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

*— Paul Vasquez,
Assistant Vice President*

## CHALLENGE: WHAT INSPIRED CHANGE?

When it comes to security, banks are under a microscope. Recent cybersecurity threats have forced many banks to take action to address potential vulnerabilities within their security platform. Banks must comply with various security and financial regulations, including the Payment Card Industry-Data Security Standard (PCI-DSS), Gramm-Leach-Bliley Act (GLBA) and the Sarbanes-Oxley Act (SOX). Security auditors have suggested that banks focus on securing internal access to customer data by implementing a "strong" multifactor authentication solution.

First National Bank of Long Island auditors recommended that the IT team increase the number of characters required for user passwords.  Although the migration to a more complex password raises the bar on security, it also increases the day to day friction. Because complex passwords are hard to remember, they create a drain on the IT staff when users experience lockouts or simply forget their password.  It's not unusual to receive dozens of password reset requests during a typical workday and that number only increases when employees return from vacation.

As the bank reviewed the many options for multifactor authentication, the use of biometrics emerged as a preferred option.

## PATH TO BIO-KEY

In this particular case, the bank had already made a failed attempt to integrate a biometric authentication solution.  During their initial attempt, the bank tried to install the technology but encountered a few issues which prevented them from moving forward.

Years later, after reevaluating the benefits that biometric technology delivers from a security and workflow standpoint, the bank decided to make a second attempt to go biometric.

After conducting their due diligence, they decided to narrow their selection process down to three potential vendors.  Imprivata, a Fiserv Solution and BIO-key were all asked to provide capabilities presentations and ultimately demonstrate their solution offerings.

Upon reviewing the performance capabilities and costs of the three companies, First National Bank of Long Island selected BIO-key.

## SOLUTION

The bank had several requirements for this project.  They needed a fingerprint reader that supported Windows 7, the current environment and supported Windows 10, which they planned to upgrade to in the near future.

Their initial goal of securing access to the device via Windows soon blossomed into wanting to use biometric authentication across multiple applications.  It's not unusual for new customers to want to expand their biometric sign-in experience across additional use cases.  The bank asked BIO-key to install ID Director for Windows, which integrates directly with Active Directory to provide a strong

layer of biometric authentication that can be used as a single sign-on solution or multifactor authentication option in conjunction with Windows apps.

## HURDLES

The bank did have a staff member that questioned the security of enrolling their fingerprint in the system. Upon understanding that they had already submitted their fingerprint during the e-Verify background check process, the employee was at ease. Additionally, it should be noted that BIO-key takes the initial fingerprint image and converts it into a mathematical template using our patented Vector Segment Technology (VST). The VST template is encrypted and can only be interpreted by our proprietary software.

## OUTCOME & ROI

The addition of BIO-key solutions helped the bank in many ways. First and foremost, BIO-key fulfilled the bank's desire to deploy a "strong" multifactor authentication solution. ID Director for Windows allowed the bank to secure roving workers operating on shared workstations without relying upon entering a complex password for each entry. Workflow was streamlined and optimized by the ease of one-touch instant authentication.

The bank's IT team was particularly pleased as password resets were "greatly reduced – thanks to fingerprint authentication."

Possibly the best news of all, especially for a bank, because they really understand the value of a dollar, BIO-key's entire suite of solutions including fingerprint readers, ID Director software and ongoing tech support cost LESS than the bank anticipated spending on the project.

## Key Benefits

- Solution for Roving Users and Shared Workstations
- Greatly Reduced Password Resets
- Complex Password Reduction
- Easy to Use and Implement
- Biometrics are the Strongest Form of Authentication
- One-Touch Access
- Affordable

## Featured Products

### PIV-Pro

PIV-Pro is BIO-key's highly accurate **FIPS 201 compliant** scanner, providing best in class biometric fingerprint authentication for our government and healthcare customers.

### ID **Director** for Windows

ID Director for Windows Features secure and convenient fingerprint biometric authentication that operates at the **Active Directory** tier, independent of any end point device, as required to support shared workstations and roving users. IDDfW delivers a simple, secure biometric authentication experience without the need to enroll on each device, or having to provide a token to each user, while also supporting traditional multi-factor authentication option.

With IDDfW, enterprise customers will meet the most stringent compliance requirements, while delivering a **trusted biometric authentication solution** and a superior user experience.

To learn more about this project or other customer deployments, contact **info@bio-key.com**