NEXT PERIMETER

PCI COMPLIANCE

COMPREHENSIVE GUIDE TO PROTECT YOUR CUSTOMERS AND BRAND

888-286-4816
NextPerimeter.com

TABLE OF CONTENTS

INTRODUCTION TO PCI COMPLIANCE

Business. Customers. Trust. Success. Security. These are the building blocks of a growing business. If you remove security, you might just find yourself without customers and a business.

Business success is built on trust – if you are B2B, customers trust that your team is going to deliver on time and fulfill your contractual obligations. If you're business-to-consumer (B2C), your guests demand a highly personalized experience from start to finish while treating their personal and sensitive information with the utmost security. If your organization experiences a data breach that compromises cardholder data, you might find out just how important information security and maintaining PCI compliance is to your business' ability to thrive in today's market

New advances in eCommerce and payment technology required new standards and regulations to protect business and consumers. Enter the Payment Card Industry Data Security Standard (PCI DSS), a standard put forth by the five largest credit card companies to help reduce costly consumer and data breaches.

Understanding and navigating PCI DSS compliance can feel overwhelming for business owners. In this guide, we cover everything you need to know about PCI DSS compliance and walk you through best practices to safeguard your business and customers.

HISTORY OF PCI COMPLIANCE

The internet gold rush of the late 1990s and early 2000s created adventurous merchants who wanted to leverage the internet for eCommerce. As acceptance of online payments gained ground, so too came the risks. Online payments caught the eye of malicious individuals. Soon cybercriminals began compromising card processing systems, e-retailers, and payment networks to extract cardholders' information to purchase prepaid cards, gift cards and goods online or resale. With major credit card companies facing skyrocketing rates of fraud and backlash from consumers Visa, MasterCard, American Express, Discover, and JCB came together to create a comprehensive standard for all merchants in the payment cycle, on December 15, 2001, PCI DSS Version 1.0 was released.

As the internet era began to reach maturity with online payments garnering mainstream adoption, more businesses brought their payment processing systems online, many companies began connecting virtual and physical terminals wirelessly and interconnecting multiple locations to establish centralized databases. Today, businesses collect vast quantities of personal information to create more connected and personalized experiences for customers.

These brand-new opportunities of commerce subjected businesses as well as consumers to more risks – and the opportunity for scammers to take charge card details from compromised networks

HISTORY OF PCI COMPLIANCE

To help with managing compliance standards, the payment brand names also established the PCI Security Standards Council as an independent body, with a set mission to "monitor threats and improve the industry's means of dealing with them, through enhancements to PCI Security Standards and by the training of security professionals." The PCI Security Standards Council is led by a policy-setting Executive Committee, composed of representatives from the five founding global payment brands and Strategic Members. A Board of Advisors, drawn from Participating Organizations, provides input to the organization and feedback on the evolution of the PCI Standards.

It's key to note that the PCI Security Standards Council is responsible for setting the standards and requirements that seller must adhere to – such as self-assessment questionnaires, security checklists, and PCI-compliant applications, it's the responsibility of the card brands to enforce PSI DSS compliance criteria among sellers and organizations that accept credit cards.

WHAT IS PCI DSS COMPLIANCE?

The Payment Card Industry Data Security Standard (PCI DSS) was developed by the five major credit card companies American Express, Discover, JCB, Master Card and VISA to encourage and enhance cardholder data security and facilitate the broad adoption of consistent data security measures globally to mitigate risks involved through online purchases or transactions while preventing data loss and security breaches.

PCI DSS provides a baseline of technical and operational requirements designed to protect account data. PCI DSS applies to all entities involved in payment card processing—including merchants, processors, acquirers, issuers, and service providers. PCI DSS also applies to all other entities that store, process or transmit cardholder data (CHD) and/or sensitive authentication data (SAD).

WHO DOES PCI COMPLIANCE APPLY TO?

PCI Compliance applies to any business that accepts credit or debit card transactions from any of the five major card associations (brands), including American Express, Discover, JCB, MasterCard or Visa.

PCI Compliance applies to any business that accepts credit or debit card transactions from any of the five major card associations (brands), including American Express, Discover, JCB, MasterCard or Visa.

For example, a managed IT service provides that provides managed firewalls or security solutions to a merchant or business accepting card payments is considered a ‘service provider’ and is co-responsible for maintaining PCI compliance.

While PCI DSS has no legal authority to compel compliance, it is a requirement of any business that wishes to facilitate transactions from any of the major card associations.

NEXT PERIMETER

PCI DSS REQUIREMENTS

A. SECURE NETWORK

Build and Maintain a Secure Network and Systems

- Install and maintain a firewall configuration to protect cardholder and account data
- Do not use vendor-supplied defaults for system passwords and other security parameters.

B. SECURE CARDHOLDER DATA

Protect Cardholder Data

- Protect stored cardholder data from compromise and unauthorized access.
- Encrypt transmission of cardholder data across open, public networks.

C. VULNERABILITY MANAGED

Maintain a Vulnerability Management Program

- Protect all systems against malware and regularly update anti-virus software or programs.
- Develop and maintain secure systems and applications.

D. ACCESS CONTROL

Implement Strong Access Control Measures

- Protect stored cardholder data from compromise and unauthorized access.
- Encrypt transmission of cardholder data across open, public networks.

E. NETWORK MONITORING AND TESTING

Regularly Monitor and Test Networks

- Protect stored cardholder data from compromise and unauthorized access.
- Encrypt transmission of cardholder data across open, public networks.

