TOKEN

TokenCore.com

NON-BANK FINANCIAL INSTITUTIONS | FTC SAFEGUARDS RULE (16 CFR PART 314)

Token & the FTC Safeguards Rule

The FTC Safeguards Rule (16 CFR Part 314), implementing the GLBA, applies to non-bank financial institutions including auto dealers, mortgage brokers, payday lenders, finance companies, tax preparers, and investment advisors not registered with the SEC. The 2021 amendments — and the deadline that took effect June 9, 2023 — added a hard MFA requirement at § 314.4(c)(5), expanded encryption obligations at § 314.4(c)(3), and tightened service-provider, monitoring, and incident-response controls. TokenCore Wearable and TokenCore Portable deliver FIDO2-certified, phishing-resistant, hardware-bound MFA that maps directly to the elements below.

Requirements Mapping

§ Section	Requirements	How Token addresses it
314.4(c)(5)	Implement multi-factor authentication for any individual accessing any information system, unless the Qualified Individual approves in writing the use of reasonably equivalent or more secure access controls.	FIDO2-certified MFA combining possession (TokenCore Wearable or Portable) and inherence (on-device fingerprint match) on every login. Phishing-resistant, origin-bound credentials defeat reverse-proxy and AiTM kits that defeat OTP, SMS, and push-MFA — the controls the FTC has cited as inadequate in recent enforcement actions against non-bank lenders and dealers.
314.4(c)(1)	Place access controls, including technical and, as appropriate, physical controls, to authenticate and permit access only to authorized users.	Hardware-bound credentials make every access decision tie to a specific device and a specific person. Match-on-chip biometrics: the fingerprint template is created and verified inside the secure element and never leaves the device. No shared secrets, no phishable factors.
314.4(c)(3)	Encrypt all customer information held or transmitted both in transit over external networks and at rest; if infeasible, secure with effective alternative compensating controls approved by the Qualified Individual.	Authentication private keys are generated and held inside an EAL5+ certified secure element and cannot be exported, copied, or replayed. NFC and BLE channels carry only signed FIDO2 assertions, never credentials. Hardens the authentication leg of the encryption requirement and supports the Qualified Individual's compensating-control review.
314.4(c)(8)	Implement policies, procedures, and controls to monitor and log the activity of authorized users and detect unauthorized access or use of, or tampering with, customer information.	Every authentication produces a signed, attestable event tied to a specific authenticator and individual user. Feeds Splunk, Sentinel, Okta, and Microsoft Entra logs with tamper evident identity signals, direct evidence for the FTC's expected monitoring and audit-trail capability.
314.4(f)	Oversee service providers — select providers capable of maintaining appropriate safeguards; require by contract that they implement and maintain such safeguards; periodically assess them.	Token authenticators extend the same phishing-resistant MFA standard to MSPs, processors, brokers, and outsourced support teams that touch customer information — supporting contractual safeguard obligations and the periodic assessment requirement under § 314.4(f).
314.4(h)	Establish a written incident response plan designed to promptly respond to, and recover from, any security event materially affecting customer information.	Phishing-resistant authentication removes the most common initial-access vector behind ransomware and account takeover. Reduces both the frequency and blast radius of events that would trigger the FTC notification requirement under § 314.5 (events affecting 500 or more consumers, reported within 30 days).
314.4(a) & (i)	Designate a Qualified Individual responsible for the information security program; require written annual reports to the board on the program's status.	Token deploys in hours alongside Okta, Microsoft Entra, Ping, Duo, and CyberArk — no a rip-and-replace. Gives the Qualified Individual a defensible, documented control upgrade to cite in the annual board report and to anchor the written approval of any compensating-control deviation under § 314.4(c)(5).

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.