PAYMENTS | PCI DSS V4.0.1 | SECTION 15 REQUIREMENTS

# Token & PCI DSS v4.0.1

PCI DSS v4.0.1 (June 2024) Section 15 codifies the twelve detailed requirements that merchants, processors, acquirers, and service providers must satisfy to protect cardholder data. Requirement 8 — Identify Users and Authenticate Access — was substantially strengthened in v4.x, mandating MFA for all access into the cardholder data environment (CDE), all administrative access, and all remote network access. TokenCore Wearable and TokenCore Portable deliver FIDO2-certified, phishing-resistant, hardware-bound MFA that maps directly to the requirements below.

## Requirements Mapping

| § Requirement | What it requires | How Token addresses it |
|---|---|---|
| 8.3.1 | All user access to system components is authenticated via at least one of: something you know, have, or are. | TokenCore Wearable and TokenCore Portable deliver possession (hardware-bound device) plus inherence (on-device fingerprint match) on every login. Match-on-chip: the fingerprint template is created and verified inside the secure element and never leaves the device. |
| 8.3.2 | Strong cryptography is used for all authentication factors during transmission and storage. | FIDO2-certified design: authentication private keys are generated and held inside an EAL5+ certified secure element and cannot be exported. NFC and BLE channels carry only signed assertions, never the credential — there is no shared secret to transmit or store. |
| 8.4.1 | MFA is implemented for all non-console administrative access into the CDE. | One-touch MFA for admins logging into Windows, macOS, vSphere, AWS / Azure / GCP consoles, and CyberArk PAM. Replaces phishable OTP and push MFA — the vector behind the MGM, Coinbase, and Snowflake admin compromises. |
| 8.4.2 | MFA is implemented for all non-console access into the CDE. | Hardware-bound MFA gates every workforce login that touches CDE-scoped systems. Origin-bound FIDO2 credentials defeat reverse-proxy and AiTM kits that defeat OTP, SMS, and push-MFA on the same workflows. |
| 8.4.3 | MFA is implemented for all remote network access (originating from outside the entity's network) by personnel and third parties. | Same authenticator covers VPN, ZTNA, VDI, and remote-desktop entry. Drop-in alongside Okta, Microsoft Entra, Ping, and Duo — no rip-and-replace, deployment in hours rather than weeks. |
| 8.5.1 | MFA system is not susceptible to replay; cannot be bypassed; uses at least two different factor types; access is granted only after all factors succeed. | FIDO2 origin-bound assertions are cryptographically bound to the relying party — replay-resistant by design. Possession (the device) and inherence (on-device biometric) are two distinct factor types, evaluated together before the assertion is signed and released. |
| 7.2 & 8.2.5 | Access is granted by business need-to-know; access for terminated users is immediately revoked. | Hardware-bound credentials tie every access decision to a specific device and a specific person. Lost, stolen, or departing-credential revocation is one action in your IAM console — the credential dies with the device. No password rotation, no help-desk reset window. |
| 10.2 | Audit logs are implemented to support detection of anomalies, suspicious activity, and forensic analysis of events. | Every authentication produces a signed, attestable event tied to a specific authenticator and individual. Feeds Splunk, Sentinel, Okta, and Entra audit logs with tamper-evident identity signals — direct evidence for QSA testing of § 10.2.1 user-identification logging. |
| 12.8 | Risk to information assets associated with Third-Party Service Provider (TPSP) relationships is managed. | Token authenticators extend the same phishing-resistant MFA standard to contractors, MSPs, and TPSPs that touch the CDE — supporting written-agreement and due-diligence obligations under § 12.8.2 and § 12.9 (TPSP responsibility). |

## Token Products Referenced

### TokenCore Wearable

FIDO2 authenticator. EAL5+ certified secure element, 508 DPI on-device fingerprint sensor, BLE + NFC. Match-on-chip biometrics; private keys never leave the ring. Designed for shared workstation retail, call center, and back office settings.

### TokenCore Portable

Wireless FIDO2 hardware security key with on-device fingerprint sensor and secure element. Field-upgradable firmware. Drop-in replacement for OTP and tap-only keys for admin, developer, and TPSP workforce.