F. INFORMATION SECURITY

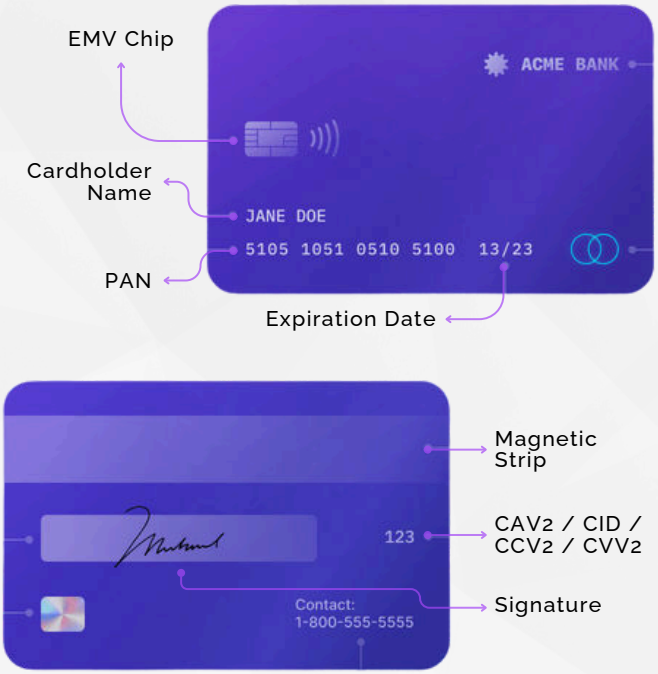
Maintain an Information Security Policy

- Maintain a policy that addresses information security for all personnel.

HOW DOES THE PCI SECURITY STANDARDS COUNCIL DEFINE ACCOUNT DATA?

PCI DSS applies to all entities involved in payment card processing—including merchants, processors, acquirers, issuers, and service providers. PCI DSS also applies to all other entities that store, process, or transmit cardholder data and/or sensitive authentication data. Cardholder data and sensitive authentication data are defined as follows:

Cardholder Data	Sensitive Authentication Data
• Primary Account Number (PAN) – 16-digit card number • Cardholder Name • Expiration Date • Service Code	**THIS DATA CANNOT BE STORED PER PCS DSS 3.2** • Full track data (magnetic-stripe data or equivalent on a chip) • CAV2/CVC2/CVV2/CID • PINs/PIN blocks



It's important to understand what data elements PCI DSS allows them to store and what measures they must take to protect those data. To prevent unauthorized storage, only Council certified PIN entry devices and payment applications may be used.

The primary account number is the defining factor for cardholder data. If cardholder name, service code, and/or expiration date are stored, processed or transmitted with the PAN, or are otherwise present in the cardholder data environment (CDE), they must be protected in accordance with applicable PCI DSS requirements.

In general, no payment card data should ever be stored by a merchant unless it's necessary to meet the needs of the business. Sensitive data on the magnetic stripe or chip must never be stored. Only the PAN, expiration date, service code, or cardholder name may be stored, and merchants must use technical precautions for safe storage.

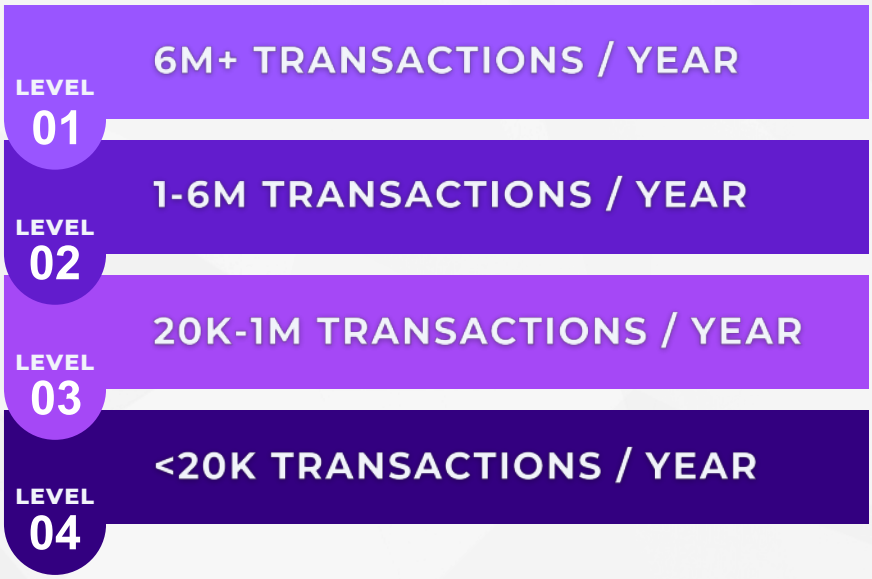
PCI COMPLIANCE LEVELS

If you accept card payments (card present, t present or online) with any one of the five PCI DSS card brands (American Express, Discover, JCB International, MasterCard, and Visa), then your company is required to be PCI DSS compliant. Each merchant is categorized in one of four levels (Level 1 – Level 4) based on the number of transactions processed across all channels and whether or not your company has experienced a cyberattack that compromised cardholder account data.

Merchants with higher volumes of transactions are held to more stringent compliance standards than their lower volume counterparts because of the inherent risks. For example, Level 4 merchants processing 6 Million or more transactions are required to work with Internal Security Assessors (ISAs), Qualified Security Assessors (QSAs), and PCI Council Approved Scan Vendors (ASVs) to maintain their PCI DSS compliance status.

