Starting Your PCI Compliance Journey

A GUIDE TO ACHIEVE AND MAINTAIN
PCI COMPLIANCE

pcipal

Safeguarding reputations and trust

Table of contents

A Beginner's Guide to PCI DSS	04
PCI DSS v4.0	07
Merchant Levels	11
Which SAQ is Right for You?	13
What is a QSA?	16
Multi-Factor Authentication	20
Point-to-Point Encryption	22
Tokenization	25
Your Annual PCI Checklist	26
PCI Glossary	30

A Beginner's Guide to PCI DSS

The Payment Card Industry Data Security Standard (PCI DSS) is a set of requirements that are designed to protect sensitive cardholder data wherever it is stored, processed or transmitted. These requirements apply to any organization that handles card payments in any capacity.

If you work for a company who takes card payments from customers, you are responsible for keeping that data as safe and secure as possible – not just to protect your customers but to protect your business as well.

HISTORY OF PCI DSS

Prior to 2004, each major credit card brand (Visa, Mastercard, JCB, American Express, Discover Financial Services, and UnionPay) had their own sets of policies and standards that organizations were expected to follow as a way of ensuring organizations had a minimal level of security when it came to handling sensitive payment data.

In order to mitigate the complexity of having multiple standards to adhere to, the credit card brands got together in 2004 and released the first version of the PCI DSS. Two years later, the PCI Security Standards Council (PCI SSC) was formed as a governing entity for the PCI DSS.

There are a number of private organizations who participate in the development of the PCI DSS by registering for and joining special interest groups (SIGs). Each participating organization can contribute to the activities which are mandated by that special interest group.

The 12 Standards of PCI DSS

The PCI DSS is a set of 12 standards which apply to any organization who stores, processes and transmits credit card details from the major card schemes. The twelve core standards as laid out by the PCI SSC are:

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
3. Protect stored cardholder data
4. Encrypt transmission of cardholder data across open, public networks
5. Use and regularly update anti-virus software or programs
6. Develop and maintain secure systems and applications
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
10. Track and monitor all access to network resources and cardholder data
11. Regularly test security systems and processes
12. Maintain a policy that addresses information security for employees and contractors

The Risks & Penalities of Non-Compliance

While PCI DSS compliance is not a legal requirement, it is mandatory if your organization wants to process transactions with the major card schemes.

If a system is compromised and the company is found not to be PCI DSS compliant, the business could face severe penalties, such as:

- brand damage & job losses
- lawsuits and legal costs
- a drop in share price
- insurance claims & regulator fines
- higher banking fees
- potentially, the ability to accept card payments being revoked

These, coupled with the fraud losses, the cost of replacing cards, loss of customer confidence, and the ensuing decrease in sales can all lead to a company suffering huge financial losses.

In 2021 luxury retailer, Neiman Marcus, was the victim of a data breach that exposed personal and financial information contained in the online accounts of approximately 4.6 million customers.

Customers' names, contact information, payment card numbers and expirations dates (without CVV), virtual giftcards, usernames, passwords, security questions, and answers were compromised in the hack.

The Dallas-based chain's breach ended up costing $1.5 million in settlement fees with 43 state attorneys. As part of the multistate settlement, Neiman Marcus has agreed to several injunctive provisions aimed at preventing similar breaches in the future, including complying with PCI DSS requirements.

PCI DSS v4.0

The first release of the PCI DSS (v1.1) was in 2004. At only 12 pages long and with a strong focus on the recording and storage of credit card data, it's very different from today's PCI DSS v4.0, which recently replaced PCI DSS version 3.2.1. The newest evolution of the standard aims to address emerging threats and technologies better and provide innovative ways to combat new threats by achieving four goals:

1. Continue to meet the security needs of the payment industry
2. Promote security as a continuous process
3. Add flexibility for different methodologies
4. Enhance validation methods

The 12 requirements of the PCI DSS have remained a constant throughout all versions. As it has evolved, more details on how organizations should achieve and maintain PCI compliance have been added. The size and type of organization will determine the process, but it can largely be broken down into six key areas:

SCOPE - determine which system components and networks are in scope for PCI DSS

ATTEST - complete the appropriate Attestation of Compliance (AOC)

