



BIO-key Introduces Passkey:YOU, a Phish-resistant, Phoneless and Tokenless Biometric FIDO Passkey Authentication Solution

Convenient, Lower-cost FIDO Passkey Authentication Provides a Superior User Experience powered by BIO-key's Identity-Bound Biometrics

Holmdel, NJ– June 14, 2024 – [BIO-key® International, Inc.](#) (NASDAQ: BKYI), an innovative provider of workforce and customer Identity and Access Management (IAM) software infrastructure featuring passwordless, phoneless and token-less Identity-Bound Biometric (IBB) authentication solutions, today announced the launch of a unique biometric FIDO passkey authentication solution targeting underserved workplace scenarios in manufacturing, retail, healthcare, call center and Sensitive Compartmentalized Information Facilities (SCIFs): [Passkey:YOU](#).

Eliminating passwords and implementing multi-factor authentication (MFA) is a goal of nearly every security-conscious enterprise, but mainstream IAM platforms offer only limited “what you have” authentication options based on phone apps and FIDO tokens. These options are ill-suited for many workplace scenarios that prohibit the use of phones or personal devices, leading to challenges in implementing passwordless or MFA without using phones. The current industry-standard phoneless authentication solution is FIDO hardware tokens, requiring enterprises to purchase two or more FIDO hardware tokens for every user, ranging in cost from \$25-\$70 each, not to mention replacing user tokens when lost. The leading FIDO token manufacturer states that 25% annual token replacement is typical. The economics of procuring hardware tokens for tens of thousands of roving users to access an often much smaller set of shared workstations and devices just doesn’t make business sense.

Passkey:YOU avoids the high cost of buying FIDO hardware tokens for every user, turning the unfavorable economics of FIDO hardware tokens on its head by placing authentication hardware at device access points, not in every user’s pocket. Passkey:YOU leverages the managed hosted FIDO-certified passkey capabilities of BIO-key’s partner IDmelon’s managed passkey solution to replace per-user tokens and phones as device authenticators with a simple touch of a shared USB fingerprint scanner or the tap of a standard door access badge to a shared USB NFC scanner connected to any Windows workstation to unlock a managed Passkey for the user, authenticating the user without a phone or a FIDO hardware token needed.

In its biometric mode, Passkey:YOU is powered by BIO-key’s renowned [Identity-Bound Biometrics](#), allowing an unlimited number of users to be their own phish-proof credential, eliminating the need for them to carry any device or token to authenticate and get work done. BIO-key’s biometric platform includes privacy law-compliant workflows and provides user controlled privacy dashboards, ensuring that enterprises can use biometrics with confidence that they will comply with privacy laws in every jurisdiction. Passkey:YOU’s phoneless and tokenless authentication is a user-centric, more cost-effective approach that is ideally suited for scenarios where users operate without phones, such as manufacturing shop floor, retail, call center, higher education, and

healthcare. In addition to biometric access, Passkey:YOU also supports standard proximity door access cards as authenticators for appropriate security applications.

By eliminating the requirement for a phone or FIDO hardware token to strongly authenticate users, Passkey:YOU fills gaps in mainstream authentication, and is a drop-in, zero-configuration replacement for any application or identity provider that currently accepts FIDO hardware tokens or phone-based passkeys. Passkey:YOU can be deployed as a hosted or on-premise deployment, and provides security teams immediate visibility into user access patterns to third-party applications that traditional FIDO security keys do not. Passkey:YOU facilitates passwordless workflows and integrates seamlessly into zero-trust frameworks and existing Identity and Access Management (IAM) platform identity providers such as Microsoft Entra, Okta, Ping and Duo. With Passkey:YOU, users can effortlessly present a biometric-secured FIDO passkey, serving as a drop-in replacement for existing FIDO and WebAuthn passkeys or hardware tokens, ensuring secure and convenient authentication for every user.

“FIDO Passkeys are quickly becoming the dominant means to combat phishing and eliminate passwords for enterprise users,” said Jim Sullivan, SVP of Strategy and Chief Legal Officer at BIO-key. “Unfortunately, the mainstream ‘what-you-have’ approaches center on phone apps and hardware key-based passkeys, which don’t work in many workforce user scenarios. Our customers asked us to solve the passwordless and multi-factor authentication challenge arising among the largest segments of their digitally enabled workforces – what-you-have authentication approaches are inefficient, allow account sharing, and are too expensive. With our partner IDmelon, we developed a BIO-key-secured passkey authentication solution that makes using passkeys to eliminate passwords effortless while instantly identifying users with certainty. This authentication product should be a valuable tool for hundreds of thousands of global enterprises that struggle to deliver passwordless and strong authentication all users with their existing IAM platform choice.”

