BANKBROKERS

# PCI DSS Version 4.0

## What’s Changing?

# PCI DSS Version 4.0
## What's Changing?

**Chris Lawrence**

Global Merchant
Services Advisor

The Payment Card Industry Data Security Standard (PCI DSS) has been protecting businesses and consumers for the best part of two decades, since 2004. But the latest version- version 4.0- is becoming the new normal, with the previous v3.2.1 being retired on March 31st, 2024. So, what exactly has changed? And what do you need to do to be ready?

# New in Version 4.0

The PCI DSS has changed numerous times over the years, adapting to the ever-changing threats and needs of consumers. The current version has been in place since 2018, and with how much payments have evolved since then, it is high time for an update.

Version 4.0 has gone through an extensive development process to ensure its goals are met and are reasonable and achievable for all those affected. This involved over 6,000 items of feedback from over 200 companies beginning in 2019 through to 2021, before version 4.0 was officially released in March 2022.

In each version of the PCI DSS, rules are broken down into 12 requirements that businesses must meet in order to satisfy the security standard. All 12 have seen multiple alterations in the transition to v4.0, but the PCI Security Standards Council has highlighted 4 key aims that encapsulate what the latest version is all about:

## 1 CONTINUE TO MEET THE SECURITY NEEDS OF THE PAYMENTS INDUSTRY

As payments change, so do the threats that face them. We are seeing a shift towards digital payments on a scale not seen when previous versions of the PCI DSS were released. This means that new measures must be taken to meet the new risks, including expanded multi-factor authentication requirements, updated password requirements, and new e-commerce and phishing requirements.

## 2 PROMOTE SECURITY AS A CONTINUOUS PROCESS

In the past, it would be simple to meet all the requirements of PCI DSS and stop there, but that fails to acknowledge the changing and ongoing threats to security. Maintaining and continually evaluating payment security is vital to stay ahead of bad actors looking to take advantage. As such, the new PCI DSS requirements include clearly assigned responsibilities for each requirement and added guidance to assist in better understanding of how to implement and maintain security.

## 3 INCREASE FLEXIBILITY FOR ORGANISATIONS USING DIFFERENT METHODS TO ACHIEVE SECURITY OBJECTIVES

In the age of fast-moving technology and innovation, it is difficult for regulators to allow for new, enhanced methods of keeping payments safe, or even just non-traditional methods that are equally secure. That is why in v4.0, the PCI Security Standards Council has attempted to make allowances for organisations to take some liberties in how they meet the requirements, with targeted risk analyses, a more customised approach, and allowances for group, shared, and generic accounts.

## 4 ENHANCE VALIDATION METHODS AND PROCEDURES

As a continued commitment to transparency and granularity, PCI DSS v4.0 aims to enhance methods and procedures of verification, with more detailed reporting and increased alignment between reported information and information summarised in an Attestation of Compliance.

While these 4 key points have been highlighted, there are plenty of other changes to be aware of, including updated firewall terminology to support the more diverse technologies used by businesses to meet the objectives normally fulfilled by firewalls. Full details of all the above changes and more are available on the PCI Security Standards Council website.

# WHAT BUSINESSES NEED TO KNOW

Since version 4.0's initial release last year, businesses have had the choice of which PCI DSS version to be compliant with- the new v4.0, or the pre-existing v3.2.1. However, as of March 31st next year, version 3.2.1 will be permanently retired, meaning that any business not yet in compliance with the new regulations is running out of time to meet the requirements.

It can be a daunting task for businesses, as there are many changes in the new requirements, and tackling them all can be challenging. However, with the right support, organisations will find that crafting a fully compliant security strategy will be worth the effort, embedding the principles of the PCI DSS into the business and putting consumer safety first.

The new emphasis placed on security as an ongoing task will be the key to compliance. By regularly maintaining and assessing security systems, it will become easier to identify gaps and weaknesses, find non-compliant areas, and reinforce the idea of putting security first. When creating your business' strategy for version 4.0, take the idea of continuous security to heart, and build out from there.

## BRINGING IT ALL TOGETHER

With the end of PCI DSS version 3.2.1 fast approaching, it is time for any business that has not already reassessed their payment security to do so. Version 4.0 puts the ideals of continuous security, flexibility, innovation, and further security in the digital age at the heart of its regulatory framework and will help protect businesses and consumers from the ever-changing threats that payments face.

For the businesses not yet fully compliant, a challenging task lies ahead, but one that can be overcome with intelligent and committed strategies that embed security in the foundation of a business. Combined with the support of industry experts, any business is capable of taking the new guidelines to heart and utilising them to achieve greater success than before.

## CONTACT US

Contact us for further information and testimonials on how Bankbrokers can help you. In addition, how industry specialists have helped review merchant services options and solutions to lower costs and offset the impact of rising inflation.

Our team of friendly experts can help your business secure the support you need.

Email:
clawrence@bankbrokers.co.uk

Web: https://bankbrokers.co.uk

Call on (+44) 7852 591574
Write to our office:
Bankbrokers, Bank Chambers,
Brook Street, Hampshire,
SO32 1AX, UK