ASSESS - examine the compliance of system components in scope following the testing procedures for each PCI DSS requirement

SUBMIT - submit the SAQ, ROC, AOC and other requested supporting documentation to the acquirer (for merchants) or to the payment brand/ requestor (for service providers)

REPORT - assessor and/or entity completes required documentation, including documentation of their custom approach

REMEDIATE - if required, perform remediation to address requirements that are not in place, and provide an updated report

Steps to Compliance

The first step in becoming PCI compliant is to determine where credit card data is present within your organization, the cardholder data environment (CDE). This is comprised of the people, processes, and technologies that handle cardholder data or sensitive authentication data.

PEOPLE

The PCI DSS recognizes that people are the biggest threat when it comes to the security of credit card data. As organizations expand their digital and payment channels, the risk of data breaches and cybercrime against sensitive consumer data increases.

Organized crime is moving towards Cardholder Not Present (CNP) channels as other areas become more secure. It comes as little surprise therefore, that cyberattacks have increased exponentially since 2020.

The threat from people can be intentional, accidental, external or internal. For example, criminals can access software and systems externally, or they can trick staff who have access to sensitive payment card data to unknowingly give up this information in numerous ways (e.g. phishing emails, posing as consumers, etc.).

Additionally, the pandemic exposed a significant risk of internal staff stealing credit card data when operating in a remote environment as it is difficult to

ensure their employees are working in environments that minimize the potential of exposure.
Key PCI DSS requirements to consider: 1, 2, 3, 7, 8, 9, 10, 12

PROCESS

PCI DSS does not only refer to card processing. It also covers the end-to-end journey where payment card data is present in an organization and the processes involved. This can range extensively from a simple payment terminal through to multiple digital and telephone-based payment channels in a large contact center.

In order to understand which processes are in scope of PCI DSS, we must first understand and differentiate types of account data, which is all the information on a credit card.

Organizations are prohibited from storing Sensitive Authentication Data such as the security code (CVC/CVV) and PINs and in instances where it needs to be recorded, it must be rendered unrecoverable after authorization. Cardholder data such as Primary Account Number (PAN) and expiration date can be stored but under strict conditions.

For example, the PAN can only be partially visible and should also be unrecoverable if stored. Each of the PCI DSS requirements are pertinent to the payment process. As such, organizations should map and assess all processes against each of the twelve standards.
Key PCI DSS requirements to consider: All

TECHNOLOGY

The evolution of how we pay for goods and services has been the driving force behind subsequent versions of the PCI DSS and has shaped the shift in focus from the storage and recording of card data in the early years, to the technologies involved in accepting card payments we see today. Who would have envisioned in 2004 that it would be possible to pay for goods with a tap of a watch or a phone on a card terminal?

Where the twelve requirements have been consistent, elaboration and clarification have been added to ensure organizations are aware of how technology is vital not only in the payment process itself, but also as a way of securing the data across all business communication channels.
Key PCI DSS requirements to consider: 1, 3, 4, 5, 6, 8, 10, 11

Proving PCI Compliance

Achieving and maintaining PCI compliance depends on the size and type of organization. Broadly speaking, organizations can be split into two categories; Merchants and Payment Service Providers **(PSPs).**

These are then subcategorized based on criteria set by the PCI SSC. This will determine how PCI compliance should be evidenced, either by:

- Self Assessment Questionnaires (SAQs)
- Annual audits by a Qualified Security Assessor (QSA) along with supporting documentation, such as Report On Compliance (ROC) or Attestation of Compliance (AoC)

MERCHANT LEVELS DEFINED

There are four different categories that your organization may fall into, defined primarily by the number of transactions you process, but also by perceived additional security risks.

These criteria allow the PCI SSC to determine the risks your customers might face when transacting with you, and therefore, determines which level of security they need to enforce in order to improve payment security.

The following guidelines will help you decide which merchant level applies to you and which steps you need to take to ensure PCI DSS compliance.