Every seller falls into one of the four categories depending on their transaction volume during a 12-month period. While each credit card brand has its own slightly different criteria, generally the PCI-compliance levels are as follows*:

PCI DSS COMPLIANCE LEVELS



LEVEL 1 MERCHANTS

Level 1 is the highest level of PCI compliance of the four merchant levels. Merchants that process over 6 million transactions per year whether card present, card not present, online or in-store, are considered a Level 1 Merchant. In addition, any merchant that has had a data breach or successful cyberattack (internal or external) that resulted in compromised payment card information is automatically elevated to Level 1. It's important to note that card associations can enhance the compliance level of a merchant at their discretion. Here are the requirements for Level 1 merchants to sustain PCI compliance:

- File an Annual Report on Compliance (ROC) by a Qualified Security Assessor (QSA) or Internal Auditor if signed by an officer of the company. It's highly recommended by the PCI Council for the Internal Auditor to obtain a PCI SSC Internal Security Assessor ("ISA") certification
- Submit an Attestation of Compliance (AOC) form
- Conduct quarterly network scans by an Approved Scan Vendor (ASV)

LEVEL 2 MERCHANTS

Merchants that process one to six million transactions across all channels annually are designated as Level 2 merchants. Level 2 merchants are required to complete the following to maintain PCI compliance:

- Complete a Self-Assessment Questionnaire (SAQ) annually– here's a link to the PCI DSS SAQ version 3.2
- Submit an Attestation of Compliance (AOC) form (Word document link) each year
- Complete and obtain evidence of passing a vulnerability scan with an Approved Scanning Vendor (ASV)
- Conduct a quarterly network scan by an ASV

LEVEL 3 MERCHANTS

Any merchant with more than 20,000 combined transactions annually but less than or equal to one million total transactions across all channels is considered a Level 3 merchant. Level 3 merchants are required to:

- Complete a Self-Assessment Questionnaire (SAQ)
- Submit an Attestation of Compliance (AOC) form each year
- Complete and obtain evidence of passing a vulnerability scan with an Approved Scanning Vendor (ASV)
- Conduct a quarterly network scan by an ASV

LEVEL 4 MERCHANTS

Level 4 merchants include any seller that processes less than 20,000 payment transactions across all channels. Level 4 merchants are required to:

- Complete the Annual Self-Assessment Questionnaire (SAQ)
- Submit an Attestation of Compliance (AOC) form each year
- Conduct a quarterly network scan by an Approved Scan Vendor (ASV)

SERVICE PROVIDERS AND PCI DSS COMPLIANCE

A Service Provider is a business entity directly involved in processing, storage, or transmission of cardholder data on behalf of another business. This also includes companies that provide services that control or impact the security of cardholder data (e.g. Next Perimeter). Service providers include companies that provide managed IT services, managed firewalls, intrusion detection software or services, and in general security or infrastructure support for organizations that accept card payments.

PCI DSS COMPLIANCE SERVICE PROVIDER LEVELS

LEVEL 01 STORE, PROCESS OR TRANSMIT >300K TRANSACTIONS

Level 1 Service Providers are service providers that store, process, or transmit more than 300,000 credit card transactions annually.

PCI Requirements:

- Annual Report on Compliance (ROC) by a Qualified Security Assessor (QSA)
- Quarterly network scan by an Approved Scanning Vendor (ASV)
- Penetration Test
- Internal Scan
- Bi-annual network segmentation tests
- Attestation of Compliance (AOC) Form

LEVEL 02 STORE, PROCESS OR TRANSMIT <300K TRANSACTIONS

These are service providers that store, process, or transmit less than 300,000 credit card transactions annually.

PCI Requirements:

- Annual Self-Assessment Questionnaire (SAQ)
- Quarterly network scan by an ASV
- Penetration Test
- Internal Scan
- Bi-annual network segmentation tests
- AOC Form

Note: In some cases a Level 2 Service Provider will be asked by its partners, clients, or integration partners to validate compliance as a Level 1 with a QSA onsite assessment. Level 2 Service Providers will also sometimes choose to validate as a Level 1 to be listed as one of Visa's Global Registry of Approved Service Providers.

HOW TO BECOME PCI COMPLIANT

The first step a business must take to become PCI compliant is to shift its belief that obtaining and sustaining PCI DSS compliance is difficult to achieve. Many business owners become intimidated after their initial research or perceive that achieving PCI DSS compliance is more expensive and difficult than it actually is. While, yes, the process can be complex – it's imperative that businesses don't procrastinate or slack on shoring up PCI DSS compliance policies, payment data management procedures, and/or avoid taking a proactive approach to cybersecurity.

Secondly, business executives and stakeholders need to stop thinking about PCI Compliance solely in terms of 'meeting compliance' and instead translate 'meeting compliance' to 'implementing and maintaining a strong physical, data and cybersecurity posture'. The vast majority of PCI compliance penalties are levied as the result of a data breach that occurred because the organization refused to implement foundational security best practices or did not have active threat monitoring, detection, and remediation strategies.

Being PCI compliant involves implementing security controls outlined in the PCI DSS, signing a contract agreeing to a payment brand or merchant acquirer's terms for PCI compliance, and completing an annual self-assessment.

These are the five (simplified) steps a business will need to take to become PCI compliant:

1. Analyze Your Merchant Compliance Level

The first step once you're ready to begin the journey of PCI compliance is to review the four merchant levels (discussed above) to identify what your PCI requirements or action items are to complete. There are different security standards based on what banks you work with and how many transactions you hand. Also, whether or not your business has been a victim of a data breach that compromised cardholder data. Different companies have different standards here—for example, here are MasterCard's, and Visa's criteria for, which describe four and five levels of businesses, respectively. Analyze where you fall, and how your business is described in PCI's general standards so you're ready for the next steps.

