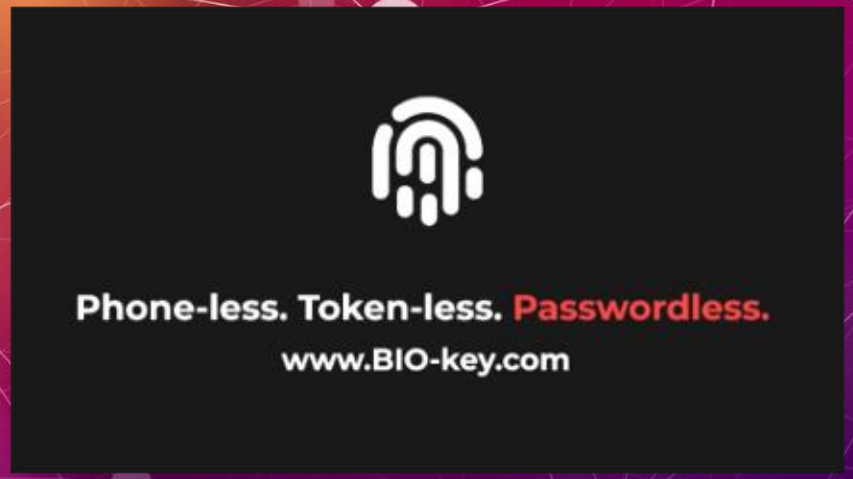
BIO-key®



Nasdaq: BKYI

Identity and Access Management Solutions Delivering Stronger Security and Greater Efficiency, Flexibility and ROI

January 2026

www.BIO-key.com

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; 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 execute and deliver on contracts in Africa; 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 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, 2024 and other filings with the Securities and Exchange Commission. 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.

BIO-key at-a-Glance

NASDAQ	BKYI
Recent Price	$0.60
52-Week Range	$0.51 - $1.97
Shares/Equivalents (1)	10.8M
Market Cap	**$ 6.5M**
LTM Revenue (2)	$ 6.3M
Price/Sales (3)	**1.0x**
Insider Ownership	~ 7%

Balance Sheet Items as of Sept. 30	2025
Cash Equivalents (4)	**$2.0M**
Total Current Assets (4)	$3.7M
Total Assets (4)	$10.1M
Debt	$1.4M
Stockholders' Equity (4)	$6.0M
Book value per share at 9/30/25	$0.83
Recent Share Price	$0.60
Price-to-Book (5)	0.7x

(1) includes Oct.'25 sale of 3.1M shares at $1.02 via warrant exercise for gross proceeds of $3.1M.

(2) Majority of revenues derive from annual recurring licensing fees, recurring maintenance and support.

(3) Compares to median software industry price/sales ratio of ~ 3.1x and cybersecurity comps: OKTA, CYBR & CHKP trading between 6x and 17x sales.

(4) Does not include $3.1M of gross proceeds from sale of 3.1M shares in October.

(5) Median software industry price-to-book ratio is 3.3x.

Investment Considerations

High Margin Recurring Revenue Base + Expanding Global Footprint

- Annual revenue base has grown to ~$6.3M from $2.8M in 2020
- Blended gross margin of 70 to 80% depending on software/hardware mix
- Trimmed operating losses in 2024 and 2025 through ongoing operating cost reductions
- Further operating/financial improvement anticipated via BIO-key branded sales in Europe/EMEA region
- BIO-key is expanding market reach via strategic partners and growing traction in defense and regulated industries
- 40M+ global users authenticate with BIO-key

Expanding Need for Enhanced System Access Protection

- Existing solutions are failing with growing consequences
- Growing regulatory / cyber insurance standards drive enhanced solution adoption
- Growing base of sophisticated Banking and Defense customers requiring highest levels of security

Attractive Valuation

- BKYI trades at 1x Price/Sales vs. software industry and cybersecurity comp. medians of ~3.1x & 7.7x
- Unrecognized value for strategic partnerships / investments and Nasdaq platform

Growing EU Cybersecurity Mandates

- **NIS2 makes strong access and identity controls (including MFA or equivalent) mandatory** for "essential" and "important" entities across sectors such as energy, transport, health, banking, and digital infrastructure, with national laws due by 17 Oct 2024. Article 21 specifically requires organizations to implement multi-factor or continuous authentication and secure communications where appropriate, making MFA an explicit expectation rather than an optional control.
- **The 2024 EU cybersecurity regulation requires all EU bodies to implement multi-factor authentication** on all network and information systems, setting a strong benchmark for public-sector security.
- **Member State NIS2 transposition laws (rolled out 2024–2025) generally interpret NIS2 as requiring MFA** for privileged, administrative, and remote access for in-scope operators, tightening expectations on how accounts are protected in practice.
- **The EU Cyber Resilience Act (2024) introduced mandatory cybersecurity-by-design requirements** for products with digital elements, including identity and access-control obligations that will indirectly push vendors to embed MFA/strong authentication into software, IoT, and embedded products sold in the EU.

