the Internet must be written using secure programming code.

Goal 4: 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

Reduce the opportunities for accidental or inappropriate viewing of the credit card information by limiting who has access to the information. *Each* employee, contractor or individual authorized to process the credit card files must use strong passwords and have a unique ID. Sharing user accounts and passwords violates compliance requirements. If credit card files are stored off-site (see *Guidelines for Backing Up Information*), a designated individual should visit that site at least annually to confirm proper compliance. These requirements apply to paper files as well as electronic files. You must properly dispose of files that are no longer needed to ensure the sensitive information is not discovered by unauthorized individuals (see *Erasing Information and Disposal of Electronic Media Guide* at http://www.dhses.ny.gov/ocs/resources/).

Goal 5: 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

Work with your Information Technology (IT) Manager to make certain that log files are kept for all access to the network environment associated with the credit card data. Systems should be monitored constantly for access and data usage. This information will alert you to any potential problems and be useful to prove the logs are being kept. In the event, or suspicion, of a breach, these logs will be required for investigation (see *Cyber Incident Response Guide* at http://www.dhses.ny.gov/ocs/resources/). Under Requirement 11, organizations need to use Approved Scanning Vendors (ASVs) to test the computer system for vulnerabilities. Tests include penetration tests, vulnerability scanning and application scanning. More will be provided on scans in the following section.

Goal 6: Maintain an Information Security Policy

Requirement 12: Maintain a policy that addresses information security

An Information Security Policy is a best practice no matter what information is being handled or stored. The policy must be implemented and staff must be trained on the policies, procedures and processes associated with it.

PCI: Continuous Process PCI compliance is an ongoing process with these three primary steps:

1. Assess: taking an inventory of your IT assets and business processes for payment card processing, and analyzing them for vulnerabilities that could expose cardholder data
2. Remediate: fixing those vulnerabilities
3. Report: compiling of records required by PCI-DSS to validate remediation, and submission of compliance reports to the acquiring bank and card payment brands with which you conduct business

More information is available at: www.pcisecuritystandards.org/pdfs/pcissc_getting_started_with_pcidss.pdf

Step 1: ASSESS To determine your organization's compliance with the PCI Data Security Standard, begin with an inventory of all IT assets and business processes where a payment card is processed. Once all the assets and processes are identified, use the Standards above to follow the flow of the credit card payment process in your organization. Remember to include any third party partners that may be involved. All components of the process must be checked for vulnerabilities.

The PCI Standards Council provides two types of independent experts to help with assessments: the Qualified Security Assessor (QSA) and the Approved Scanning Vendor (ASV). QSAs have trained personnel and processes to assess and prove compliance with PCI DSS. ASVs provide commercial software tools to perform vulnerability scans for your systems.

Complete Self-Assessment Questionnaire (SAQ) Organizations which are not required to do on-site assessments for PCI-DSS compliance use the SAQ, a validation tool. You can complete the questionnaire yourself or contract with a QSA to complete it. SAQs must be performed annually by all organizations, regardless of level. An organization may fit one of five SAQ Validation Types.

See chart below.

Self-Assessment Questionnaire (SAQ)

SAQ Validation Type	Description	SAQ Type	Total number of questions
1	Card-not-present (e-commerce or ail/telephone-order) merchants, all cardholder data functions outsourced	**A**	**11**
2	Imprint-only merchants with no electronic cardholder data storage	**B**	**21**
3	Stand-alone dial-out terminal merchants, no electronic cardholder data storage	**B**	**21**
4	Merchants with Point–of-Sale or payment system connected to Internet. No electronic cardholder data storage	**C**	**38**
5	All other merchants that are SAQ-eligible	**D**	**226 (full DSS)**

The SAQ form can be found on the PCI website (https://www.pcisecuritystandards.org/security_standards/documents.php?category=saqs).
Any "NO"answers result in noncompliance and remediation must be done to bring the organization into compliance.

Step 2: REMEDIATE Remediation is the process of fixing vulnerabilities – including technical flaws in software code or unsafe practices in how an organization processes or stores cardholder data. Steps include:

- Scanning your network with software tools that analyze infrastructure and identify known vulnerabilities
- Reviewing and remediating vulnerabilities found in on-site assessment (if applicable) or through the SAQ process
- Classifying and ranking the vulnerabilities to help prioritize the order of remediation
- Applying patches, fixes, workarounds, and changes to unsafe processes and workflow
- Re-scanning to verify that remediation actually occurred.[2]

Perform network level security scan A vulnerability scan is required for all externally accessible (Internet facing) IP addresses, and all internal IP addresses associated with credit card data. External scans must be performed by an ASV, one which can be found on the PCI website. This scan is done to identify any problem areas on the network where malicious persons may attack. All vulnerabilities found must be remediated and the network scanned again to confirm all problems are addressed. Each time a change is made to the network, the network should be scanned again to identify any new problems or errors.