2. Complete a Self-Assessment Questionnaire (SAQ)

The self-assessment questionnaire (SAQ) is a relatively painless guidebook you can use to assess your current compliance level. There are actually nine different versions of the SAQ guidebook, but don't let that intimidate you. These versions are available for different business types, so you'll only need to the book that applies to your business. When you have it, the guidebook will walk you through about a dozen different requirements, and for each, you'll answer "yes," "no," or "N/A." This will help you identify the missing pieces of your company's payment security. Most businesses will fall between Merchant Levels 2 – 4, the requirements are relatively same across these levels:

- Complete a Self-Assessment Questionnaire (SAQ)
- Submit an Attestation of Compliance (AOC) form each year
- Complete and obtain evidence of passing a vulnerability scan with an Approved Scanning Vendor (ASV)
- Conduct a quarterly network scan by an ASV

3. Now That You've Completed Your ASV – It Might Be Time to Remediate

You've completed your Self-Assessment Question (SAQ) and done your due diligence in researching PCI standards. Your business is now ready to obtain and provide evidence of passing a vulnerability scan by an Approved Scanning Vendor. If this is your first time completing a ASV, you might find that you have a few items to remediate. Work with your IT team to correct any security vulnerabilities, hardware upgrades, or documentation required to bring your business into full compliance. We've created a 9-Step Approach to Creating an Effective PCI Compliance Remediation Plan plan below to help you get started. Once you've made the necessary changes, it's time to have the ASV rescan and document proof that your organization passed. If remediation was required, take a moment and review your SAQ for accuracy and update as needed.

4. Complete a formal attestation of compliance.

Once you've made any changes necessary and have updated your SAQ, you can fill out a formal attestation of compliance (AOC). This is a formality that claims your business is fully compliant with all relevant PCI standards—and again, there are nine different types based on the nature and size of your business. Once you're done with that, you can have a qualified security assessor review your work and create a report on your compliance to validate your own findings.

5. File the paperwork.

Congratulations – the long hours of research, determination (and possibly some dread), and money spent has paid off. Your business is ready to package up all the paperwork and deliver to the card associations or banks you process payments with. You'll need to submit your SAQ, AOC, proof that you passed your ASV, and any other documentation requested.

HOW MUCH DOES IT COST A BUSINESS TO BECOME COMPLIANT?

As soon as you realize that your business is required to be PCI compliant. Most business owners immediately think – how much is this going to cost my company?

It's a simple question but a difficult one to answer.

The associated cost required to bring your business into full PCI compliance will largely depend on how far behind you are on some of the deferred business items a lot of companies tend to ignore.

For example, if your network is set up in a way that is really far from meeting compliance. It can feel overwhelmingly difficult to get the network compliant. Whereas, if your network is set up correctly in the first place – it may just be a matter of running an internal and external scan, then fixing a couple missing items, like an SSL certificate or closing an open port.

HOW MUCH DOES IT COST A BUSINESS TO BECOME COMPLIANT?

The area that a lot of businesses struggle with is setting the network up correctly from the onset. Segregating areas of your network could be expensive because you may need to replace or upgrade hardware like your firewall or replace your Best Buy purchased 'good enough' routers with business-class switches that will enable you to properly segment your network for better security.

In terms of security, many businesses might fall behind the curve when implementing end-to-end encryption between communication platforms or remote access controls.

For example, if you're forwarding port 3389 so you can access your computer from home while at work then you're probably not PCI compliant. Most routers can forward a port, not every router can support an encrypted connection like a VPN.

If you were to complete an external scan, the scan would spot the open port and this weak link in your security controls would need to be resolved in order to become PCI compliant. Giving an exact cost is virtually impossible because it depends on so many factors specific to your business' environment:

- What is your businesses' PCI scope?
- Does your business utilize File Integrity Monitoring (FIM) software to detect unauthorized access and personnel to unauthorized modification (including changes, additions, and deletions) of critical system files, configuration files or content files?
- Is your business currently using tokenization services, credit card vaulting, point-to-point encryption (P2PE) and/or end-to-end encryption (E2EE) to significantly limit your PCI scope?
- Has your team established and adhere to basic security best practices?
- Does your business have a formal patch management strategy to patch and resolve time-sensitive vulnerabilities quickly?
- Is your IT environment well documented with a complete inventory of all the connections between your cardholder data environment, other networks, and devices?

Aside from how your current IT infrastructure is presently set up, another key factor that will help your business avoid exerting unnecessary time, resources, and expenses is to ensure that your business has accurately determined the scope of the cardholder data environment. Whether leaning on the side of caution or from a lack of understanding of the intricacies of PCI DSS compliance requirements, many businesses over-scope their cardholder data environment which often leads to wasted resources. As you can see the actual cost required to obtain PCI compliance is highly-variable and unique to your business, contact Next Perimeter for a network assessment. We've helped hundreds of companies secure their network, strengthen security controls and implement IT systems or process that to become PCI compliant.

HOW LONG DOES IT TAKE TO BRING A BUSINESS INTO FULL PCI DSS COMPLIANCE?