Growing U.S. Cybersecurity Mandates

Executive Order 14306 (June 2025) & CISA BOD 25-01

- Sustained secure software development and cloud security baselines; mandatory Secure Cloud Business Applications (SCuBA) configurations for federal agencies, reinforcing MFA, phishing-resistant auth, and secure-by-default in cloud environments.

DOD CMMC Final Rule (effective Nov. 2025)

- Phased rollout of Cybersecurity Maturity Model Certification for defense contractors; requires MFA, access controls, and maturity-level assessments—major driver for enterprise MFA/identity solutions.

NIST/CISA Guidance Expansions

- Updated Secure by Design bad practices (Jan 2025), draft cloud/token protection (IR 8587), and continued enforcement of post-quantum readiness and KEV patching—amplifying demand for MFA and secure identity tools.

SEC Cybersecurity Disclosure Rules (S-K Item 106)

- Effective for 2024 with annual reporting on processes and 8-K disclosures on incidents.

Cyber-Insurance Mandates

- Federal Trade Commission (FTC Section 5 expansion)
- Cybersecurity & Infrastructure Security Agency (CISA) Dec. 2023 guidance to eliminate use of easy to exploit default passwords

Amazon Web Services

- Mandated MFA for most privileged users
- BIO-key Launched on AWS Marketplace August 2024

BIO-key Use Cases

Reducing Cyber Risk

Prevent cyberattacks, including ransomware.

300% increase in US cybercrimes since the start of the pandemic.

Improving Usability

Users have too many passwords to remember

IT support flooded with password reset calls.

Each password reset call costs $70.

Reducing Costs

Enterprises have too many IAM solutions to manage with limited IT resources/ cyber-expertise.

Top brands are too expensive for SMEs.

BIO-key streamlines solutions, reducing vendor & IT team costs.

Compliance & Insurance

HIPAA, PCI, NYDFS, etc. requires added security & privacy controls.

Cyber insurance requires enhanced controls, especially MFA.

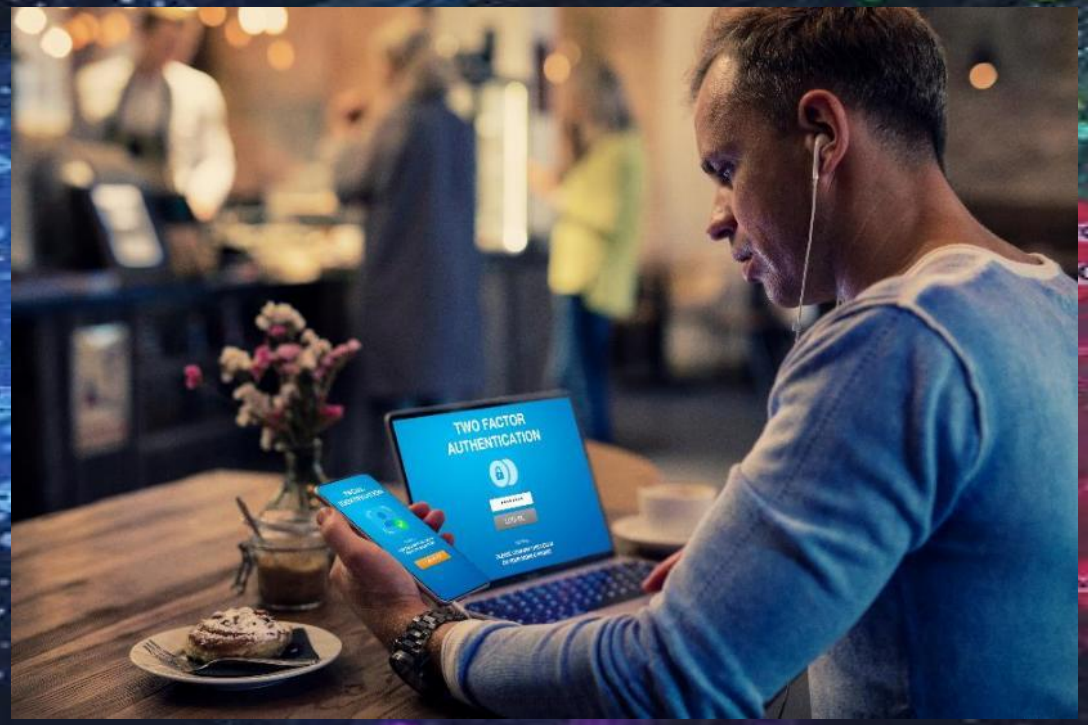
BIO-key enables regulatory & cyber insurance compliance.

