BIO-key Identity and Access Management Solutions Deliver Greater Security, Efficiency, Flexibility and ROI

September 2024

www.BIO-key.com

BIO-key®

Nasdaq: BKYI

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, 2022 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.

BKYI at-a-Glance…

NASDAQ	BKYI
Recent Price	**$1.24**
52-Week Range	$1.21 - $12.06
Shares/Equivalents Out.	2.0m
Market Cap	**$ 2.5m**
Enterprise Value (EV)	$ 3.3m
LTM Revenue	$ 7.0m
Software/Recuring Rev. (ARR)	$ 5.8m
EV-to-LTM Revenue *	0.5x
Insider Ownership	~235k ~11.8%

* Peers OKTA, CYBR & CHKP trade at a 6x to 13x revenue.

Investment Considerations

Recurring Revenue Growth & Expanding Footprint

- Over 40M global users currently authenticate with BIO-key
- 2023 revenue rose 10.5% to $7.8M; Growth expected for full-year 2024
- 1'H operating loss trimmed to ($2.2M) vs. ($2.6M) (ex. $1.5M hardware reserve in 1H'23)
- Software/ARR has grown to $5.8M from $3M in 2020
- Blended gross margin over 70%

Compelling Valuation

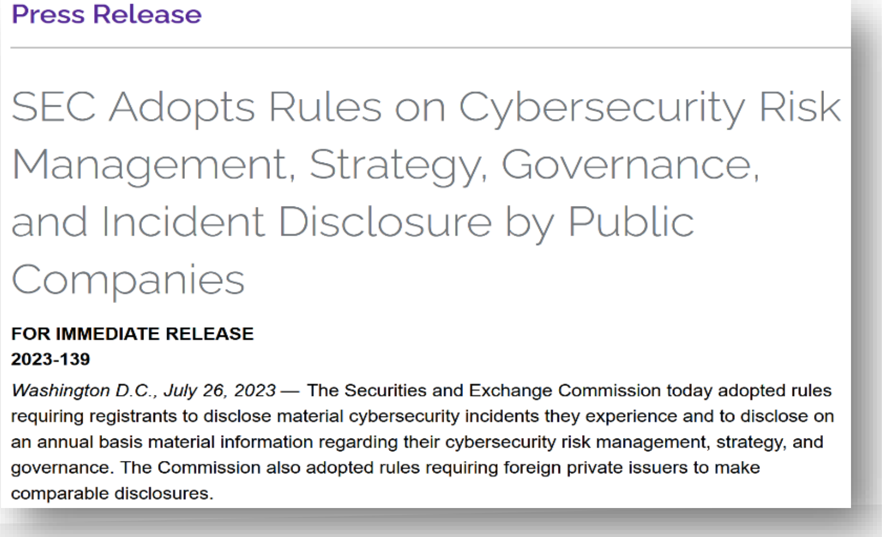
- BKYI trades at 0.5x EV/LTM Revenue vs. median 7.6x for identity comps (OKTA, CYBR, CHKP)
- High margin ARR base of $5.8M and growing
- Unrecognized value of public Nasdaq listing

Expanding Market Opportunity for MFA/Cybersecurity

- Failure of existing methods – breaches, ransomware, reliance on phones/tokens, high costs
- Cyber Insurance and regulations driving adoption of enhanced MFA solutions
- Growing BKYI market reach via large partners, direct sales and Channel Partners

Cybersecurity/MFA Market Opportunity

- **Cyber-Insurance mandates**
- Federal Trade Commission **(FTC Section 5 expansion)**
- Cybersecurity & Infrastructure Security Agency **(CISA) Dec 2023 guidance to manufacturers** to eliminate use of (easy to exploit) default passwords
- **Amazon Web Services mandates MFA** for most privileged users by mid 2024;
  - BIO-key Launched on AWS Marketplace in August 2024.
- Dec. 2023 **IT-ISAC** (Info Sharing & Analysis Ctr.) whitepaper called on SaaS and & cloud companies to embrace secure by default Principles (elevate security);
- SEC cybersecurity disclosure rules effective Dec. 2023.