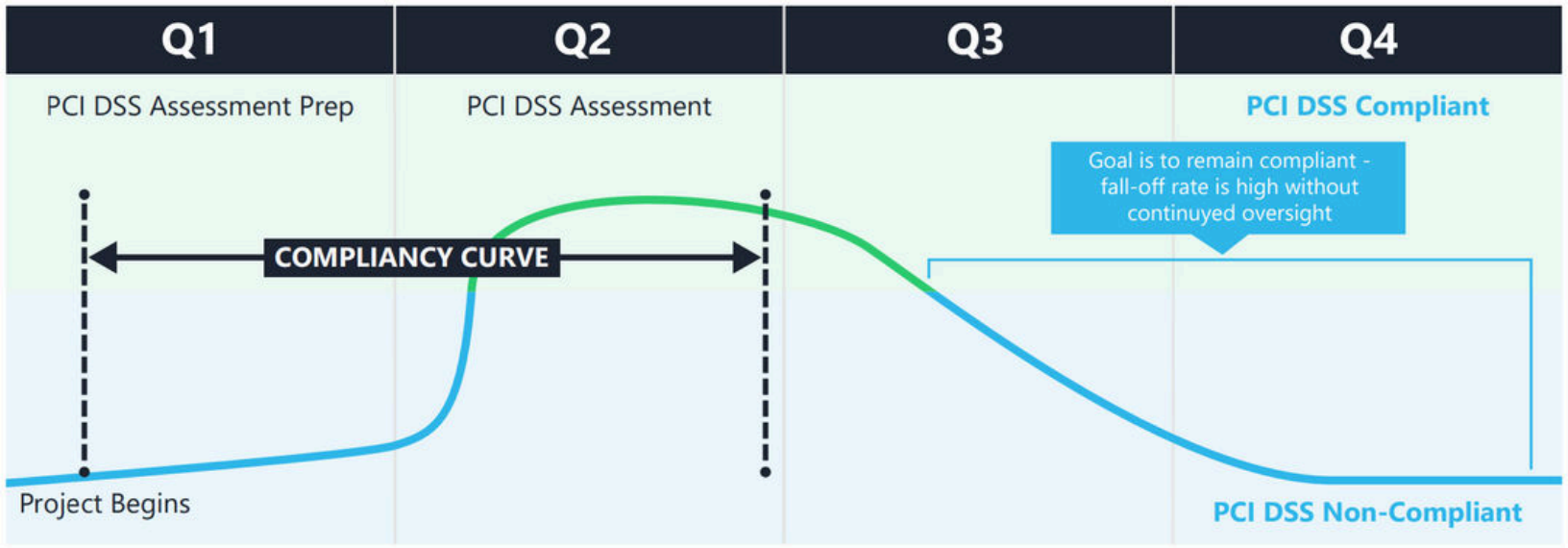
In our experience, most networks that were configured correctly from the start will only require a day's work to bring the business into compliance. Of course, there's training that must be done with relevant personnel so that everyone understands PCI compliance and your now well-optimized strategy to sustain PCI DSS compliance. However, from a technological perspective, minimal work is usually required if your IT environment is up-to-par. By properly configuring your network and operating using IT best practices, you can avoid time-consuming PCI compliance remediation effort down the line.

CHALLENGES TO MAINTAINING COMPLIANCE

Organizations are struggling to maintain PCI DSS compliance. According to a PCI Security Council report released in January, more than 44 percent of companies see the effectiveness of the PCI DSS controls and overall compliance decline after a PCI assessment is completed. This correlates with the three percent compliance decline seen for the first time since Verizon started tracking PCI compliance in 2012. While the cause for declining compliance is myriad the PCI Security Council outlines five common reasons that businesses begin dropping out of PCI compliance:

1. The digital age and technology continue to evolve at breakneck speeds. Pressures to adapt to ever-increasing customer demands and emerging technologies and the resulting changes to an organization's business goals, structure, and technology infrastructure.
2. Organizational complacency, assuming what was good enough last year will be good enough in future
3. Overconfidence in organizational practices, resulting in a lack of resources devoted to regular monitoring, detection, tracking, or an effective employee training program can push business out of compliance.
4. Inability to assign the right people, tools, and processes, and lack of executive leadership commitment to maintaining
5. Failure to accurately scope the organization's cardholder data environment (CDE) as business practices evolve with the introduction of new products or services,

Businesses that focus solely on annual PCI DSS assessments to validate the quality of their cardholder data security programs are missing the intent of PCI DSS to enhance cardholder data security, and likely see their PCI DSS compliance state "fall off" between assessments. In order to maintain a consistent level of security and compliance, organizations should focus on implementing an effective physical and digital security posture with integrated security monitoring, threat detection and prevention systems that work cohesively to secure the IT environment as a whole instead of solely on "meeting compliance."



HOW MUCH COULD FAILING PCI COMPLIANCE COST YOUR BUSINESS?

According to Verizon's Payment Security Report 47.5% of businesses assessed did not meet full compliance. If your business does not comply with PCI standards, you could be at risk for data breaches, fines, card replacement costs, costly forensic audits and investigations into your business, brand reputation damage, and more. Standard fines and penalties imposed by Payment Card Brands for card data breaches take into consideration the following:

- Number of card numbers stolen
- Circumstances surrounding the incident
- Whether track data was stored or not
- Timeliness of reporting incident

HOW MUCH COULD FAILING PCI COMPLIANCE COST YOUR BUSINESS?

Although PCI compliance is not a law but rather a set of standards established and regulated by the major card brands, if your business is not compliant you might expect any one or all of the following scenarios:

PCI NONCOMPLIANCE FEE:

Most payment processing companies will charge a PCI non-compliance fee if your business does not fulfill all the PCI DSS requirements, such as not submitting the annual Report on Compliance (ROP) or Self-Assessment Questionnaire (SAQ), Attestation of Compliance (AOC), or proof that you've passed your vulnerability scans completed by an Approved Network Scan (ANS) service provider. Non-compliance fees are largely dependent on your Merchant Service Provider's terms and conditions but can range from $10 – $45 (or more) for each month out of compliance. The card brand can also levy fines which we discuss below.