Step 3: REPORT You are required to submit regular reports for PCI compliance to your acquiring bank(s) and card payment brands with which you conduct business. PCI-SSC is not responsible for PCI compliance. All organizations must submit a quarterly scan report, which must be completed by a PCI approved ASV. Organizations with larger transaction flows must do an annual on-site assessment completed by a PCI approved QSA and submit the findings to each acquiring bank.

Organizations with smaller flows may be required to submit an annual Attestation within the Self-Assessment Questionnaire[3]. An Attestation of Compliance form, also found online, must be signed by an executive in the organization.

Summary

Organizations must comply with the PCI Data Security Standard and validate compliance. Compliance (securing the credit card process) requires ongoing adherence to the standard and applies to every organization, regardless of transaction volume. Validation confirms organizations, service providers, payment applications, and PIN entry devices are compliant with the standard. This involves either an annual QSA assessment or self-assessment questionnaire and a quarterly scan as determined by the merchant level. **Check the PCI Standards website for changes.**

Where can I find help? There are several websites to assist you in securing your organization's credit card process. The first site below contains extensive information including forms and is updated frequently.

- PCI Security Standards Council https://www.pcisecuritystandards.org/ has several worksheets for assisting with the Self-Assessment Questionnaire, storage, offers compensating controls guidance and other related materials.

- Visa Customer Information Security Program http://usa.visa.com/merchants/risk_management/cisp.html?ep=v_sym_cisp

- MasterCard Site Data Protection Program http://www.mastercard.com/us/company/en/whatwedo/site_data_protection.html

- Discover http://www.discovernetwork.com/merchants/fraud-protection/

[2] https://www.pcisecuritystandards.org/pdfs/pcissc_getting_started_with_pcidss.pdf
[3] https://www.pcisecuritystandards.org/pdfs/pcissc_getting_started_with_pcidss.pdf

- American Express
  https://www212.americanexpress.com/dsmlive/dsm/int/shared/supportcenter/fraudprevention.do?vgnextoid=b9afcfa5e7bbe210VgnVCM200000d0faad94RCRD

- Cyber Security Non-Technical Guides http://www.dhses.ny.gov/ocs/

- "Data Breaches: What the Underground World of "Carding" Reveals"
  https://www.pcisecuritystandards.org/pdfs/DataBreachesArticle.pdf

American Express, Discover, JCB, MasterCard, Visa Merchant Levels Defined

Level	AMEX	Discover	JCB	MasterCard	Visa
1	Merchants processing over 2.5 million American Express Card transactions annually or any merchant that American Express otherwise deems a Level 1	All merchants processing a total of more than 6 million card transactions annually on the Discover network. Any merchant Discover, in its sole discretion determines should meet the Level 1 compliance validation and reporting requirements All merchants required by another payment brand to validate and report their compliance as a Level 1 merchant	Merchants processing over 1 million JCB transactions annually, or compromised merchants	Merchants processing over 6 million MasterCard and Maestro transactions annually, identified by another payment card brand as Level 1, or merchants that have experienced an account data compromise	Any merchant-regardless of acceptance channel - processing over 6,000,000 Visa transactions per year. Any merchant that Visa, at its sole discretion, determines should meet the Level 1 merchant requirements to minimize risk to the Visa system.
2	Merchants providing 50,000 to 2.5 million American Express transactions annually Any merchant that American Express otherwise deems Level 2	All merchants processing a total of 1 million to 6 million card transactions annually on the Discover network. All merchants required by another payment brand to validate and report their compliance as a Level 2 merchant.	Merchants processing less than 1 million JCB transactions annually	Merchants processing 1 million to 6 million MasterCard and Maestro transactions annually	Any merchant-regardless of acceptance channel - processing 1,000,000 to 6,000,000 Visa transactions per year.
3	Merchants processing less than 50,000 American Express transactions annually	All merchants processing a total of 20,000 to 1 million card-not-present only transactions annually on the Discover network All merchants required by another payment brand to validate and report their compliance as a Level 3 merchant	N/A	Merchants processing 20,000 to 1 million MasterCard and Maestro e-commerce transactions annually	Any merchant processing 20,000 to 1,000,000 Visa e-commerce transactions per year.
4	N/A	All other merchants	N/A	All other MasterCard Merchants	Any merchant processing fewer than 20,000 Visa e-commerce transactions per year, and all other merchants-regardless of acceptance channel-processing up to 1,000,000 Visa transactions per year.