Merchant PCI DSS Levels

LEVEL	BUSINESS CRITERIA	PCI DSS REQUIREMENTS
4	• Merchants processing less than 20,000 Visa or Mastercard e-commerce transactions annually • All other merchants processing up to 1 million non-ecommerce transactions annually	• These largely depend on the requirements of the merchant's acquiring bank • Typically include an SAQ and quarterly network scan by an ASV
3	• Merchants processing between 1 million and 6 million Visa, Mastercard, or Discovery transactions per year via any payment channel • Merchants processing between 50,000 to 2.5 million American Express transactions annually • Merchants processing less than 1 million JCB transactions annually	• Annual Self-Assessment Questionnaire (SAQ) (Mastercard requires merchant staff to be ISA certified or use a QSA for an onsite assessment) • Quarterly network scan by Approved Scanning Vendor (ASV)
2	• Merchants processing between 20,000 and 1 million Visa and Mastercard e-commerce transactions annually • Merchants that process 20,000 to 1 million Discover card-not-present only transactions annually • Less than 50,000 American Express transactions annually	• Annual Self-Assessment Questionnaire (SAQ) • Quarterly network scan by ASV • Attestation of Compliance (AoC) form
1	• Merchants processing more than 6 million Visa, Mastercard, or Discover transactions annually via any payment channel • Merchants processing more than 2.5 million American Express transactions annually • Merchants processing more than 1 million JCB transactions • Merchants that have suffered a data breach or cyberattack that resulted in cardholder data (CHD) being compromised • Merchants identified by another card brand as Level 1	• Annual Report on Compliance (RoC) by a Qualified Security Assessor (QSA) (or ISA accredited staff member for Mastercard) • Quarterly network scan by Approved Scanning Vendor (ASV) • Attestation of Compliance (AoC) form

Payment Service Providers

For Payment Service Providers (PSPs), there are only two levels:

Level 1 - If a service provider processes, stores and/or transmits transactions for JCB, or **more than 300,000** Visa, Mastercard, American Express or Discover transactions, they must obtain an annual RoC prepared by a QSA and undergo quarterly vulnerability scanning by an ASV.

Level 2 - If the service provider processes, stores and/or transmits **fewer than 300,000** Visa, Mastercard, American Express or Discover transactions, they must validate their PCI compliance by way of SAQ and undergo quarterly vulnerability scans by an ASV.

Once an organization understands which of these categories it falls into, it can then determine how to prove its compliance with the PCI DSS. For most organizations, this will be completion and submission of Self-Assessment Questionnaires (SAQ).

Which Self-Assessment Questionnaire (SAQ) is Right for You?

If your organization processes fewer than 6 million transactions annually, you may be able to evidence PCI compliance via a Self-Assessment Questionnaire (SAQ). The very first step towards correct completion is to choose the right SAQ.

Organizations come in all shapes and sizes. This is why a range of SAQs has been developed to suit a variety of business types.

Which SAQ is correct for you?

SAQ A

Who is it for?

Cardholder-Not-Present (CNP) merchants that have fully outsourced all cardholder data functions to PCI DSS validated third-party service providers, with no electronic storage, processing, or transmission of any cardholder data on the merchant's systems or premises.

Actions Required:

- Paper copies of cardholder data must be destroyed or protected
- Details of third-party service providers must be kept
- Compliance of third-party services must be monitored
- Completion of SAQ A (22 questions)

SAQ A-EP

Who is it for?

E-commerce merchants who outsource all payment processing to PCI DSS validated third parties, and who have a website(s) that doesn't directly receive cardholder data but that can impact the security of the payment transaction. No electronic storage, processing, or transmission of any cardholder data on the merchant's systems or premises.

Actions Required:

- Any e-commerce merchant formerly using SAQ A should read guidelines to identify whether they should now complete the new SAQ A-EP form instead
- Completion of SAQ A-EP (193 questions)

SAQ B

Who is it for?

Merchants using only imprint machines with no electronic cardholder data storage.

Actions Required:

- Ensure terminals (which can now connect via Bluetooth, Ethernet and GSM/LTE) are isolated from networks and therefore not putting cardholder data at risk
- Completion of SAQ B (41 questions)

SAQ B-IP

Who is it for?

Merchants without electronic cardholder data storage who process payments via standalone PTS-approved point-of-interaction (POI) devices which have IP connections to payment processors. This type of transaction can take place in person or via MOTO.