PCI NONCOMPLIANCE FINE:

If a security breach occurs, and consumer credit card data is leaked or compromised AND your records indicate non-compliance; you might end up being fined $5,000 to $100,000 per month by the credit card associations.

PCI FINES FOR STORING SENSITIVE AUTHENTICATION DATA:

Up to $100,000 per month. Sensitive authentication data includes full track data (magnetic-stripe data or equivalent on an EMV chip), CAV2/CVC2/CVV2/CID, PINs and PIN blocks.

PCI NONCOMPLIANCE & REVOCATION:

If non-compliance persists and/or credit card data is compromised due to a sheer amount of negligence or sloppy IT infrastructure, your acquiring bank may revoke your ability to accept credit cards, and place you on a merchant account blacklist (Match List – see below) which could effectively end your ability to do business.

Other financial implications in the event of a data breach affecting card data:

- Fines levied by card associations to make notifications to all cardholders and replace credit cards
- Costs of notifying taxpayers of an incident, as directed by the Identity Theft Protection Act
- Forensic Investigation Costs
- The cost associated with discontinuing accepting cards
- Cost of an annual on-site security compliance audit estimated $20,000 every year

- Business reputational damage – probably the most significant side effect of a data breach is the loss of trust by consumers. If your customers cannot trust your business to keep their data safe, you might find that they simply switch brands or take their hard-earned money to one of your competitors. According to Verizon's Data Breach Report, 69 percent of consumers would be less inclined to do business with a breached organization.

WHAT IS THE TERMINATED MERCHANT FILE OR MASTERCARD MATCH LIST?

Merchant accounts (read businesses) that partake in fraudulent practices, receive excessive chargebacks or consumer complaints, or unintentionally facilitated, by any means, the unauthorized disclosure or use of account information may find themselves on the Terminated Merchant File (TMF) or MATCH (Member Alert to Control High Risk Merchants) List.

MATCH is a system created and managed by Mastercard which essentially is a 'merchant blacklist' database that contains information about businesses (and their owners) whose credit card processing privileges have been terminated.The MATCH list not only affects the principal business owner – when a business is placed on the MATCH list, the business name, principal and any business partners are recorded on this blacklist. If you end up on this blacklist, you might find it extremely difficult to obtain a new merchant account by any other bank.

If you are able to find a merchant service provider that is willing to work with a business on the MATCH list, you will likely experience higher interchange rates and additional fees to mitigate the risks associated with your lack of compliance or less-than-ideal past business practices. While the MATCH list uses codes to categorize the conditions and practices that resulted in a merchant being added to the MATCH list, it is a system largely without any checks and balances. MasterCard's own words clearly state that they do not verify or confirm the accuracy of the information reported, from section 11.1 of their MATCH Overview:

The best way to prevent find yourself on the MATCH list is to ensure that your business is PCI compliant, adheres to cybersecurity best practices, follow your card brand's term of service, and avoid any risky transactions or unethical business practices. Review the table below to understanding how merchants are categorized on MasterCard's MATCH List:

"MasterCard does not verify, otherwise confirm, or ask for confirmation of either the basis for or accuracy of any information that is reported to or listed in MATCH. It is possible that information has been wrongfully reported or inaccurately reported. It is also possible that facts and circumstances giving rise to a MATCH report may be subject to interpretation and dispute."

The best way to prevent find yourself on the MATCH list is to ensure that your business is PCI compliant, adheres to cybersecurity best practices, follow your card brand's term of service, and avoid any risky transactions or unethical business practices.

MATCH List Reason Code	Title	Explanation
01	Account Data Compromise	Account data is stolen from the card-present merchant and used with other merchants
02	Common Point of Purchase	Account data is stolen from the card-present merchant and used with other merchants
03	Laundering	The merchant processed transactions that did not involve a bona fide cardholder
04	Excessive Chargebacks	The merchant breached predetermined chargeback thresholds

MATCH List Reason Code	Title	Explanation
05	Excessive Fraud	The merchant breached predetermined fraud-to-sales dollar volume thresholds
06	MasterCard Questionable Merchant Audit Program	The merchant is labeled a “Questionable Merchant,” as determined by MasterCard guidelines
07	Bankruptcy, Liquidation, Insolvency	The merchant is unable to discharge all financial obligations
08	Violation of Standards	The merchant was in violation of one or more of the card network’s regulations
09	Merchant Collusion	The merchant participated in fraudulent collusive activities
10	**PCI DSS Noncompliance**	**The merchant wasn’t compliant with PCI DSS requirements**
11	Illegal Transactions	The merchant processed illegal transactions
12	Identity Theft	The business owner’s identity is in question

PCI DSS COMPLIANCE REMEDIATION

A readiness assessment from a Qualified Security Assessor (QSA) will likely uncover gaps in PCI compliance that will need to be addressed before a formal PCI review. If a QSA identifies compliance issues during the readiness assessment, you may be able to address some of those issues by reviewing and minimizing your scope of compliance, but existing issues will have to be properly remediated to comply with PCI DSS standards.

After the QSA conducts a readiness assessment, you can expect the assessor will work with your business to:

- identify and explain any existing gaps in compliance;
- develop a remediation plan, including technical fixes and policy and procedural updates; and recommend tools or third parties that can help complete the necessary technical and policy work.