Kathy Pinto | VP of IT
Orange Bank & Trust

"BIO-key provides both biometric authentication and a proven suite of IAM solutions that provide **greater** security, flexibility, and value over approaches offered by other vendors."

Mainstream MFA Offers Only “Device Assisted Authentication“

Phone Apps



OR

User tokens

The Future is:

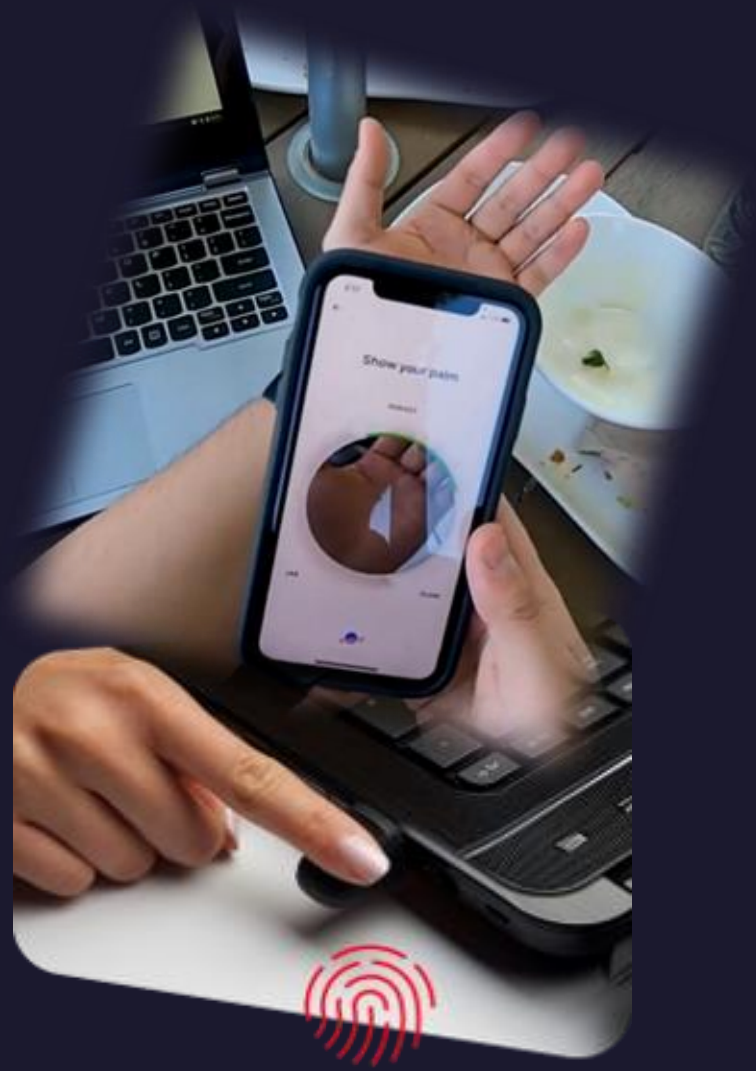
Phone Apps Had Worked for Desk-Based Workers, but…

- Employees often must leave phones in a locker
  - Clean Desktop (Call Center)
  - Data Security/Privacy
  - No Distractions
  - Safety (Manufacturing, Shop Floor, Healthcare)
- Several states & EU require compensation for work-related personal phone use
  - California Labor Code § 2802(a): employer shall indemnify employee for all necessary expenditures/losses incurred in direct consequence of discharge of duties..."
  - Unpaid compensation can lead to costly class action claims
- SMS authentication is easily hacked or compromised