Actions Required:

- Ensure POI devices are isolated from other networks
- Paper merchant receipts must be the only type of cardholder data retained.
- Completion of SAQ B-IP form (84 questions)

SAQ C

Who is it for?

Merchants with payment application systems connected to the Internet, no electronic cardholder data storage.

Actions Required:

- Ensure the technology used to enter cardholder details is isolated from other networks and is strongly protected
- Completion of SAQ C (162 questions)

SAQ C-VT

Who is it for?

Merchants who manually enter a single transaction at a time via a keyboard into an Internet-based virtual terminal solution that is provided and hosted by a PCI DSS validated third-party service provider. No electronic cardholder data storage.

Actions Required:

- Ensure the technology used to enter cardholder details is isolated from other networks and is strongly protected
- Completion of SAQ C-VT (79 questions)

SAQ D

Who is it for?

All merchants not included in descriptions for the above SAQ types.

Actions Required:

- Vulnerability scans and penetration testing required
- Completion of SAQ D which includes all 329 PCI DSS requirements, marking non-applicable sections with caution

SAQ D (Service Providers)

Who is it for?

All service providers defined by a payment brand as being SAQ- eligible, processing less than 300,000 transactions per year

Actions Required:

- Vulnerability scans and penetration testing are required
- Completion of SAQ D (all 329 PCI DSS requirements), marking non-applicable sections with caution. Additional 'Service Provider Only' requirements are identified within the PCI DSS

SAQ P2PE-HW

Who is it for?

Merchants using only hardware payment terminals that are included in and managed via a validated, PCI SSC-listed P2PE solution, with no electronic cardholder data storage.

Actions Required:

- All data must be entered via a validated P2PE hardware device. No vulnerability scan or penetration testing required
- Completion of SAQ P2PE-HW (33 questions)

What is a Qualified Security Assessor (QSA)?

A Qualified Security Assessor (QSA) is an impartial third party hired by a merchant to conduct an assessment and offer advice on how it can become compliant with the Payment Card Industry Data Security Standard (PCI DSS).

THE ROLE OF A QSA

The involvement of a QSA depends on the merchant level. All merchants fall into one of four merchant levels based on their credit card transaction volume over a 12-month period. Level 3 and 4 merchants will not necessarily need the assistance of a QSA to be PCI compliant. Level 1 merchants will require an on-site assessment and an annual Report on Compliance (ROC) completed by a QSA. During the PCI assessment, the QSA will determine whether the organization has met the 12 PCI DSS requirements before completing a ROC.

BECOMING A QSA

To qualify as a QSA, an individual must meet information security education requirements and receive appropriate training from the PCI Security Standards Council. They must also be full-time employees of an approved

Having a QSA conduct a gap analysis as a starting point to establish what the business is currently doing against the PCI DSS allows for any areas found non-compliant to be addressed ahead of an audit.

PCI security and auditing firm and be re-certified annually.

Because the quality of PCI DSS validation assessments can have a significant impact on the application of the security measures and controls, the qualification requirements they must meet are demanding and detailed. Once an applicant has been accepted by the PCI SSC, they then have to complete the two-day QSA training course and pass an open-book exam, then they will receive official certification.

INTERACTING WITH INTERNAL SECURITY ASSESSORS

Internal Security Assessor (ISA) sponsor companies are organizations that have been qualified by the PCI SCC and are intended to aid your compliance processes and provider internal insight. The council runs an ISA Program, which gives employees of ISA sponsor companies the opportunity to receive training and earn a qualification. The aim of this training is to improve an organization's understanding of PCI DSS and the requirements they must meet to be compliant.

It will also help to improve interactions with QSAs and enhance the reliability, quality and consistency of PCI DSS self-assessments.

Choosing a QSA

As in any profession, there can be considerable differences between the technical skills of individual QSAs, so ultimately the security of your card payments is only as good as your assessor.

There are three questions you should ask to give your organization the best chance of hiring a reputable and thorough QSA:

1. WHAT TYPE OF ORGANIZATIONS HAVE THEY PERFORMED PCI DSS ASSESSMENTS FOR?
The type of organization a QSA has worked for in the past is important because the payment card processing equipment and applications tend to vary from sector to sector. Using an assessor with prior experience in your industry can improve the level of security guidance provided.

