

Case study

Krumland Auto Group implements MFA and Identity-Bound Biometrics.



Overview

Krumland Auto Group, a trusted automotive dealership with a legacy spanning over 70 years, found itself at a pivotal moment when new FTC Safeguards Rule requirements mandated stronger data protection measures.

As a business handling sensitive customer information, Krumland needed to implement a comprehensive security program that included multi-factor authentication (MFA) across diverse environments; from shared workstations on the sales floor to roving desktops in the shop.



Challenge

The solution had to accommodate unique user scenarios, such as technicians working in rugged conditions where phones or tokens were impractical, without disrupting daily operations – and an impending change in regulations.

Key issues:

-  **Compliance deadline:** Meeting strict FTC Safeguards Rule requirements for MFA before the regulatory deadline.
-  **Complex user needs:** Supporting technicians who could not use mobile devices or tokens due to protective gear and work conditions.
-  **Integration and coverage:** Implementing a flexible MFA solution that secured desktops, web apps, remote access, and integrated with existing systems like Microsoft Active Directory and Cisco VPN.

“Krumland Auto Group needed to meet new compliance requirements without disrupting its retail operations. For dealerships handling sensitive customer data, security must be strong yet practical. By implementing BIO-key’s passwordless, identity-bound biometrics, Krumland achieved compliance and protected critical information while keeping workflows simple. This is the kind of that every retail organization should strive for.”




NAME, BIO-key Leadership

Solution

Krumland Auto Group implemented BIO-key’s PortalGuard IDaaS with Identity-Bound Biometrics (IBB) to meet FTC Safeguards Rule compliance and enhance security across desktops, web apps, and remote access.

The solution delivers phoneless, tokenless, passwordless MFA integrated with Microsoft Active Directory and Cisco VPN, supported by fingerprint readers for shared workstations and shop-floor environments. This architecture ensures secure, seamless access while addressing unique operational challenges.

Technical highlights:

-  **Passwordless MFA with IBB:** FIDO2-compliant biometric authentication eliminates reliance on phones or tokens, providing phishing-resistant security.
-  **Flexible integration:** PortalGuard integrates with existing Microsoft AD and Cisco VPN infrastructure for centralized identity management.
-  **Hardware-enabled access:** PIV-Pro and SideSwipe fingerprint readers deployed at workstations enable quick, secure authentication for roving users and technicians.

Impact

The deployment transformed Krumland Auto Group's security posture while preserving operational efficiency. The solution not only ensured compliance with FTC Safeguards Rule but also delivered measurable productivity gains and improved user experience across the organization.

Key outcomes:



Regulatory compliance achieved: Met FTC Safeguards Rule requirements ahead of the deadline, avoiding potential penalties.



Enhanced productivity: Eliminated authentication delays for technicians, saving an estimated \$6 million annually in lost productivity.



Improved security and user experience: Delivered phish-resistant MFA and passwordless authentication without reliance on phones or tokens, ensuring seamless access for all employees.

Use cases

- Automotive retail compliance
- Passwordless MFA for shared workstations
- Identity-bound biometrics for operational efficiency

Customer benefits

- Highest level of assurance without complexity
- Reduced risk of credential theft
- Improved productivity and compliance

Strategic value

This deployment shows how BIO-key helps retail organizations achieve compliance without disrupting operations.

By implementing passwordless, identity-bound biometrics, Krumland Auto Group secured sensitive customer data and met regulatory requirements while maintaining productivity. It reinforces BIO-key's commitment to delivering practical, high-assurance security for retail environments.



"It prevented us from losing millions of dollars in lost revenue due to the new MFA requirements placed on dealerships like ours. Forcing technicians to remove their gear just to access their phones would create a tremendous loss of productivity for them, which in turn would cost us money."

IT Director, Krumland Auto Group





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

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