BIO-key's Unique Differentiator: Phoneless / Tokenless Biometric Authentication

Identity Bound Biometrics create a centrally managed, unique biometric identity to verify users anywhere, based on **who they are**, NOT what they carry, know or could share

- Centrally secured, privacy law compliant
- Patented, high security data and integrity protection
- Captured using USB fingerprint scanners or MobileAuth app



Cannot be phished, handed over, shared, forgotten, or stolen

Perfect for situations where phones and hardware tokens will not work, are costly, cumbersome, unreliable, or unsafe single points of failure

Enterprise-controlled enrollment

Affordable and easy to implement

Passkey:YOU™

Eliminates Phones/Hardware Tokens for Restricted Environments, Delivering Greater Efficiency and Cost Savings versus Tokens

Uses BIO-key Biometric authentication to replace FIDO2 hardware tokens for signing into shared workstations

Use Cases:

- Manufacturing
- Repair Centers
- Call centers
- Retail
- Healthcare
- Sensitive Compartmented Information Facilities (SCIFs)

- Compatible with existing identity infrastructure: Microsoft Entra, Okta, Ping and others
- FIDO-Certified
- Simplified and more secure account recovery when other authenticators are lost

Value Proposition / Recent Deployments

- Complete MFA offering with **Phoneless & Tokenless** authentication
  - Leverages patented biometric capabilities **widely deployed** in the highest-security settings in the world.

- Growing Deployment Momentum - particularly in Global Military/Defense, Financial Services & Healthcare
  - Significant biometric identity solution for Middle East defense-sector organization
  - $600k follow-on order for prominent foreign defense ministry, bringing total project revenues over $3M.
  - Completed Biometric IAM Deployment for New Int'l Defense Agency in Record Time
  - National Bank of Egypt deploys advanced MFA & Single Sign-On to 30,000 employees

- In Proof of Concept with key accounts:
  - Residential construction
  - Retail grocery
  - Call centers
  - Automotive OEM

Gartner Highlights BIO-key' Value

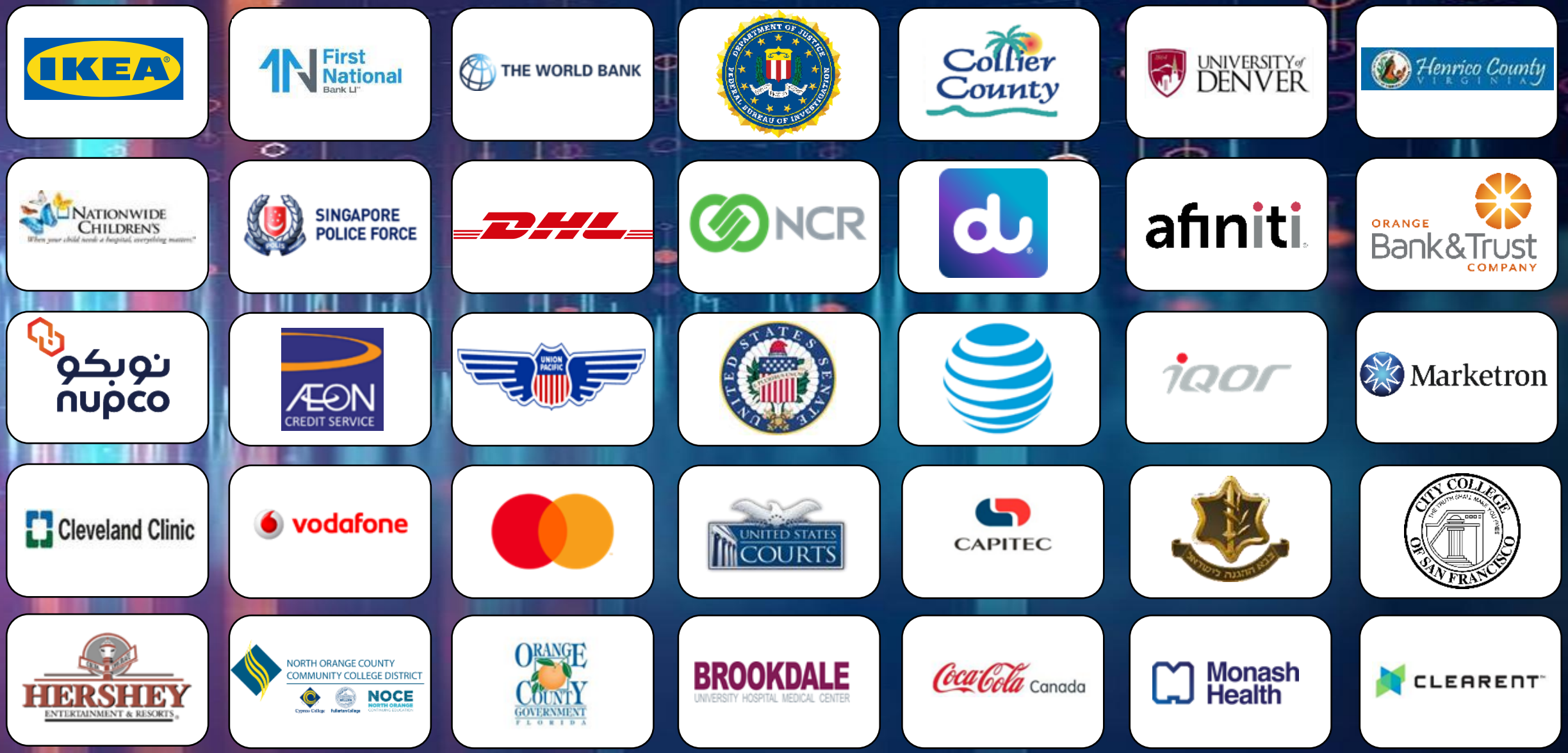
- "User authentication is fundamental to identity-first security and an imperative for security and risk management leaders responsible for identity and access management."
- "Unlike the two other types of authentication credentials (knowledge and possession), **biometric traits are inherent to a person, thus providing a uniquely human basis** for authentication."
- "Biometric authentication potentially **frees the person from having to remember a password or carry a token, enhancing user experience.** Biometric traits also provide a robust basis for binding other authentication credentials to a living person via identity verification."