2. WHAT IS THEIR BACKGROUND?
The experience and background of the QSA depends on the aspects of PCI DSS compliance you wish to improve.

3. WHO WILL BE CARRYING OUT THE WORK?
It can be the case that you have discussions with a particular QSA to ascertain their suitability, only for a different QSA to carry out the work. Make sure the assessor you have been talking to is the same assessor who arrives on site.

“Delivering secure and compliant payment and communications services is more vital than ever for organizations, caught as they are in the grips of both tightening regulations and consumer demand for trustworthy services.”

Geoff Forsyth | PCI Pal

Multi-Factor Authentication

Prior to 2018, Multi-Factor Authentication (MFA) was only required for remote access to any Cardholder Data Environment (CDE). With the introduction of PCI DSS v4.0 however, Multi-Factor Authentication will soon be mandatory for all access into the cardholder data environment as part of the expansion of Requirement 8 of the PCI DSS. With these measures being such an important part of CDE security, here's everything you need to know about multi-factor authentication.

WHAT IS MFA?

MFA is simply a security system that requires more than one type of identification or authentication before allowing user access.

The term can refer to two-factor authentication or higher and must include different types of factors. The forms of authentication required usually encompass knowledge, possession and inherence, i.e. something the user knows, something they possess and something they are. Examples of these include:

Knowledge – a password, login number, username or PIN.

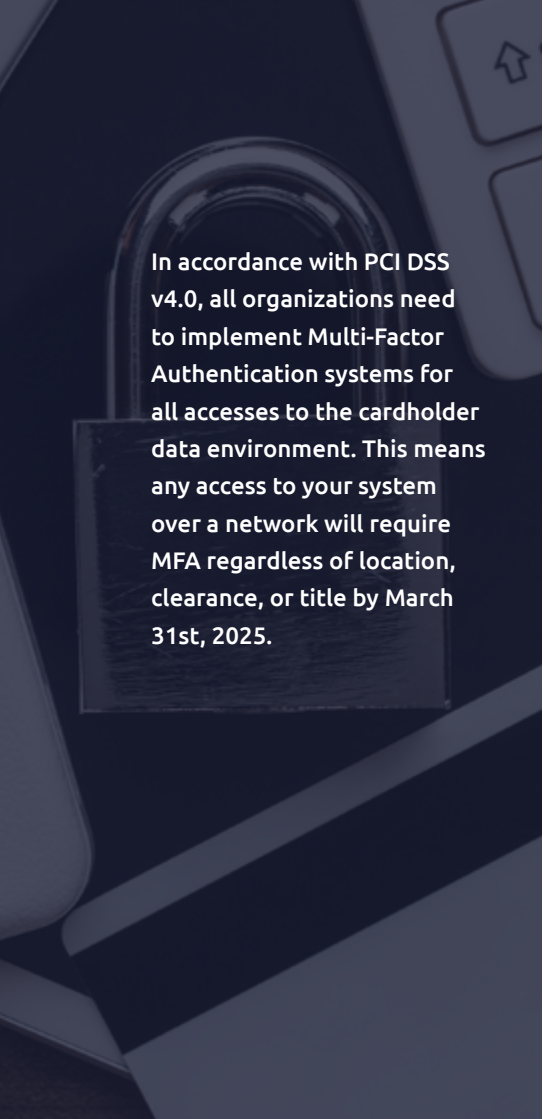
Possession – a physical object, such as a key, swipe card or token.

Inherence – biometric identifications, such as fingerprints, iris scans or voice recognition.

WHY IS MFA USEFUL?

The idea behind Multi-Factor Authentication is that it simply makes accessing sensitive data more difficult, providing potential hackers with more barriers than just a password.

By requiring several, separate identification factors consisting of at least two different types of forms, the system is less easily compromised, making Cardholder Data Environments safer from unauthorized access.



In accordance with PCI DSS v4.0, all organizations need to implement Multi-Factor Authentication systems for all accesses to the cardholder data environment. This means any access to your system over a network will require MFA regardless of location, clearance, or title by March 31st, 2025.

