



**STARTING YOUR PCI
COMPLIANCE JOURNEY**



Contents

Intro	3
A Beginner's Guide to PCI Compliance	4
PCI DSS 3.2: What's New?	6
What are Merchant Levels?	8
Which Self-Assessment Questionnaire (SAQ) is Right for You?	10
What is a Qualified Security Assessor (QSA)?	12
What is Multi-Factor Authentication?	14
What is Point-to-Point Encryption (P2PE)?	16
What is Tokenisation?	18
Your Annual PCI Checklist.....	20
PCI Glossary	22

Intro

PCI Pal is a suite of secure payment solutions designed to descope your contact centre from the requirements of the Payment Card Industry Data Security Standard, but what is the PCI DSS and how can you ensure your organisation is compliant?

To further your understanding, our payment security experts have compiled this starter guide, covering the basics of PCI compliance and some key factors you need to be aware of. Whether you're planning to go it alone or decide to work with a third-party solution provider, we hope you'll find this information and expert insight helpful as you embark on your compliance journey.

If there are any questions we haven't answered or you'd simply like to discuss your specific requirements in more detail, please get in touch. We'd love to hear from you!

GET IN TOUCH

 ^{U.K.} +44 207 030 3770

 ^{U.S.} +1 866 645 2903

 info@pcipal.com

 www.pcipal.com

Chapter 1

A Beginner's Guide to the PCI DSS

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.

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

Whether you've been referred to us by your bank or you're in charge of compliance for your organisation this is where you'll find everything you need to know about PCI DSS, including how it works, who it affects, and why it's so important.



What is PCI DSS?

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

In order to mitigate the complexity of having multiple standards to adhere to, the credit card brands got together and in 2004 released the first version of the Payment Card Industry Data Security Standard (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 organisations who participate in the development of the PCI DSS by registering for and joining special interest groups (SIGs). Each participating organisation can contribute to the activities which are mandated by that SIG.

How Does It Work?

The PCI DSS is a set of 12 standards which apply to any organisation who stores, processes and transmits credit card details from the major card schemes. In short, if your company take card payments then the PCI DSS applies, and you need to prove compliance against the standards. The twelve 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

Why is the PCI DSS important?

The PCI DSS requirements are designed to combat card fraud by keeping cardholder data safe from hackers and preventing other security breaches.

With data breaches on the increase, laws and regulations have come into effect as a way of strengthening data protection globally. The PCI DSS is a global standard, but it isn't a law. However, almost all data protection laws consider payment card data to be personal data. As such, non-compliance with the PCI DSS may also mean a breach of other legislation and therefore subject to scrutiny and potential fines.

By ensuring your contact centre is PCI DSS compliant, you are also protecting your business – both financially and legally. A single data breach is now estimated to cost a company \$3m on average, while the loss of connectivity caused by a breach or Distributed Denial of service (DDoS) attacks can prevent businesses operating for long periods of time. Not only can this negatively affect or even ruin a company's reputation, it also damages confidence in the industry as a whole.

What are the Risks and Penalties of Non-Compliance?

As mentioned, PCI DSS compliance is not a legal requirement, but it is mandatory if your organisation 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, lawsuits and legal costs, a drop in share price, job losses, insurance claims, regulator fines, higher banking fees, and 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, would your organisation survive?

Chapter 2

PCI DSS v3.2.1

The first release of the PCI DSS (v1.1) was in 2004. At only 17 pages long and with a strong focus on the recording and storage of credit card data, it's very different from the today's, 3.2.1, which is 139 pages long and accompanied by additional documents which offer specific advice and guidance on a more granular level, such as guidance on PCI compliance for large organisations, on protecting telephone based payment card data, and what to do should an organisation fall victim to a data breach.

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

- 1. Scope** – determine which system components and networks are in scope for PCI DSS
- 2. Assess** – examine the compliance of system components in scope following the testing procedures for each PCI DSS requirement
- 3. Report** – assessor and/or entity completes required documentation (e.g. Self-Assessment Questionnaire (SAQ) or Report on Compliance (ROC)), including documentation of all compensating controls
- 4. Attest** – complete the appropriate Attestation of Compliance (AOC)
- 5. Submit** – submit the SAQ, ROC, AOC and other requested supporting documentation such as ASV scan reports to the acquirer (for merchants) or to the payment brand/requestor (for service providers)
- 6. Remediate** – if required, perform remediation to address requirements that are not in place, and provide an updated report

The first step in becoming PCI compliant is to determine where credit card data is present within your organisation, the cardholder data environment (CDE.) This is comprised of the people, processes, and technologies that handle cardholder data or sensitive authentication data. Once identified, organisations can then identify which requirements they need to adhere to and implement action accordingly.