It's important to note that the PCI Security Standards Council has implemented controls to prevent a conflict of interest, due to strict requirements regarding "separation of duties", a QSA cannot conduct remediation efforts identified during a readiness assessment. A QSA can, however, recommend a third-party to assist in the remediation and fill gaps identified by the QSA.

OUR 9-STEP APPROACH TO CREATING AN EFFECTIVE PCI COMPLIANCE REMEDIATION PLAN

01 | PLAN AHEAD

Removal efforts can be lengthy and difficult for all parties involved; with the gaps in compliance recognized, it is very important to outline and also settle on a workable remediation strategy at the start.

02 | GET ORGANIZED

We recommend growing your remediation tasks into categories; both key categories being technological and policy/procedural. You may need to update server configurations, install a business firewall, or develop brand-new plans and procedures, etc. Creating an effective well-organized PCI compliance remediation plan will save your team time, money, and potential frustration throughout the process.

03 | ASSIGN RESPONSIBILITIES

Identify the teams and stakeholders responsible for the ownership of all remediation efforts, requirements and milestones required to bring these areas of responsibility into compliance. In this step, business owners need to identify any additional tools, resources or outside providers such as a Managed Service Provider that specializes in PCI compliance.

04 | REVIEW REMEDIATION TOOLS AND SERVICES

The QSA that completed your readiness assessment can help you identify open-source compliance tools to avoid costs from adding up quickly. Your QSA can also help you to identify different information-security plan templates to speed up the remediation efforts, as well as offer industry-specific expertise if available. Likewise, it's always wise to outsource security initiatives to specialists with the background and expertise to give your business a fighting chance in a rapidly changing threat landscape.

05 | BUDGET. BUDGET.

Even though the cost of non-compliance far exceeds the initial investment to ensure your business meets PCI compliance each year. Costs can quickly add up – between potentially being required to purchase new POS hardware, buying a more robust server, security software, acquiring additional user licenses to prevent concurrent access, working with an outside IT firm, and relevant third-party subscriptions, the cost of compliance can quickly get out of hand.

OUR 9-STEP APPROACH TO CREATING AN EFFECTIVE PCI COMPLIANCE REMEDIATION PLAN

[*cont.]* By completing all your research before starting any remediation efforts, your team will be able to craft an accurate budget and minimize the scope creep that is far too common in projects of this nature. accurate budget and minimize the scope creep that is far too common in projects of this nature.

06 | SET. REMEDIATE!

Set a time frame for remediation efforts. Tighten up network's defenses, lock down sensitive data, complete your security documentation, and get ready for your QSA review.

07 | TEST AND VERIFY

Your team can see the end of the tunnel, now test each in-scope component to verify that each system and your updated processes/procedures meet PCI compliance.

08 | CONTACT THE QSA FOR A FORMAL PCI REVIEW

If your team has resolved each recommendation from the readiness assessment, this should be a fairly straight forward process to confirm you're now PCI compliant.

09 | STAY PCI COMPLIANT.

Congratulations! You're now officially PCI compliance, the work doesn't stop here. Business security and compliance is a fluid objective – moving forward be sure to assign responsibilities and follow through with your up-to-date compliance strategies. Don't forget to inspect and test your systems regularly according to your continuing compliance plan.

PCI COMPLIANCE AND HOSPITALITY

– ARE YOU PART OF THE 38.5% THAT MADE FULL COMPLIANCE?

The hospitality industry needs personal data to successful – but that comes with a price. According to the HTFP Journal, it was the most affected vertical in the last years, obtaining an entire 40% of all data breaches that happen worldwide.

Hotels, spas, and high-end resorts seek to provide 5-star interconnected hyper-personalized experiences to delight customers, hopefully creating lifetime loyal patrons. Underlying this need for more personal information, hotels and resorts have specific needs for booking or payment purposes, like cardholder data, passport numbers, and driver's license information. Yet, the reality is that the hospitality industry is struggling with securing personal data and PCI compliance.

In fact, Verizon reports that only 38.5 percent of hospitality organizations demonstrated full PCI compliance. The lowest compliance sustainability of all industries measured.

The Marriot/Starwood data breach is thought to be the third-largest data breach in recorded history with an estimated 500 million guest records (Yahoo! captured first and second place by total of accounts compromised). Marriot's compromised data includes names, mailing addresses, phone numbers, email addresses, passport numbers, dates of birth, gender, Starwood Preferred Guest loyalty program account information, arrival and departure times, and reservation dates. What's most concerning is that Marriot is the top hotel provider for the American government and military personnel.

In recent news: in the middle of October vpnMentor's cybersecurity team alerted AutoClerk of an open database exposing records containing the sensitive data of hotel customers as well as US military personnel and officials. AutoClerk is a reservations management, a service owned by Best Western Hotels and Resorts group. AutoClerk is used by resorts to manage online bookings, guest profiles, payment processing, loyalty programs, and revenue. According to vpnMentor, hundreds of thousands of booking reservations were available online in an open Elasticsearch database, data ranging from full names, date of birth, phone numbers, and masked credit card numbers to travel costs, check-in times and room numbers. All of this data was available online without any security barriers or encryption.

Just these two incidents taken together, highlight exactly why penetrable security or lacking foundational security best practices in the hospitality sector threatens consumer privacy, shareholder value, and even national security.

If two international multibillion-dollar organizations can be hacked and lack the operational maturity to secure their IT infrastructure, how vulnerable are small and midsized operations without the security resources, budget, and specialized personnel?

Verizon's 2019 Data Breach Investigations Report, states 43% of cyberattacks target small businesses, will continue to increase as cybercriminals turn to easier targets to steal sensitive customer data. According to the third Hiscox Cyber Readiness Report, the number of businesses reporting cyber incidents has gone up from 45% last year to 61% in 2019.