MFA BEST PRACTICES

While organizations will need to update their MFA practices over the next three years, 8.4.1 specifies that MFA is mandatory for all admin access into the CDE. Guidance released by the PCI SSC states a few simple ideas for MFA best practice.

Independence of Authentication Mechanisms – organizations need to make sure that the mechanisms used to authenticate different factors are independent and cannot compromise one another.

Protection of Authentication Factors – to meet validation requirements for PCI DSS v4.0 Requirement 8, each factor of authentication needs to be protected. Meaning passwords should be secure, difficult to guess, and follow the industries best practices in achieving security. Hardware or biometric data should be kept private and safe from unauthorized replication. Factors should also not be verified on a step-by-step basis as this could allow unauthorized users to determine the validity of individual factors over time.

Laws and Regulations –additionally, local laws and regulations are important to keep in mind. For example, both the European Union Directive on Payment Services and the Federal Financial Institutions Examination Council have additional requirements when it comes to consumer payments authentication or high risk transactions.

Point-to-Point Encryption

If you're responsible for PCI DSS compliance within your organization, the idea of being able to reduce the lengthy and complicated self-assessment process, as well as your costs and accountability for data breaches, no doubt sounds appealing.

Fortunately, such a possibility does exist, and it comes in the shape of Point-to-Point Encryption or P2PE.

What is Point-to-Point Encryption?

Point-to-Point Encryption is a standard set of requirements created by the PCI Security Standards Council to ensure maximum security for payment card data. It involves the secure and undecipherable encryption of data from the moment a card is swiped, or payment details taken, to the moment the relevant banking service receives those details.

HOW IT WORKS

P2PE works by encrypting card information from the moment it is taken (known as the point of interaction (POI), using an algorithm that turns the data into unreadable codes. These codes are then transferred directly to the processor where they are decrypted automatically using a secure key, before being passed onto the relevant bank.

Since the decryption is carried out automatically, the merchant or processor does not have to decrypt data manually nor do they need access to the secure key; therefore, they never have access to their customer's personal card data. A P2PE solution will even supply a token to the merchant with each transaction, helping them to identify and refund or rectify a payment later, without revealing the card information.

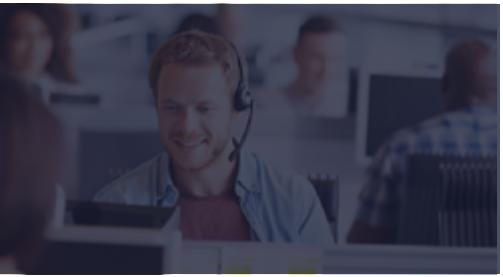
WHY P2PE

While many E2E and P2P solutions are similar, P2PE only refers to encryption solutions that specifically meet the PCI Security Standards Council's requirements. Many E2E solutions don't meet the standard because they include other systems between the POI and the point of processing, elevating the risk of fraud or hacking.

P2PE transfers data directly from the point of interaction to the point of processing, with no other systems in between – hence the name Point-to-Point – making it a much more secure (and quicker) process. P2PE is also an assessable, verifiable standard, whereas E2E has no standards or requirements protecting data once it has been taken.

Descope & Reduce PCI DSS Assessment Cost with P2PE

A PCI-listed P2PE solution can significantly reduce the number of PCI DSS requirements applicable to a merchant's cardholder data environment. It's down to the solution provider to ensure all the requirements of the standard are met and that they are providing a complete and secure system.



If data breach does occur, the P2PE solution provider would be held accountable for any ensuing fines or penalties related to the P2PE component. This passed-on accountability also makes PCI DSS assessments much easier for a merchant using a P2PE solution. However, it does not completely remove the applicability of PCI DSS in the merchant environment.

For example, on the PCI DSS SAQ, an organization responsible for their own encryption has to go through 12 sections and 329 questions, whereas those using a P2PE solution provider only have to cover four sections and 35 questions. Reducing this lengthy assessment process saves both time and money.

CHOOSING A PCI-VALIDATED P2PE SOLUTIONS PROVIDER

When it comes to choosing a P2PE solution provider, there are some big names that you will have already heard of. Mastercard, WorldPay and Verifone are all well-known examples of PCI-validated P2PE solution providers.

