PCI DSS Compliance

BEYOND IDENTITY

About PCI DSS

The Payment Card Industry Data Security Standard (PCI DSS) is a compliance standard intended to enforce a baseline security requirement for institutions and businesses that handle payment card data. PCI DSS encompasses a wide range of technical and operational requirements, including authentication, storage, networking and physical security of payment card data. **Beyond Identity does not store or manage payment card data, but as an authentication provider we are able to provide simple and powerful tools to support you on your PCI DSS compliance journey.**

About PCI DSS Revision 4

In 2022, the PCI DSS 4.0 standard was released, which was the most recent major revision since v3.2.1 introduced in 2018. The updated version included new requirements for strong authentication when accessing cardholder data, as a defense against identity-based attacks like phishing. PCI DSS 4.0 requires risk-based assessments that generally follow **NIST Zero Trust Architecture** guidelines. As a secure access provider, Beyond Identity can help you achieve your compliance objectives around PCI DSS by introducing phishing-resistant MFA to your workforce and administrators. In this document we will outline some of the specific requirements to achieve PCI DSS 4.0.1, and how Beyond Identity can greatly simplify your path to compliance.

PCI DSS on Authentication

PCI DSS is intended for all companies that accept, process, store or transmit payment card data, and so it provides some flexibility to allow different access control methods. Compliant organizations are free to choose between (from **section 8.3.1**):

- Something you know, such as a password or passphrase.
- Something you have, such as a token device or smart card.
- Something you are, such as a biometric element.

These authentication factors are not all created equal, however! The PCI DSS 4.0 standard introduces new requirements for password management and multi-factor authentication (MFA) that can be difficult to maintain and complex for your users to follow. Beyond Identity provides the simplest solution to meet PCI DSS requirements by focusing on the authentication factors that are simplest to secure, maintain and use: device-bound passkeys and biometrics.

PCI DSS Compliance

BEYOND IDENTITY

What are the new authentication requirements in PCI DSS 4.0?

Password complexity rules

PCI DSS 4.0 introduces new requirements for the use of strong authentication factors. For organizations that use passwords to authenticate, Section 8.3 requires a minimum password length of 12 characters, and mandates that all passwords to be rotated every 90 days. Administrators must also document their password management procedures, and provide guidance to users on how and when to update their passwords. **Beyond Identity's passwordless MFA eliminates these requirements entirely, by removing passwords as an authentication factor.**

Expanded MFA requirement

PCI DSS 4.0 also expands the requirements for MFA, requiring that it be implemented for all access to cardholder data systems. This requirement encompasses your workforce users as well as any cloud environments or providers you use, making it a challenge to implement across your entire organization. **Beyond Identity's MFA is simple to deploy and administer, and helps you satisfy these requirements across your entire fleet.**

What other PCI DSS requirements can we help you solve?

Protect your users from phishing attacks

PCI DSS 4.0 section 5 requires administrators to take active steps to mitigate and protect against phishing attacks. **Beyond Identity's phishing-resistant MFA helps you eliminate a wide range of identity-based threats, including adversary-in-the-middle attacks, social engineering, session takeover and credential theft.**

Protect your system components from vulnerabilities

Beyond Identity helps our customers achieve the device trust requirements in PCI DSS 4.0 section 6 by adding device posture checks into their access controls. Using our powerful policy engine, you can require up-to-date vulnerability patches, antivirus software, and MDM/EDR tools in place before granting any access to sensitive data. You can implement these controls for both your managed and unmanaged devices, giving you unique control over BYOD infrastructure.

PCI DSS Compliance

BEYOND IDENTITY

What other PCI DSS requirements can we help you solve?

Evaluate your current system

Beyond Identity deployment teams support our customers in a thorough evaluation of their existing authentication methods and points to identify areas where passwordless authentication can be implemented along with a deployment plan for supporting the rollout.

Unique to Beyond Identity, our passwordless phishing resistant MFA supports all major operating systems, identity providers, and seamless integrations with enterprise identity infrastructure to maximize deployment of secure authentication.

Select a FIDO2-compliant provider

Beyond Identity is FIDO2 certified and delivers phishing-resistant MFA with device-bound passkeys and continuous device posture, exceeding PCI standards.

Monitor access to system components and cardholder data

PCI DSS 4.0 section 10 deals with monitoring and audit logs for access to cardholder data. **Beyond Identity provides an immutable audit log of hardware-backed authentication events that is compatible with many SIEMs and other data warehousing tools.** We can assist you in your auditing and monitoring requirements with the data we retrieve from each authentication.

Avoid shared authentication credentials

PCI DSS 4.0 section 8 requires that all users be assigned unique identification factors before any access to system components or cardholder data. Use of shared credentials is not allowed except when necessary on an exception basis. **Beyond Identity's platform authenticator helps our customers achieve compliance by providing your workforce with unique, non-transferrable identity factors that can not be shared by multiple users.**

PCI DSS Compliance

BEYOND IDENTITY

What other PCI DSS requirements can we help you solve?

Use strong cryptography to secure authentication factors in transmission

Section 8 also requires that any authentication factors that are transmitted must use strong cryptography to protect the credential from unauthorized access. **Beyond Identity's MFA does not transmit any biometric information over the wire, and all passkey information is secured using the device TPM or secure enclave.**

Define your access control model

Section 7 in PCI DSS 4.0 defines requirements for least privileged access to system components and cardholder data. **Beyond Identity helps you achieve these requirements by simplifying your access controls.** You can define custom permissions based on job function that grant the minimum necessary permissions to each member of your workforce.

Meet PCI DSS Compliance with Beyond Identity

Beyond Identity's "secure by design" architecture makes it simple to meet and surpass the authentication guidelines in PCI DSS.

Engineered to completely eliminate identity-based attacks, we can help you achieve your IT and security requirements. If you are curious to learn more, schedule a demo with us.