FORTRA

How to Comply with PCI Data Security Standards

How Managed File Transfer Solutions Can Help Meet v3.2 (3.2.1), and upcoming v4.0

PCI Data Security Standard 3.2 and 3.2.1

Implications for Managed File Transfer Solutions

If you work for any organization that processes credit or debit cards, then you must achieve and maintain PCI DSS compliance. The Payment Card Industry Data Security Standard (PCI DSS) is a proprietary information security standard for organizations that process credit or debit cards. The standard is a moving target as it is frequently updated to address new security threats or to clarify issues that have been exposed as problems in prior versions.

Version 3.2 of PCI DSS was announced in April 2016, with minor changes for v3.2.1 added in May 2018. Being up to date on current compliance standards helps ensure you avoid hefty industry fines and helps protect you against a potentially costly and reputation-harming data breach.

Here's what you need to know to comply with current PCI DSS standards. And what you should be looking at to be ready to comply with v4.0 by the March 2024 deadline.

Brief Summary of v3.2.1 Highlights

- **PCI Requirement 8.3.1:** Multi-factor authentication is now required for all non-console access compared to only remote access in v3.2.
- **PCI Requirement 6.4.6:** This new requirement mandates merchants certify proper security is in place if the cardholder data environment is changed.
- **PCI Requirements 10.8 and 10.8.1:** Requires service providers to report any failures in their critical security controls in a timely manner (file integrity management, firewalls, physical and logical access controls, etc.).
- **PCI Requirement 12.11:** This requirement states service providers must perform quarterly reviews to ensure their personnel are following the correct operational and security policies and procedures.

Why Do PCI DSS Standards Keep Changing?

Cybersecurity is an ever-evolving field that continually expands to cover new technology and emerging threats. The PCI Security Standards Council updates PCI DSS regulations to address these new concerns and provide greater clarity regarding existing and upcoming requirements.

What are the Key Requirements of PCI DSS

While many requirements of v3.2 were slightly reworded from previous versions for the sake of clarity or to take changing industry terminology into account, there are five main requirements of note. The three that apply to everyone are multi-factor authentication, SSL and TLS migration, and PAN storage. If you are a service provider or fall under the DESV (Designated Entities Supplemental Validation), you have additional considerations.

Who Has to Comply with PCI DSS?

Anyone processing cardholder data should be paying attention to PCI DSS compliance. However, not every PCI DSS requirement applies to every organization. While some of the current requirements apply to all entities that fall under PCI DSS, several updates are aimed specifically at service providers. Appendix A3—the DESV—applies only to entities designated by payment brands or acquirers as needing additional assessment.

Multi-factor Authentication

Protecting administrative access to the cardholder data environment (CDE) is imperative. Regardless of the method used to gain access to a network, the goal of an intruder is typically to find a device to which they can gain administrative rights. Once they have that, they can move throughout the network, gaining access to additional machines until they reach the valuable cardholder data. Multi-factor authentication provides an added layer of protection at critical points.

Version 3.2 updates requirement 8.3 from "two-factor authentication" for authentication for remote network access to "multi-factor authentication" to reflect the possibility of organizations having more than two forms of authentication. The requirement also expanded to include all individual, non-console administrative access and all remote access to the CDE.

With this change, entities allowing any kind of non-console access will need multi-factor authentication, regardless of whether that access is happening remotely, from within the organization's own network, or from the CDE.

SSL and Early TLS Migration

The Secure Sockets Layer (SSL) first appeared in the 1990s and grew to be a widely accepted security standard. However, SSL is now considered to have several vulnerabilities. Version 3.2 of PCI DSS requires organizations to work toward upgrading to a strong cryptographic protocol, meaning at least TLS 1.1, although TLS 1.2 is strongly recommended.

This applies to a few PCI DSS requirements that require strong cryptography or additional security features: requirements 2.2.3, 2.3, and 4.1. PCI DSS version 3.2 requires all service providers to deploy a secure service offering.

PCI DSS 3.2 requirement updates regarding multi-factor Authentication, SSL & TLS Migration and PAN Storage APPLY TO EVERYONE.

PCI DSS Compliance for Service Providers

Service providers play a critical role in keeping card-holder data protected for their customers, and weaknesses in their security practices have been a common factor in breaches. A recent Nilson Report estimated $28.6 billion in payment card-related losses occurred in 2020 (over one-third of them in the U.S.). They also predict this number will reach $408 billion in losses by 2030. With these staggering statistics, it is imperative service providers do their part to adhere to the protection measures outlined in PCI DSS standards.