For a more comprehensive selection you can also check out the PCI Security Standards Council's directory of Point-to-Point Encryption Solutions.

Defining Tokenization

Tokenization is a solution which helps businesses process telephone payments to reduce the burden of PCI DSS compliance by allowing them to store less cardholder data on their systems. When no data of this type is stored, the amount of compliance which needs to be conducted is greatly reduced.

The process replaces Primary Account Numbers (PANs) and other sensitive data with a "token" when they are shared via a telephone transaction.

Each token is a randomly assigned replacement value, which ensures it cannot be reverse engineered. As it is not an encryption or code, it also cannot be broken by hackers to give access to customer details.

BENEFITS OF TOKENIZATION

When businesses process payments via telephone, customer data may be stored on their systems or it might be conveyed via keypad touch tones. Unfortunately, because contact centers are typically part of large, sprawling and interconnected businesses, it is very difficult indeed to keep this data safe and inaccessible.

Tokenization means that customer data never even reaches the company itself. Instead, companies store each identifying token, while a specialized third-party provider takes care of processing the payment and storing the information securely.

This process doesn't just keep customer data safe, it also protects the reputation of businesses and mitigates the impact of security breaches. Additionally, it relieves organizations of many of the PCI DSS compliance hoops they must jump through annually or even quarterly.

Your Annual PCI Checklist

If your organization takes card payments from customers over the phone or via digital engagement channels such as SMS or WebChat, there are certain checks you must perform to ensure the security of cardholder data. The Payment Card Industry Data Security Standard (PCI DSS) is the information security standard for organizations that handle card payments from the major card schemes, including Visa, Mastercard, American Express, Discovery, UnionPay and JCB.

To remain compliant, the following checks must be performed throughout the year to maintain security and mitigate the risks of a compromise of card or personal data.

It's worth noting that if you're using a solution like PCI Pal then most of the PCI DSS requirements will already be met.

Although the PCI SSC sets the security standards, each card provider also has its own program for compliance, validation levels and enforcement. Compliance is not enforced by the PCI SSC however, but rather by the individual card issuer or acquiring banks.

You can find more information about compliance for each card scheme from the following links:

- **American Express –** americanexpress.com/datasecurity
- **Discover Financial Services –** https://discoverglobalnetwork.com/solutions/pci-compliance/pci-overview
- **JCB International –** jcbeurope.eu/business_partners/security/pcidss.html
- **Mastercard Worldwide –** mastercard.com/sdp
- **Visa Inc –** visa.com/cisp
- **Visa Europe –** visaeurope.com/ais
- **UnionPay –** unionpayintl.com/en/

The Continuous 3-Step Process to PCI Compliance

There are three continuous steps that should be carried out to ensure PCI DSS requirements are met:

1. Assess – Identify cardholder data and take an inventory of your IT assets and business processes for payment card processing, then assess them for vulnerabilities that could lead to a compromise of cardholder data.

2. Remediate – Resolve any vulnerabilities and not store any cardholder data that you do not need.

3. Report – Compile and submit compliance reports to the banks and card schemes you do business with, along with any remediation validation records if applicable.

Annual Checks to Perform in Your Contact Center

Your merchant level dictates the standards you will need to maintain for PCI DSS compliance. This decides whether you need an annual security assessment carried out by a PCI SSC-accredited QSA, or if you can complete an SAQ.

Regardless of the assessment method required, the following steps must be taken each year:

- ☐ Complete an annual risk assessment
- ☐ Ensure third parties that store, process and/or transmit card data have maintained PCI DSS compliance and are registered with the card schemes
- ☐ If you are installing a third party application in your contact center, simplify your compliance by ensuring the product and particular version used is Payment Application Data Security Standard (PA DSS) compliant
- ☐ If you use an integrator to bring the products together, make sure they are certified to the required standard
- ☐ Train your staff to follow PCI DSS procedures
- ☐ Make sure you only store data that is essential and that it is encrypted and/or masked
- ☐ Protect your data network and make sure you are using a firewall and up-to-date anti-virus software
- ☐ Perform network scans on a quarterly basis. These have to be performed by an approved scanning vendor (ASV)
- ☐ You should also discuss security with your web hosting provider to ensure they have secured their systems appropriately. Web and database servers should also be hardened to disable default settings and unnecessary services
- ☐ Annual Pin Entry Device (PED) tests need to be run to identify any vulnerability
- ☐ Any software or hardware you use to process transactions should have approval from the Payment Card Industry Security Standards Council (PCI SSC)

If this all sounds like a lot to deal with, you might like to consider partnering with a hosted PCI solution provider like PCI Pal.