People

The PCI DSS recognises that people are the biggest threat when it comes to the security of credit card data. Organised crime is moving towards Cardholder Not Present (CNP) channels as other areas become more secure. 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 give up this information in numerous ways (e.g. phishing emails) and there is also the risk of staff intentionally stealing credit card data.

Key PCI DSS requirements to consider: 1, 2, 3, 7, 8, 9, 10, 12.

Process

This isn't just referring to card processing but covers the end to end journey where payment card data is present in an organisation 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 centre. 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. Sensitive Authentication Data such as the security code (CVC/CVV etc) and PINs must not be stored by organisations and in instances where it needs to be recorded, it must be rendered unrecoverable. Cardholder data such as Primary Account Number (PAN), 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 standards are pertinent to process. As such, organisations should map and assess all processes against each of the twelve standards.

Key PCI DSS requirements to consider: All

Technology

Who would have envisioned in 2004 that it would be possible to pay for goods with a tap of a watch on a card terminal? 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. Where the twelve requirements have been consistent, elaboration and clarification has been added to ensure organisations are aware of how technology is vital not only in the payment process itself, but also as a way of securing the data.

Key PCI DSS requirements to consider: 1, 3, 4, 5, 6, 8, 10, 11



Chapter 3

How is PCI compliance proven?

This depends on the size and type of organisation. Broadly speaking, organisations can be split into two categories; Merchants and Payment Service Providers (PSPs). Merchants accept card payments and PSPs act as a third party in the storage, processing and transmission of card data. These are then subcategorised 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).

What are Merchant Levels?

There are four different categories that your organisation may fall into, defined primarily by the number of transactions you process, but also by the perceived additional security risks. These criteria allow the PCI SSC to determine the possible risks your customers might face when transacting with you, and therefore, determines which level of security they need to

enforce in order to improve their payment security.

Which Merchant Level Does Your Contact Centre Fall Into?

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 level 1

Criteria:

- 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 annually

- Merchants that have suffered a data breach or cyberattack that resulted in cardholder data (CHD) being compromised
- Merchants that have been identified by another card brand as Level

Validation requirements:

- 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

Merchant level 2

Criteria:

- Merchants processing between 1 million and 6 million Visa, Mastercard, or Discover 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

Validation requirements:

- 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)
- Attestation of Compliance (AoC) form

Merchant level 3

Criteria:

- 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

Validation requirements:

- Annual Self-Assessment Questionnaire (SAQ).
- Quarterly network scan by ASV.
- Attestation of Compliance (AoC) form.

Merchant level 4

Criteria:

- 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

Validation requirements:

- These largely depend on the requirements of the merchant's acquiring bank
- Typically include an SAQ and quarterly network scan by an ASV

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. These service providers must validate their PCI compliance by way of SAQ and undergo quarterly vulnerability scans by an ASV.

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

Chapter 4

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

If your organisation 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. Organisations 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; and/or standalone, dial-out terminals 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 (162 Questions)

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))

SAQ D (For merchants)

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 (For service providers)

Who is it for?

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

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. Additional 'Service Provider Only' requirements are identified within the PCI DSS

Impressions

17,811

↓ 5.05%

Avg. daily viewers

115,945

↓ 7.26%

150,000

120,000

May

a tip



Chapter 5

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).

What is 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 onsite assessment and an annual Report on Compliance (ROC) completed by a QSA. During the PCI assessment, the QSA will determine whether the organisation has met the 12 PCI DSS requirements before completing a ROC.

How Does Someone Become 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 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.

How Do They Interact with Internal Security Assessors?

Internal Security Assessor (ISA) sponsor companies are organisations that have been qualified by the PCI SCC. The council runs an Internal Security Assessor Programme, 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 organisation's understanding of PCI DSS and the requirements they must meet to be compliant. It will also help to improve interactions with Qualified Security Assessors and enhance the reliability, quality and consistency of PCI DSS self-assessments. The result is the proper and consistent application of PCI DSS measures and controls.

