Passkeys for Banking: A Comprehensive Guide for U.S. Bankers

Regulatory Landscape

In the U.S. banking cybersecurity domain, there's a significant move towards Multi-Factor Authentication (MFA). Regulatory bodies like the Federal Trade Commission (FTC) have updated the Gramm-Leach Bliley Safeguard's Rule, mandating financial institutions to adopt MFA for all users. The New York Department of Financial Services (NYDFS) has been championing MFA since 2017 and is now proposing expanded requirements. The Cybersecurity and Infrastructure Security Agency (CISA) emphasizes phishing-resistant standards.

Understanding Passkeys

Endorsed by the FIDO (Fast IDentity Online) Alliance, passkeys mark a transition from password-based to passwordless authentication. FIDO's approach focuses on local authentication, using either a physical device or biometric data. The primary advantage of passkeys is their resistance to phishing and replay attacks.

The Role of the FIDO Alliance

The FIDO Alliance, backed by global brands, including major U.S. financial institutions like Bank of America and JPMorgan Chase, aims to standardize and promote robust authentication protocols. Their collaboration has led to the FIDO authentication standard evolving into passkey authentication.

Why Secure and User-Friendly Authentication Matters

For banking customers, a blend of security and usability is crucial. Banks can differentiate themselves by offering phishing-proof authentication, ensuring a consistent

user experience across all platforms. This not only enhances customer trust but also ensures regulatory compliance.

FIDO: The Gold Standard of Online Authentication

FIDO stands tall in the realm of authentication standards. Supported by global industry leaders, FIDO represents extensive collaboration and research. Its phishing-proof nature ensures that even intercepted user credentials are rendered useless.

Challenges in Implementing New Authentication Technologies

Banks often face hurdles when integrating new technologies due to diverse user-facing applications and varied technological platforms. Historical attempts at overhauling IT infrastructures have often led to over-budget projects that were eventually abandoned. Thus, introducing new authentication technology without disrupting the existing tech stack is vital.

Revolutionizing MFA Implementation

The BNP Paribas Success Story: Secfense's "no-code" approach offers an especially beneficial solution for large institutions. BNP Paribas's adoption of Secfense’s User Access Security Broker led to:

- Expansion of MFA to 43% more applications than initially planned.
- 82% reduction in IT specialist engagement.
- Savings of $778,000 compared to traditional MFA deployment.
- 100% utilization of existing MFA methods.
- 100% reduction in software developer engagement.
- 87% reduction in implementation costs.

With Secfense, U.S. banks can introduce FIDO & passkeys seamlessly, ensuring phishing-proof security and a smooth customer transition.

Experience the Future of Banking Security

Dive into Our Proof of Value Offering: We invite institutions to experience a Proof of Value (POV). This hands-on experience provides comprehensive MFA protection, introduces microauthentications, and offers full-site protection akin to VPN functionalities. All we ask is the dedication of one specialist for 10 hours over a week and honest feedback post-POV. Dive in and ensure your bank remains compliant, secure, and customer-centric.