VISA, American Express, Discover, JCB, MasterCard
Merchant Validation Requirements Defined

Level	AMEX	Discover	JCB	MasterCard	Visa
1	Annual onsite review by QSA (PCI DSS Assessment) and Quarterly Network Scan by ASV	Complete an annual on-site assessment using the PCI DSS Requirements and Security Assessment Procedures. On-site assessment may be performed by a Qualified Security Assessor OR merchant's internal auditor Complete Quarterly Network Vulnerability Scans performed by an Approved Scanning Vendor	Annual onsite review by QSA (PCI DSS Assessment) and Quarterly Network Scan by ASV		
2	Quarterly Network Scan by ASV	Complete an annual self-assessment using the applicable PCI DSS Self-Assessment Questionnaire ("SAQ") Complete Quarterly Network Vulnerability Scans performed by an Approved Scanning Vendor	Annual Self-Assessment Questionnaire and Quarterly Network Scan by ASV	Annual onsite review by QSA (PCI DSS Assessment) and Quarterly Network Scan by ASV	Annual Self-Assessment Questionnaire and Quarterly Network Scan by ASV
3	Quarterly Network Scan by ASV (recommended)	Complete an annual self-assessment using the applicable PCI DSS SAQ Complete Quarterly Network Vulnerability Scans performed by an Approved Scanning Vendor	N/A	Annual Self-Assessment Questionnaire and Quarterly Network Scan by ASV	
4	N/A	Validation and Reporting Requirements determined by the merchant's acquirer Annual self-assessment using the applicable PCI DSS SAQ AND Quarterly Network Vulnerability Scans performed by an Approved Scanning Vendor are recommended	N/A	Annual Self -Assessment Questionnaire (recommended), Quarterly Network Scan by ASV, and compliance validation requirements set by acquirer	

Glossary

ASV	Approved Scanning Vendor
Acquirer	A financial institution that supports merchants by providing services for processing payment card transactions
Cardholder Data	At a minimum, cardholder data contains the full PAN. Cardholder data may also appear in the form of the full PAN plus any of the following: • Cardholder name • Expiration date • Service Code See Sensitive Authentication Data for additional data elements that may be transmitted or processed as part of a payment transaction. Full magnetic stripe or the primary account number (PAN) plus any of the following: Cardholder name, expiration date, service code
CISP	Visa's Cardholder Information Security Program
Compromise	Intrusion into a computer system where unauthorized disclosure, modification, or destruction of cardholder data is suspected.
CVV	Card Validation/Verification Value. Three-digit value printed to the right of the signature panel on the back of the credit card. American Express uses a four-digit code above the card number on the face of the card. May also be referred to as CAV (Card Authentication Value), CVC (Card Validation Code) or CSC (Card Security Code).
DISC	Discover Information and Security Compliance
DSOP	American Express's Data Security Operating Policy
DSS	Data Security Standard
Full Track / Magnetic Stripe Data	Also referred to as "track data". Data encoded in the magnetic stripe or chip used for authorization during payment transactions. Can be the magnetic stripe image on a chip or the data on the track 1 and/or track 2 portion of the magnetic stripe. Entities must not retain full magnetic stripe data after obtaining transaction authorization.
Issuer	Financial institution that holds contractual agreements with and issues cards to cardholders
Merchant	Any business owner, agency or **government organization** authorized to accept credit card transactions in exchange for goods and services
PABP	Visa's Payment Application Best Practices
PA-DSS	Payment Application Data Security Standard
PAN	Primary Account Number – payment card number
Payment Brands	Processing organization that licenses members and merchants to issue and accept credit cards, respectively (Visa, MasterCard, etc.)
PCI	Payment Card Industry

PCI-DSS	Payment Card Industry Data Security Standard
PIN	Personal Identification Number
POS	Point of Sale
PTS	PIN Transaction Security Standard
QSA	Qualified Security Assessor
SAQ	Self Assessment Questionnaire
SDP	MasterCard's Site Data Protection
Service code	Three-digit or four-digit value in the magnetic-stripe that follows the expiration date of the payment card on the track data. It is used for various things such as defining service attributes, differentiating between international and national interchange, or identifying usage restrictions.
Service Provider	Organizations that process, store, or transmit cardholder data on behalf of members, merchants, or other service providers
SSC	Security Standards Council