BIO-key's Passkey:YOU boasts unique technology and efficiency differentiations from existing passkey approaches:

- **Cost & Efficiency:** Passkey:YOU cuts lifecycle costs by 50 – 70% compared to FIDO hardware tokens while exceeding strong authentication requirements of cyber insurers to avoid increased premiums or dropped coverage.
- **Flexibility and Familiarity:** Passkey:YOU can be easily integrated into existing authentication processes for identity providers, applications, and infrastructure, because it presents to FIDO-compliant relying parties as a standard FIDO authenticator. There’s no need to rip and replace existing identity providers. Passkey:YOU has a minimal contact surface with existing systems because it leverages FIDO-certified workflows. One-time enrollment enables access across multiple devices and locations, without configuration of any relying party necessary.
- **Security:** Passkey:YOU is powered by BIO-key's Identity-Bound Biometrics, which supports over 30 different fingerprint scanners interchangeably, utilizes centrally managed and

encrypted NIST-certified biometrics, secured by patented 1024-bit encryption to defeat man-in-the-middle and replay attacks.

- **Biometric Privacy Law Compliance:** BIO-key's enrollment and operational workflows were designed to ensure compliance with global biometric privacy laws, ensuring that enterprises can yield the benefits of biometrics with confidence that compliance and privacy are integral to the platform.

Please visit the BIO-key website to learn more about Passkey:YOU and Identity-Bound Biometrics.

About BIO-key International, Inc. (www.BIO-key.com)

BIO-key is revolutionizing authentication and cybersecurity with biometric-centric, multi-factor identity and access management (IAM) software securing access for over forty million users. BIO-key allows customers to choose the right authentication factors for diverse use cases, including phoneless, tokenless, and passwordless biometric options. Its hosted or on-premise PortalGuard IAM solution provides cost-effective, easy-to-deploy, convenient, and secure access to computers, information, applications, and high-value transactions.

BIO-key Safe Harbor Statement

All statements contained in this press release other than statements of historical facts are "forward-looking statements" as defined in the Private Securities Litigation Reform Act of 1995 (the "Act"). The words "estimate," "project," "intends," "expects," "anticipates," "believes" and similar expressions are intended to identify forward-looking statements. Such forward-looking statements are made based on management's beliefs, as well as assumptions made by, and information currently available to, management pursuant to the "safe-harbor" provisions of the Act. These statements are not guarantees of future performance or events and are subject to risks and uncertainties that may cause actual results to differ materially from those included within or implied by such forward-looking statements. These risks and uncertainties include, without limitation, our history of losses and limited revenue; our ability to raise additional capital to satisfy working capital needs; our ability to continue as a going concern; our ability to protect our intellectual property; changes in business conditions; changes in our sales strategy and product development plans; changes in the marketplace; continued services of our executive management team; security breaches; competition in the biometric technology industry; market acceptance of biometric products generally and our products under development; our ability to convert sales opportunities to customer contracts; our ability to expand into Asia, Africa and other foreign markets; our ability to integrate the operations and personnel of Swivel Secure into our business; fluctuations in foreign currency exchange rates; delays in the development of products, the commercial, reputational and regulatory risks to our business that may arise as a consequence the restatement of our financial statements, including any consequences of non-compliance with Securities and Exchange Commission ("SEC") and Nasdaq periodic reporting requirements; our temporary loss of the use of a Registration Statement on Form S-3 to register securities in the future; any disruption to our business that may occur on a longer-term basis should we be unable to remediate during fiscal year 2024 certain material weaknesses in our internal controls over financial reporting, and statements

of assumption underlying any of the foregoing as well as other factors set forth under the caption "Risk Factors" in our Annual Report on Form 10-K for the year ended December 31, 2022 and other filings with the SEC. Readers are cautioned not to place undue reliance on these forward-looking statements, which speak only as of the date made. Except as required by law, we undertake no obligation to disclose any revision to these forward-looking statements whether as a result of new information, future events, or otherwise.

Engage with BIO-key

Facebook – Corporate: <https://www.facebook.com/BIOkeyInternational/>

LinkedIn – Corporate: <https://www.linkedin.com/company/bio-key-international>

Twitter – Corporate: [@BIOkeyIntl](https://twitter.com/BIOkeyIntl)

Twitter – Investors: [@BIO_keyIR](https://twitter.com/BIO_keyIR)

StockTwits: [BIO_keyIR](https://stocktwits.com/BIO_keyIR)

Investor Contacts

William Jones, David Collins

Catalyst IR

BKYI@catalyst-ir.com or 212-924-9800