PCI Pal is a leading provider of SaaS solutions empowering companies to take payments securely.

Our solutions provide adherence to strict industry governance and remove a business from the significant risks of non-compliance and data loss.

With extensive operations and technical experience across a myriad of industries, PCI Pal is qualified to deliver operationally efficient cloud-based payment security solutions to organizations operating on a global scale.

PCI Pal's smart PCI solutions, like Agent Assist, can be seamlessly integrated with your contact center operations to ensure compliance without compromising the customer experience.

Learn more about our solutions or reach out to one of our experts to learn how our we can help your organization build consumer trust and safeguard payment data.

Your PCI Glossary

Acquirer – The financial institution that processes your payment card transactions.

Agent Assist – A secure, PCI DSS compliant solution that uses DTMF masking to disguise a customer's key tones when a contact centre agent takes a payment over the phone.

AOC – Attestation of Compliance – a form that allows you to attest to your PCI DSS assessment results.

Audit Trail – A sequential log of your system activities.

CDE – Cardholder Data Environment – The entire environment (personnel, software, and hardware) in which data is stored, processed, and/or transmitted.

Console/Non-console Access – Physically accessing a specific port that allows for administrative actions without needing network access, or elevated access for both administrative and non-administrative actions.

CVSS – Common Vulnerability Scoring System – A method of ranking the seriousness of system vulnerabilities.

Data-flow Diagram – A comprehensive diagram documenting the flow of sensitive data through your system or network.

Descoping - keeping customers' card data out of company systems and minimizing contact areas where data is processed or stored.

DESV – Designated Entities Supplemental Validation – An extra level of security validation required by some payment brands or acquirers.

DPA – Data Protection Act – the Act and relevant legislation regarding data security in the UK.

DTMF – Dual-Tone Multi-Frequency Signaling – the system that recognizes and processes the tones on your phone.

DTMF Masking – Disguises the DTMF containing payment card data by masking them with a monotone beep, to prevent exposure to the contact center.

DoS – A denial-of-service attack in which a hacker disables a system by overloading it with requests.

E2E – End-to-End Encryption. An encryption solution that does not meet P2PE standards.

GDPR – General Data Protection Regulation – The EU's new standard for data security.

ICO – The Information Commissioner's Office – the UK's data protection regulator.

IDS – Intrusion detection system.

IPS – Intrusion prevention system.

IVR – Interactive Voice Response – An automated system that allows a computer to recognize and process speech and DTMF tones.

Multi-factor Authentication – The requirement of two or more levels of authentication to gain access to sensitive data or systems.

P2PE – Point-to-Point Encryption – A standard of encryption for the secure transmission of data from the POI to processing.

PCI DSS – Payment Card Industry Data Security Standards.

PCI SSC – The PCI Security Standards Council.

PFI – PCI Forensic Investigator – The person who investigates system breaches to analyze when, how, and why they occurred.

POI – Point of Interaction – The point at which cardholder data is taken.

QSA – Qualified Security Assessor – A PCI SSC-qualified PCI DSS assessor.

ROC – Report on Compliance – The report made after a PCI DSS assessment.

SAQ – Self-Assessment Questionnaire – the self-assessment section of a PCI DSS assessment.

Service Provider – A third-party organization that provides cardholder data processing, storage, or transmission services.

Tokenization – The use of tokens to represent sensitive data so that data is never accessible by the merchant.

THANK YOU

If you have any further questions about PCI compliance or would like to find out more about PCI Pal, please visit our website or get in touch with our team of experts today.

GET IN TOUCH

www.pcipal.com

info@pcipal.com