FINANCIAL SERVICES | 23 NYCRR 500

Token & NYDFS Part 500

NYDFS Part 500 obligates banks, insurers, and licensees to deploy effective MFA, protect Nonpublic Information, and certify compliance annually under § 500.17(b). Legacy MFA — passwords plus OTP or push — is the vector behind most recent in-scope cybersecurity events. TokenCore Wearable and TokenCore Portable replace that vector with FIDO2-certified, hardware-bound, biometrically-verified authentication that maps directly to the controls listed below.

Requirements Mapping

§ Section	Requirement	How Token addresses it
500.7	Access Privileges — limit access to Nonpublic Information; periodically review.	Hardware-bound credentials on TokenCore Wearable and TokenCore Portable tie every privileged login to a specific device and a specific person. Lost or departing user revocation is one action in your IAM console.
500.12	Multi-Factor Authentication — required for any user accessing internal networks from external networks; risk-based or stronger controls.	FIDO2-certified MFA combining possession (Wearable or Portable) and inherence (on-device fingerprint match). Match-on-chip: the fingerprint template never leaves the secure element. Phishing-resistant by design: origin-bound credentials defeat reverse-proxy and AiTM kits that defeat OTP and push-MFA.
500.15	Encryption of Nonpublic Information — protect data in transit and at rest; CISO-approved compensating controls if infeasible.	Private keys are generated and stored inside an EAL5+ certified secure element and never leave the device. NFC and BLE channels carry only signed FIDO2 assertions, not credentials. Strengthens the authentication leg of your encryption story for CISO compensating-control reviews.
500.14	Training and Monitoring — monitor authorized user activity; detect unauthorized access or tampering.	Every authentication produces a signed, attestable event tied to a specific authenticator and user. Feeds your SIEM / IAM logs with tamper-evident identity signals — strengthens audit trails per § 500.6 and Authorized User monitoring per § 500.14(a).
500.16	Incident Response — promptly respond to and recover from cybersecurity events.	Phishing-resistant authentication removes the most common initial-access vector behind ransomware and account takeover (Scattered Spider, MGM, Aflac, Change Healthcare). Reduces both the frequency and blast radius of in-scope § 500.17(a) reportable events.
500.11	Third Party Service Provider Security — require MFA and encryption from vendors with nonpublic information access.	Token authenticators extend the same phishing-resistant MFA standard to contractors, MSPs, and outsourced operations teams that touch your environment, supporting the contractual representations § 500.11(b) requires.
500.4 / 500.3	CISO oversight and written cybersecurity policy covering access controls and identity management.	Token deploys in hours alongside Okta, Microsoft Entra, Ping, Duo, and CyberArk — no a rip-and-replace. Gives the CISO a defensible, documented control upgrade to cite in the annual § 500.17(b) compliance certification.
500.12	Multi-Factor Authentication — required for any user accessing internal networks from external networks; risk-based or stronger controls.	FIDO2-certified MFA combining possession (the ring or BioStick) and inherence (on-device fingerprint match). Match-on-chip: the fingerprint template never leaves the secure element. Phishing-resistant by design — origin-bound credentials defeat reverse proxy and AiTM kits that defeat OTP and push-MFA.
500.15	Encryption of Nonpublic Information — protect data in transit and at rest; CISO-approved compensating controls if infeasible.	Private keys are generated and stored inside an EAL5+ certified secure element and never leave the device. NFC and BLE channels carry only signed FIDO2 assertions, not credentials. Strengthens the authentication leg of your encryption story for CISO compensating-control reviews.

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 in regulated workflows.