BIO-key is already seeing referred leads.

Gartner®

Source: Gartner Innovation Insight for Biometric Authentication

Customers Who Rely on BIO-key



BIO-key Go to Market Strategy

Paths to Market

- Expanding Channel Alliance Partner Program Globally
  - Deals from $25k to $500k+
- Industry Partnerships Providing Access to Low Friction Opportunities
  - AWS Marketplace, SailPoint
  - Deals from $25k to $500k+
- Direct Sales Targeted at Major Customers
  - Deals from $300k to $5M+
- Also Targeting users of Competing MFA Solutions:
  - With add-ons such as FIDO Passkey to eliminate the need/cost of tokens and phones
- Strategic Partnerships in Food Tech/Distribution and IoT & autonomous systems

Growth Strategies

Launch New Products, Enhance Solutions

- Introduce new biometric modalities
- Add functionality upgrades to WEB-key
- Add Provisioning and Governance modules to PortalGuard platform

Expand Global Reach

- Introduce Integrated Platform to International Partners & End Users
- Targeted Grow in International Partner Base to expand reach in select regions and verticals

Cross-Selling / Up-Selling

- Significant opportunity offer biometric solutions to PortalGuard & Swivel Secure customers
- Deploy PortalGuard IDaaS to legacy BIO-key/Swivel Secure customers

Grow Business Development Effort

- Find technology partners that complement integrated platform and expand opportunity base
- Offer biometric solutions to existing IAM vendors to broaden opportunities and enhance biometric brand
- Partner with other biometric modalities for integrations

Expand Sales and Partner Network

- Grow Channel Alliance Program (CAP) with new IAM partners (Resellers, MSP's, Integrators)
- Expand Master Agent program for SaaS sales
- Invest in Marketing Programs to drive broader awareness of Integrated Platform

Recent Strategic Growth Initiatives

BIO-key CyberDefense Initiative

- Building on a growing base of respected international military and security/defense customers, BIO-key formed its Cyber Defense Initiative to enhance its positioning as a critical provider of MFA, IAM and biometric enabled solutions to defense industry customers and prime contractor partners to support classified access environments aligned with EU, NATO and other cyber frameworks.
    - EU member states are expected to spend €350B or more on defense in 2026, including Germany which is boosting its 2026 budget 30% to €83B.
    - Europe's Readiness 2030 framework and ReArm Europe aims to mobilize over €800B in investments over 4 years.
        - This includes €150B for missile defense, drones, and cybersecurity.
    - NATO members also agreed to increase their defense and security spending to 5% of GDP by 2035 with 1.5% explicitly allocated to cybersecurity & security-related investments, including strengthening network defenses.

Recent Strategic Growth Initiatives (Cont.)

