keyivr

intelligent payment systems

WHAT IS PCI-DSS COMPLIANCE?

THE ESSENTIAL GUIDE

Everything you need to know about PCI-DSS and why it's important for your organisation

WHAT IS PCI COMPLIANCE?

If your organisation accepts, processes, stores or transmits card payments, the chances are you've heard of the Payment Card Industry Data Security Standard (or PCI DSS or PCIDSS as it is commonly known), but what is PCI DSS?

It's your responsibility to ensure that your customers' payment data, such as sensitive card numbers and other forms of "Sensitive Authentication Data" (SAD) are safeguarded, free from exposure from contact centre agents, fraudulent attacks (internal and external) and other security breaches. By achieving PCI compliance and adhering to the comprehensive requirements of PCI DSS your organisation can be confident that you are improving the safety of your customer's data and the way payments are processed.

In addition to this, with the introduction of the General Data Protection Regulation (GDPR) that covers strict guidelines on how personal information is stored and transmitted. Companies experiencing data breaches are facing fines from the Information Commissioners Office (ICO) of up €20m (approximately £17.5 million) or 4% of turnover, whichever is greater.

Therefore, it is crucial that organisations adopt best practice on data security across their entire corporate infrastructure and processes, not just for accepting payments.

Key IVR are PCI-DSS Level 1, version 3.2 compliant, this is the highest level of certification for PCI payments.

DOES PCI-DSS AFFECT MY ORGANISATION?

If you accept, process, store or transmit card data then PCI DSS affects your organisation. Cardholder data is continuously at risk of theft from hackers that are on the lookout for a way to exploit weaknesses in your organisation. So, no matter the size of your business, **PCI DSS** is there to protect your customers and their data, assisting in the prevention of a data breach which could have a huge impact.

WHO ENFORCES PCI COMPLIANCE?

The security standard started in December 15, 2004 by Visa, Mastercard, American Express, Discover and JCB who formed the Payment Card Industry Security Council (PCI SSC) in 2006 to manage the ongoing evolution of the Payment Card Industry (PCI).

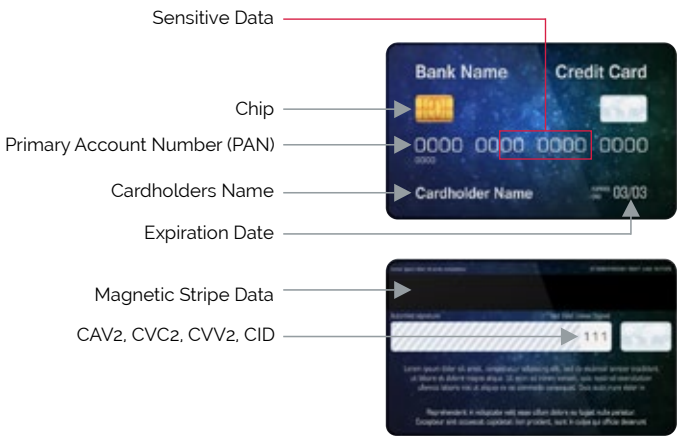
The PCI SCC continues to administer the guidelines with a focus on improving payment account security throughout the transaction process. However, it is the payment brands and acquirers, not the PCI council, that are responsible for enforcing compliance and are able to issue fines and restrictions on your ability to accept card payments.

WHAT IS DEFINED AS 'CARDHOLDER DATA' OR CREDIT CARD DATA?

The PCI Security Standards Council (SSC) defines 'cardholder data' as the full Primary Account Number (PAN) or the full PAN along with any of the following elements:

- Cardholder name
- Expiration date
- Service code

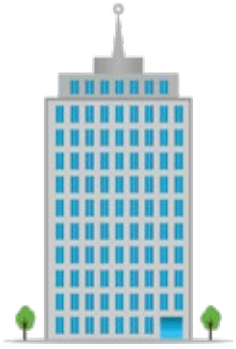
Sensitive Authentication Data, which must also be protected, includes full magnetic stripe data, CAV2, CVC2, CVV2, CID, PINs, PIN blocks and more.



HOW DO I BECOME PCI COMPLIANT?

To be PCI compliant, there are a set of **12 requirements** set by the PCI Security Standards Council (SSC) that are designed to ensure the highest level of protection for any data that is being used throughout the transaction process of a payment. This can be manually or electronically, but if organisations adhere to these requirements, they will dramatically improve their security against malicious attacks towards their organisation, including any internal risks.

There are specific reporting requirements based on your organisation's merchant level, determined by the number of transactions made over a year.



Merchant Level 1:
On-site assessment by a
Qualified Security Assessor (QSA)

Merchant Levels 2–4:
Self assessment via the
Self-Assessment Questionnaires (SAQ)

You must also have a quarterly network scan by an Approved Scan Vendor and an attestation of Compliance Form.

PCI-DSS LEVELS

All organisations will fall into one of the four merchant levels based on transaction volume over a 12-month period.

The following are the 4 levels of PCI compliance:

Level 1

A merchant processing over 6m VISA and Mastercard transactions per annum

Level 2

A merchant processing between 1m and 6m VISA and Mastercard transactions per annum

Level 3

A merchant processing between 20k and 1m VISA and Mastercard transactions per annum

Level 4

A merchant processing less than 20k VISA and Mastercard transactions per annum

Any merchant that suffers a breach involving card payment data can be escalated to a higher compliance level.

