



Case study

First National Bank of Long Island enhances security with biometric authentication.



Overview

Banks operate under intense scrutiny when it comes to cybersecurity, and First National Bank of Long Island was no exception. Faced with growing regulatory requirements and increasing threats, the bank needed to strengthen internal access controls to protect sensitive customer data.

Security auditors recommended implementing a strong multifactor authentication (MFA) solution. But traditional approaches (such as complex passwords) created friction for employees and burdened IT teams with frequent reset requests.




After a previous unsuccessful attempt at biometric integration, the bank revisited the technology, seeking a solution that could deliver robust security, compliance, and a seamless user experience across shared workstations and roving users..



Challenge

The bank needed a solution that could deliver robust security without compromising usability or productivity.

Key issues:




-  **Regulatory compliance:** Meeting stringent standards such as PCI-DSS, GLBA, and SOX while addressing auditor recommendations for stronger authentication.
-  **User friction:** Complex passwords led to frequent lockouts and dozens of daily password reset requests, draining IT resources.
-  **Failed past attempts:** A previous unsuccessful biometric deployment meant the bank needed a proven, reliable solution that could integrate seamlessly with existing systems.

Solution

First National Bank of Long Island deployed BIO-key's ID Director for Windows integrated with Active Directory to deliver secure biometric authentication for roving users and shared workstations.

The solution provides fingerprint-based MFA and Single Sign-On capabilities without requiring tokens or device-specific enrollment. Using BIO-key's patented Vector Segment Technology (VST), fingerprint data is converted into encrypted mathematical templates, ensuring compliance and strong security.

Technical highlights:

-  **Active Directory integration:** ID Director operates at the AD tier, enabling centralized management and seamless authentication across Windows environments.
-  **Biometric MFA with VST encryption:** Fingerprint templates are encrypted and proprietary, ensuring data security and compliance with financial regulations.
-  **Hardware support:** FIPS 201-compliant PIV-Pro fingerprint scanners deliver high-accuracy authentication for shared and roving user scenarios.

Impact

By replacing complex passwords with fingerprint-based multifactor authentication, the bank achieved compliance, reduced IT overhead, and improved user experience across shared workstations and roving employees.

Key outcomes:



Stronger security: Delivered a robust MFA solution that meets stringent regulatory requirements (PCI-DSS, GLBA, SOX).



Reduced IT burden: Greatly decreased password reset requests, saving time and resources for the IT team.



Improved workflow: Enabled one-touch authentication for roving users and shared workstations, eliminating friction and boosting productivity.

"BIO-key offered the best pricing, and their solutions were just as effective as their competitors."

Paul Vasquez, Assistant Vice President,
First National Bank Of Long Island

Use cases

- Financial services compliance
- MFA for roving users
- Biometric authentication for shared workstations

Customer benefits

- Strong security and compliance
- Reduced IT workload
- Improved user experience

Strategic value

This project highlights the importance of balancing strict security standards with employee freedom and usability.

By replacing complex passwords with biometric authentication, First National Bank of Long Island improved compliance and reduced IT strain while simplifying access for staff. It demonstrates BIO-key's ability to deliver strong security that works for people, not against them.



"In financial services, strict compliance and robust protection are non-negotiable. But so is enabling staff to work efficiently. By implementing BIO-key's biometric authentication, the First National Bank achieved both: strong, multi-factor security and a simple, one-touch experience that frees employees from password fatigue. This balance of security and usability is what we believe every financial institution should strive for."

NAME, BIO-key Leadership





info@bio-key.com
www.bio-key.com

© 2026 BIO-key International®. All rights reserved.