PCI Compliance Standards Guidelines

The Payment Card Industry Security Standards Council (PCI SSC) published a new version of the industry standard that businesses use to safeguard payment data before, during, and after purchase. PCI Data Security Standard (PCI DSS) version 3.2 replaced previous versions in addressing the growing threats to customer payment information. Any company that accepts, processes, or receives credit card payments must adopt it as soon as possible to prevent, detect, and respond to cyberattacks that lead to potential breaches. We have comprised answers to some of the most common questions about the update below.

Why is the PCI DSS being updated?

The council updates the PCI DSS to ensure it continues to protect against old exploits that are still causing problems, addresses new exploits, and provides greater clarity for implementing and maintaining PCI DSS controls.

What are the types of changes included in PCI DSS 3.2?

PCI DSS 3.2 includes additional clarifications to existing requirements, new or evolving requirements, as well as additional guidance. These are outlined in the Summary of Changes from PCI DSS 3.1 to PCI DSS 3.2.

What is new in PCI DSS 3.2?

Within the 12 core requirements of the PCI DSS, there are five new sub-requirements for service providers affecting requirements 3, 10, 11, and 12. New sub-requirements have also been added to requirement 8 to ensure multi-factor authentication is used for all non-console administrative access as well as cardholder data environments. There are also two new appendices. Appendix A2 incorporates new migration deadlines for removal of Secure Sockets Layer (SSL)/early Transport Layer Security (TLS) in line with the December 2015 bulletin. Appendix A# incorporates the “Designated Entities Supplemental Validation” (DESV), which was previously a separate document. All the changes are outlined in the Summary of Changes from PCI DSS 3.1 to PCI DSS 3.2.

How are these changes determined?

The standard update is part of the regular process for ensuring PCI DSS addresses current challenges and threats. This process factors in industry feedback from the PCI Council's more than 700 global Participating Organizations, as well as data breach report findings and changes in payment acceptance.

How long do organizations have to implement PCI DSS 3.2?

PCI DSS 3.1 retired on October 31st, 2016, after which all assessments need to use version 3.2. The new requirements introduced in PCI DSS 3.2 were considered best practices until January 31st, 2018. As of February 1st, 2018, they were effective as PCI requirements and must be used.

What supporting documentation is available for compliance with PCI DSS 3.2?

PCI DSS 3.2 supporting documents include updated Self-Assessment Questionnaires (SAQ), Attestation of Compliance (AOC) forms, Report on Compliance (ROC) templates, Frequently Asked Questions (FAQ) and Glossary. All of these are available in the Documents Library on the PCI SSC website.