THE RISKS AND PENALTIES FOR NOT COMPLYING

Although PCI DSS is not a legal requirement, it is mandatory if your organisation wishes to process transactions with the major card schemes. Here are some of the potential drawbacks and penalties that could occur if you do not maintain PCI compliance:

- Fines and penalties ranging from £3,000 to £6,000
- Lost confidence, so customers go to other merchants
- Diminished sales
- Cost of reissuing new payment cards
- Data breaches and fraud losses
- Legal costs, settlements and judgments
- Termination of ability to accept payment cards
- Lost jobs (CISO, CIO, CEO and dependent professional positions)
- Going out of business
- Higher subsequent costs of compliance

The bottom line is, if you're not compliant and you experience a data breach, your bank provider could choose to impose fines onto you or restrict your ability to take card payments. This can have a huge impact on how you do business.

GDPR Fines

If you experience a data breach as a result of non-compliance with PCI-DSS, you could also face investigation from the Information Commissioners Office (ICO) around your organisation's compliance with the General Data Protection Regulation (GDPR), which has the possibility of resulting in huge fines from up to €20m (approximately £17.5 million) or 4% of turnover, whichever is greater.

THE 12 REQUIREMENTS OF PCI DSS

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. Protect all systems against malware and regularly update antivirus software or programs

6. Develop and maintain secure systems and applications

7. Restrict access to cardholder data by business need to know

8. Identify and authenticate access to system components

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 Security Policy that addresses information security for all personnel

To review these requirements in more detail - click here:

12 Requirements

WHY IS PCI DSS SO IMPORTANT?

Maintaining appropriate security of cardholder data is essential and affects everybody involved. Data breaches or data theft affects the entire payment card ecosystem.

- **For customers**, they can have a sudden loss of trust in the organisations or financial institutions that "allowed" the breach to happen, and their credit can occasionally be negatively affected. It can result in a lot of reconciliation including changing passwords, handling legalities, transferring banks etc.

- **For organisations** and financial institutions, they lose their credibility and in worst case scenarios, their business. Subject to numerous financial liabilities, they have a very long-winded restoration process.

By becoming PCI compliant, organisations are not only protecting their customers, but they are protecting themselves. The PCI SSC say "Such standards help ensure healthy and trustworthy payment card transactions for the hundreds of millions of people worldwide that use their cards every day."

HOW CAN I BECOME PCI-DSS COMPLIANT?

For any organisation, becoming PCI compliant on your own can be a very timely and costly venture with a lot of room for error. Key IVR takes all the pressure off, with already established PCI-DSS level 1 compliant payment solutions, we help assess your systems and provide a secure platform to suit your organisation.

PCI DSS AND COMPLIANCE WITH THE FCA

The FCA regulations impose that any financial firm that provides services to consumers must record their phone calls for training and monitoring purposes in order to prevent, detect and deter market abuse. The Payment Card Industry Data Security Standard (PCI-DSS), on the other hand, outlines that in order to be compliant no card sensitive data can be recorded or stored by the organisation.

DTMF masking can aid with PCI compliance and adhere to FCA regulations, customers key in their sensitive card number into their phone keypad rather than reading it aloud to a call agent. The DTMF tones cannot be decrypted, so the entire call can be recorded and stored in a compliant manner without worrying about logging sensitive data.

WHAT IS DESCOPING?

PCI-DSS considers any person, system, or piece of technology that touches payment information as "in-scope". For example, call centre agents/customer service representatives (CSRs), telephony systems and the IT network and databases used to take payments are all in scope for compliance and should be reviewed as part of the 12 PCI-DSS requirements.

To reduce scope of compliance for your organisation and the number of PCI controls you would have to implement, you can decrease the number of staff and systems that are involved in card payment processing by outsourcing and "de-scoping" them to a dedicated 3rd-party provider offering PCI compliant payment systems, such as Key IVR. This can often lead to a quicker and cheaper journey to PCI compliance, allowing your organisation to focus on other business objectives.

ACHIEVING PCI COMPLIANCE & DESCOPING YOUR ORGANISATION WITH KEY IVR

Whatever stage of the PCI compliance journey you're on, we can help. By providing a range of PCI compliant payment services that fit in with how your organisation operates, we can help descope a lot of the risk and requirements needed to achieve PCI compliance.

In some examples, you could be starting with 233 detailed requirements from a Self-Assessment Questionnaire (SAQ). By outsourcing and descoping your payment channels this can reduce your SAQ to 13 'yes' or 'no' questions.

Simply want to know how to get started with your PCI compliance journey? Talk to us and we'd be happy to discuss how you currently take payments and what's needed to descope and become compliant.

We're trusted by hundreds of clients providing a range of payment services across agent assisted payments, automated telephone lines, SMS and more, processing over £800m ($1.1b) annually. Our PCI DSS Level 1 v3.2.1 platform is constantly evolving to keep ahead of the latest PCI requirements, saving you time and money when compared to building and maintaining your own PCI environment.

ABOUT KEY IVR

Key IVR provides secure cloud payment solutions to organisations and contact centres across the globe, protecting hundreds of businesses and their customers. Businesses can increase their revenue and conversion rate by taking PCI-DSS compliant card payments over the phone, with an automated IVR, on the web, via SMS or on a mobile app.

Our reliable omni-channel SaaS platform is trusted by some of the world's leading brands, processing over £800m ($1.1bn) per annum and reducing the time it takes to collect payments. It is available 24/7 in 14 languages and integrated with all leading Merchants and Payment Gateways worldwide.

START PROTECTING YOUR CUSTOMERS

Talk to Key IVR and let us help you reduce serious security risks within your organisation with our PCI-DSS compliant solutions. We work with you to design a solution that tackles your individual business challenges.

Find out more about our payment services. Alternatively, please contact us on **+44 (0) 1302 513 000** (UK), **+1 929 207 0116** (US) or email **sales@keyivr.com** to discuss your requirements.

Sophie Kelly

Critical Delivery & Senior Account Manager