Fiber Food / Boumarang Inc. Collaboration & Investment

- Collaboration with Fiber Food Systems combines BIO-key's IAM expertise with Fiber Food's tech know-how and presence in food distribution channels. ***Fiber is integrating BIO-key's solutions to enhance security, streamline access, and improve operational efficiency in high-traffic environments including across schools, universities, and large institutional cafeterias***
    - As part of the agreement, BIO-key acquired 5M shares of Boumarang from Fiber in exchange for 595,000 BKYI shares. Boumarang is pioneering sustainable, long-range drone technology powered by AI-driven hydrogen fuel

Partnership with Engineering Solutions Provider Guinn to Transform Access-Control and Cyber Security for IoT & Autonomous Systems

- Guinn Partners provides advanced engineering solutions for robotics, drones, and electric propulsion systems
    - Guinn's customers include Amazon, Boy Scouts, Gel Blaster, and Lift Foils. Guinn is a key player in the electric Vertical Takeoff and Landing (eVTOL) aircraft market, which is being driven by advancements in battery tech, increasing demand for sustainable urban air mobility, and significant private & public sector investment. Market growth is projected at 55% from 2024 to appr. $23B by 2030 (Grand View Research)
    - Guinn is also developing fleet of semi-autonomous roadside mowers - control of access to fleet management systems and to individual mowers is critical for public safety and security

Expanding IP Portfolio

18 U.S. Patents including three most recently issued…

ENABLING NEXT-GENERATION CONTINUOUS BIOMETRIC USER AUTHENTICATION (Patent 10,984,085)

- ***Patent protects method of enabling next-generation continuous and passive biometric user experiences*** with its process for enrollment and continuous authentication
- BIO-key's intelligent data pre-processing and transformation algorithms sort through varying samples of biometric data, making reliable and accurate connections between samples of different sizes, resolution qualities and points of view – supporting continuous authentication of a user's identity during ongoing activity. Methods particularly valuable for mobile devices with in-screen fingerprint sensors, cameras and microphones providing a continuous stream of partial biometric samples over time

UTILIZATION of BIOMETRIC DATA (Patent 10,002,244)

- ***Enables BIO-key to capitalize on the transition of mobile devices to in-screen, "under glass" biometric sensors -*** though patent is broad enough to apply to sensors anywhere on a device
- Patent leverages continuous stream of partial fingerprint, facial or other biometric captures that occur as user interacts with a device. Technique enables a continuous, passive authentication for greater security with little workflow impact

ADAPTIVE SHORT LISTS & ACCELERATION of BIOMETRIC DATABASE SEARCH (Patent 10,025,831)

- ***Indexing method for quickly & iteratively searching a large-scale database of biometric records***
- Large-scale Automated Fingerprint ID Systems like that used by the FBI were once the exclusive province of big-budget agencies and enterprises. BIO-key's method uses 1 or more scans of a database with varying parameters, narrowing the field of candidates with each pass. Provides unique advantage in delivering cost-effective, 1-to-many ID solutions that avoid costly resource-intensive brute force scans

BIO-key is well positioned for inevitable growth in use of Identity Bound Biometrics

BIO-key Leadership

- **Michael W. DePasquale – Chairman & CEO** 25+ years in executive management, sales and marketing
- **Cecilia Welch – CFO** 20+ years of tech operational and financial management experience
- **Mark Cochran – President PortalGuard** 20+ years of experience in Security and IAM markets
- **Jim Sullivan – CLO, SVP Strategy** 25+ years enterprise sales in identity and access management, including with key customers AT&T, Capitec Bank, World Bank, NCR & Omnicell
- **Alex Rocha – MD BIO-key EMEA** 20+ years sales & management experience in EMEA mkt
- **Kelvin Wong – MD HK Subsidiary,** co-founder of World-Wide Touch Technology; 15+ years in manufacturing and marketing management, including biometrics & payments
- **Akintunde Carlton JeJe – MD Africa** respected, experienced executive with extensive knowledge & relationships in Nigerian & African markets
- **Mira LaCous – CTO** 30+ years solution development and product management, with creative inventiveness and expansive communication

Thank You!

Michael DePasquale
BIO-key Chairman & CEO
michael.depasquale@bio-key.com
732.359.1100

Investor & Media Contacts:
William Jones; David Collins
Catalyst IR
bkyi@catalyst-ir.com
212.924.9800

BIO-key®