Facing a changing regulatory landscape designed to heighten responsibility by threatening fines, many hospitality companies are reconsidering their cybersecurity infrastructure. However, industry-specific challenges like high-employee turnover, vendor risks from connected third-party systems, franchise and chain compromises, and the vast array of systems or software available continue to expose this sector as a lucrative target for hackers.

Next Perimeter works with high-end luxury beachside resorts to local historic bed and breakfasts to major hotel operators serving thousands of rooms across multiple locations. We provide the hospitality industry with the peace-of-mind and security stakeholders need to ensure your team can capture and protect the personal data required in today's market to deliver an amazing experience that creates loyal lifetime customers

Helpful Links and Resources:

1. PCI Security Standards Council Website
2. PCI Security Standards searchable database of Approved Scanning Vendors
3. You can download the latest version of the PCI Councils Self-Assessment Questionnaire

FINAL THOUGHTS

For any business that accepts credit or debit cards, PCI Compliance is unavoidable. You need to be PCI compliant. This isn't just a matter of complying with a bureaucratic regulatory requirement or avoiding PCI non-compliance fees. A data breach that exposes your customers' cardholder data can have a catastrophic effect on your business.

A secure and strategic IT architecture is required to protect your customers, partners and brand reputation.

When you're ready to achieve and maintain PCI compliance, Next Perimeter can help.

To assist your team, we've created a list of essential questions when evaluating an MSP as your strategic partner.

TOP QUESTIONS TO ASK

WHEN EVALUATING AN MSP AS YOUR STRATEGIC PARTNER

EXPERIENCE

- [ ] How many managed services customers do you have in total?
- [ ] What is your "sweet spot" for customer size?
- [ ] How many customers do you have that are our size?
- [ ] How many endpoints do you manage?
- [ ] How many people are on your service delivery team?

VALUE

- [ ] How do you help customers save money and lower IT costs?
- [ ] How do you help customers plan for the future?
- [ ] In what situations will you advise customers to purchase technology that you don't sell?
- [ ] How do you help customers identify and mitigate vulnerabilities before problems occur?

SERVICE OFFERINGS

- [ ] What services are included in your managed services offerings?
- [ ] Do you incorporate security into your managed services offerings?
- [ ] What technologies do you support?
- [ ] What security services do you offer?
- [ ] Do you offer any IT compliance services?
- [ ] What cloud platforms do you support?
- [ ] What SLAs do you offer for incident response, and what is your SLA compliance rate?

NEXT PERIMETER

TOP QUESTIONS TO ASK

WHEN EVALUATING AN MSP AS YOUR STRATEGIC PARTNER

CUSTOMER SATISFACTION

- [ ] How do you measure customer satisfaction?
- [ ] What is your annual managed services customer churn rate?
- [ ] What is your customer satisfaction performance for the past 12 months?

OPERATIONAL EXCELLENCE

- [ ] What metrics and reports do you share with customers to demonstrate the status of their environment and incident response effectiveness?
- [ ] What's different or unique about your systems management approach?
- [ ] Are your support tools integrated into a single dashboard?
- [ ] What is the number of daily incidents resolved automatically by proprietary automation?
- [ ] How do you audit patch status and remediate vulnerabilities?
- [ ] How do you measure and report the success rates for backups?
- [ ] What is the first-call resolution rate for calls to the help desk?
- [ ] Is your organization SOC 2-certified?
- [ ] How do you ensure that technicians are knowledgeable about customer environments?
- [ ] How do you ensure knowledge is not lost when staff leaves?
- [ ] Do you adopt ITIL or similar excellent practices around IT service delivery?
- [ ] How many backups are successfully performed daily?
- [ ] How do you know they are successful?

NEXT PERIMETER

WHAT SETS US APART?

It All Starts in the Cloud

Your .com is what ties your business to the web, allowing you to get your email and collaborate online. Whether you're using Google Workspace or Microsoft 365, **Next Perimeter** has you covered. Your team can leverage our certified experts for matters concerning your email deliverability, DNS records, licensing concierge, and more.

Your Team and Workstations are Fully Covered

When your team logs into your corporate environment today, what types of protections exist? **Next Perimeter**, by default, deploys endpoint security and hardware monitoring to every workstation that we manage, ensuring productivity is at an all-time high. Your team will enjoy unlimited round-the-clock support for everyday issues ranging from authentication to hiccups with their equipment.

Battle-Tested SOPs

Whether we will handle all of your IT, or collaborate with an internal team, our procedures have been perfected against millions of business scenarios. Our system has been trained to adapt to each customer as their organizations evolve.

Future-Proofed for Compliance

We know you want your cybersecurity to be reliable, predictable, functional, and cost-effective - that's why we've simplified cyber so it's back-of-mind. By signing up for Essentials, you've created a predictable path toward future compliance needs as our agents can fulfill virtually all requirements they might ask for with simple per-user/device pricing.

NEXT PERIMETER

Let's Work Together

Phone
888-286-4816

Mail
sales@nextperimeter.com

Website
NextPerimeter.com

About Us

As a leader in cloud-first cybersecurity and IT support, Next Perimeter protects businesses from modern threats, whether in the office or remote. Our Zero Trust architecture and SaaS posture management deliver a secure, optimized endpoint experience without the need for servers or office space.

Our SASE network as a service replaces traditional VPNs with an always-on, secure connection, ensuring high-speed, reliable network security across the globe. Specializing in holistic threat detection and response, we safeguard your digital assets with cutting-edge AI-powered solutions.