PCI DSS 3.2's security requirements hold service providers more accountable for the security of their customers' data. Service providers must detect and notify customers of failing critical security control systems. Third-party penetration testing is required every six months, rather than annually as was required by the previous version of PCI DSS. Quarterly reviews are required of employees and their respective access to the CDE. And finally, service providers must provide documentation of their encryption architecture.

Designated Entities Supplemental Validation (DESV)

The DESV, or Appendix A3 of PCI DSS v3.2, applies only to entities designated by a payment brand or acquirer as requiring additional validation. For example, this could be because they are storing and transmitting an especially large volume of cardholder data, or because they have had issues with breaches in the past. However, it is recommended that all organizations follow the outlined procedures.

The DESV aims to make PCI DSS compliance an ongoing practice, rather than a hurdle which is cleared and then forgotten.

How Does PCI DSS 3.2 Impact Secure File Transfers?

Almost every organization deals with file transfers, and if you are required to comply with PCI DSS, you'll want to ensure you are using a secure file transfer method, such as a managed file transfer (MFT) solution, that enables you to achieve compliance with every new version of the regulation.

What Does This Mean?

First, your MFT software needs to support TLS 1.1 and 1.2 to ensure compliance and up-to-date encryption standards. Secondly, the solution must support role-based security with multi-factor authentication. PCI DSS requires multi-factor authentication at either the network level or system level.

The DESV requirement may or may not apply to you, but either way you should be considering how you will maintain PCI DSS compliance year-round without adding too much time and effort to the IT workload. Robust MFT solutions streamline this initiative by providing the security features, auditing, and detailed reporting that auditors want and need to see. Some MFT software can even help you easily check if your file transfers are PCI DSS-compliant.

If you haven't implemented a managed file transfer solution yet, now is the perfect time to both ensure you are compliant with PCI DSS version 3.2 and the upcoming v4.0. A comprehensive file transfer solution will continually be updated to include security features that keep pace with current threats.

Get the Guide to Learn More: PCI DSS Compliance With Managed File Transfer

What Are the New PCI 4.0 Requirements?

Version 4.0 will be mandatory by March 2024, so organizations would be wise to start preparing for the higher level of protection needed today, as it can be a time-consuming, resource-heavy process. The PCI Council recommends it be done in phases and provides a specific timeline to help meet the new requirements. To ensure full compliance with the new standards, the current version 3.2.1 will be active until it is retired March 31, 2024.

GoAnywhere MFT Users Can Be Assured of Compliance

To meet the requirements for PCI compliance, technical solutions that are automated, auditable, and centralized, such as secure file transfer from Fortra's GoAnywhere MFT, can help.

GoAnywhere MFT provides tools to help users keep sensitive data transfers compliant with PCI DSS, including:

- Support for TLS 1.1 and 1.2
- Integration with LDAP and external RSA multi-factor authentication
- Centralized control and management of file transfers
- Role-based administration and permissions
- Secure connections for the transmission of sensitive data
- Encryption of data at rest and in motion
- Strong encryption key management with separation of duties
- Ability to keep PCI-related data out of the DMZ
- Closed inbound ports into the private network to prevent intrusion
- Detailed audit logs for reporting

In addition, GoAnywhere MFT's Advanced Reporting Module can generate a Security Settings Audit Report to easily let you know if the security settings on your GoAnywhere installation are fully aligned with PCI DSS requirements. Along with this status check, the report provides recommended actions and lets you know to which section of PCI DSS the setting applies.

The PCI DSS standard will continue to evolve, but by implementing robust solutions, forward-thinking IT shops can meet current requirements while laying a solid foundation for future security enhancements.

Get Started with Help for PCI Compliance Today

Request your free 30-day GoAnywhere trial!

Start a Free Trial

About Fortra

Fortra is a cybersecurity company like no other. We're creating a simpler, stronger future for our customers. Our trusted experts and portfolio of integrated, scalable solutions bring balance and control to organizations around the world. We're the positive changemakers and your relentless ally to provide peace of mind through every step of your cybersecurity journey. Learn more at fortra.com.

fta-ga-wp-0123-r2-gm