How Should You Choose 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 organisation the best chance of hiring a reputable and thorough QSA:

1. What type of organisations have they performed PCI DSS assessments for?

The type of organisation 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.

Chapter 6

What is 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 3.2 however, Multi-Factor Authentication is now mandatory for any personnel with non-console administrative access, as part of Requirement 8 of the PCI DSS.

With these measures such an important part of CDE security, here's everything you need to know about multi-factor authentication.

What is MFA?

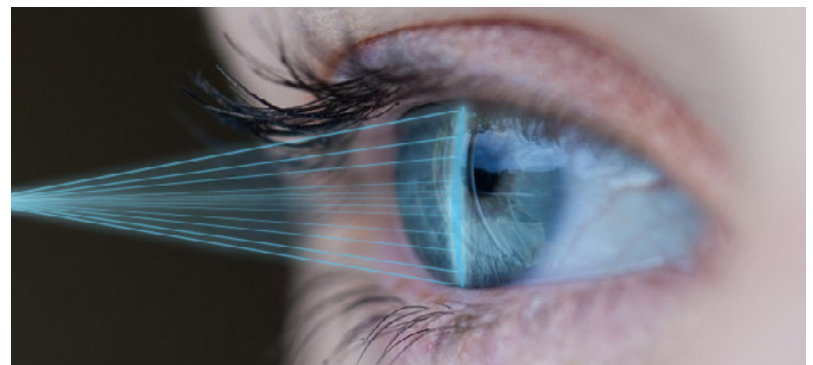
Multi-Factor Authentication is simply a security system that requires more than one type of identification or authentication before allowing user access. The term can refer to two-factor authentication or higher. The forms of authentication required usually encompass knowledge, possession and inherence, 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.

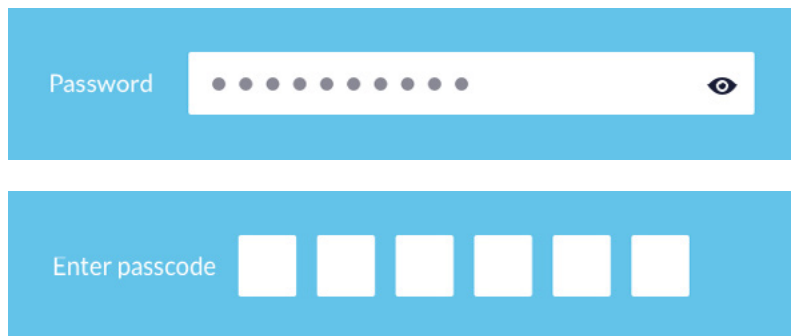
Possession – a physical object, such as a key, swipe card or token.

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, the system is less easily compromised, making Cardholder Data Environments safer from unauthorised access.



The image shows two examples of authentication input fields. The top one is a blue box with the label 'Password' on the left, a white input field containing ten grey dots, and a blue eye icon on the right. The bottom one is a blue box with the label 'Enter passcode' on the left and six white input boxes arranged horizontally.

When Do I Need to Use MFA?

In accordance with PCI DSS 3.2.1, all organisations need to implement Multi-Factor Authentication systems for any non-console administrative access. This means any admin access to your system over a network, even if this is a non-remote, on-site network that is already considered 'safe'.

MFA Best Practice

Guidance released by the PCI Security Standards Council (PCI SSC) states a few simple ideas for MFA best practice. Here are some to keep in mind:

Independence of Authentication Mechanisms – organisations 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 3.2.1 Requirement 8, each factor of authentication needs to

be protected. This simply means passwords should be secure and difficult to guess, while hardware or biometric data should be kept private and safe from unauthorised replication. Factors should also not be verified on a step-by-step basis as this could allow unauthorised users to determine the validity of individual factors over time.

Laws and Regulations – it's important to keep your local laws and regulations in mind as well as the requirements made by PCI DSS 3.2.1. 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.



Chapter 7

What is Point-to-Point Encryption (P2PE)?

If you're responsible for PCI DSS compliance within your organisation, 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 P2PE?

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 Does P2PE Work?

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 electronically, 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 ever revealing the card information.

Reducing this lengthy assessment process not only saves time but also money.

Isn't That Just End-to-End Encryption?

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.

How Can P2PE Help Descope & Reduce PCI DSS Assessment Costs?

The main benefit of a P2PE solution is that all accountability for PCI DSS compliance is automatically the solution provider's responsibility, not the merchant. 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. This passed-on accountability also makes PCI DSS assessments much easier for a merchant using a P2PE solution. For example, on the PCI DSS SAQ, an organisation 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.

Where Can I Find PCI-Validated P2PE Solution Providers?

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



Chapter 8

What is Tokenisation?

Tokenisation 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.

What are the Benefits of Tokenisation?

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 centres and their ilk are typically part of large, sprawling and interconnected businesses, it is very difficult indeed to keep this data safe and inaccessible.

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

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

Impressions

17,811

↓ 5.05%

Avg. daily viewers

115,945

↓ 7.26%

150,000

120,000

May

a tip

Chapter 9

Your Annual PCI Checklist

If your organisation 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 organisations that handle card payments from the major card schemes, including Visa, MasterCard, American Express, Discover and JCB.

To remain compliant, the following checks must be performed annually 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 programme 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 – discovernetwork.com/fraudsecurity/disc.html
- JCB International – jcbeurope.eu/business_partners/security/pcidss.html
- MasterCard Worldwide – mastercard.com/sdp
- Visa Inc – visa.com/cisp
- Visa Europe – visaurope.com/ais

What is the PCI Compliance 3-Step Process?

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

- 1. Assess** – You must 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** – You must fix any vulnerabilities and not store any cardholder data that you do not need.
- 3. Report** – The final step is to compile and submit compliance reports to the banks and card schemes you do business with, along with any remediation validation records if applicable.

Which PCI Standards Do I Need to Maintain?

Your merchant level dictates the standards you will need to maintain for PCI DSS compliance. There are four levels of merchant based on the number of transactions you process every year. This dictates whether you need an annual security assessment carried out by a PCI SSC-accredited Qualified Security Assessor (QSA), or if you can complete a Self-Assessment Questionnaire (SAQ).

What Annual Checks Should I Perform in My Contact Centre?

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 their PCI DSS compliance and are still registered with the card schemes

- If you are using a third party application in your contact centre, make sure the product and particular version you are using 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 to do so
- 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)

Reduce Your PCI Compliance Concerns

If this all sounds like a lot to deal with, you might like to consider partnering with a hosted PCI solution provider. Our smart PCI solutions, like Agent Assist, can be seamlessly integrated with your contact centre operation to ensure compliance without compromising the customer experience.

Chapter 10

PCI Glossary

When it comes to PCI DSS jargon, are you A-OK or are you more “WTH?”?

Whether you know your POS from your POI or you wouldn't know a QSA if one bit you on the nose, our glossary of PCI terms is bound to come in handy at some point. Here are just a few of the terms you're likely to come across on your PCI DSS compliance journey.

A 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 – Direct or indirect access to a mainframe, server, or system.

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.

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 signalling – the system that recognises and processes the key tones on your phone.

DTMF Masking – Disguises the key tones as a contact centre agent takes a payment over the phone by masking them with a monotone beep so that the agent has no way of accessing card information.

De-scope – To remove your contact centre from the scope of PCI DSS entirely by using a third party service provider to process, transmit and /or store all card data.

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 recognise 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.

OS – Operating system.

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

PCI DSS – Just testing!

PCI SSC – The PCI Security Standards Council.

PFI – PCI Forensic Investigator – The person who investigates system breaches to analyse 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 organisation that provides cardholder data processing, storage, or transmission services.

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

Please let us know if there are any other PCI terms you regularly come across, but don't understand. We'll give you a full explanation and will add them to our PCI glossary!

Thank you

We hope you found this eBook useful. If you have any further questions about PCI compliance or would like to find out how PCI Pal can help secure your contact centre without compromising your customer service experience, please visit our website or get in touch with our expert consultants today.

GET IN TOUCH

 **U.K.** +44 207 030 3770

 **U.S.** +1 866 645 2903

 **info@pcipal.com**

 **www.pcipal.com**



**Secure contact centre technology
from contact centre people.**



Safeguarding reputations and trust

www.pcipal.com