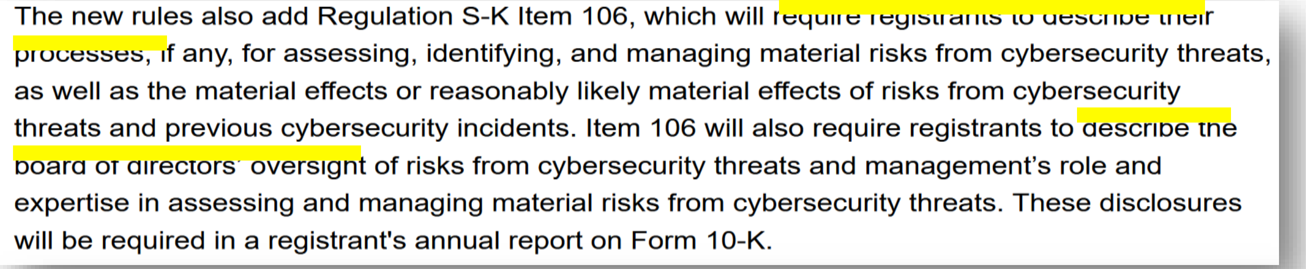


Press Release

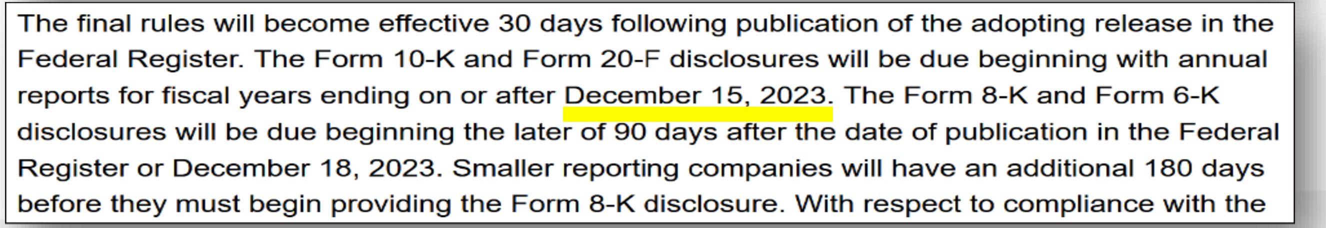
SEC Adopts Rules on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure by Public Companies

FOR IMMEDIATE RELEASE
2023-139

Washington D.C., July 26, 2023 — The Securities and Exchange Commission today adopted rules requiring registrants to disclose material cybersecurity incidents they experience and to disclose on an annual basis material information regarding their cybersecurity risk management, strategy, and governance. The Commission also adopted rules requiring foreign private issuers to make comparable disclosures.



The new rules also add Regulation S-K Item 106, which will require registrants to describe their processes, if any, for assessing, identifying, and managing material risks from cybersecurity threats, as well as the material effects or reasonably likely material effects of risks from cybersecurity threats and previous cybersecurity incidents. Item 106 will also require registrants to describe the board of directors' oversight of risks from cybersecurity threats and management's role and expertise in assessing and managing material risks from cybersecurity threats. These disclosures will be required in a registrant's annual report on Form 10-K.



The final rules will become effective 30 days following publication of the adopting release in the Federal Register. The Form 10-K and Form 20-F disclosures will be due beginning with annual reports for fiscal years ending on or after December 15, 2023. The Form 8-K and Form 6-K disclosures will be due beginning the later of 90 days after the date of publication in the Federal Register or December 18, 2023. Smaller reporting companies will have an additional 180 days before they must begin providing the Form 8-K disclosure. With respect to compliance with the

BIO-key Use Cases

Reducing Cyber Risk

Prevent cyberattacks, including ransomware.

300% increase in cybercrimes in the USA 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 & other compliance 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."

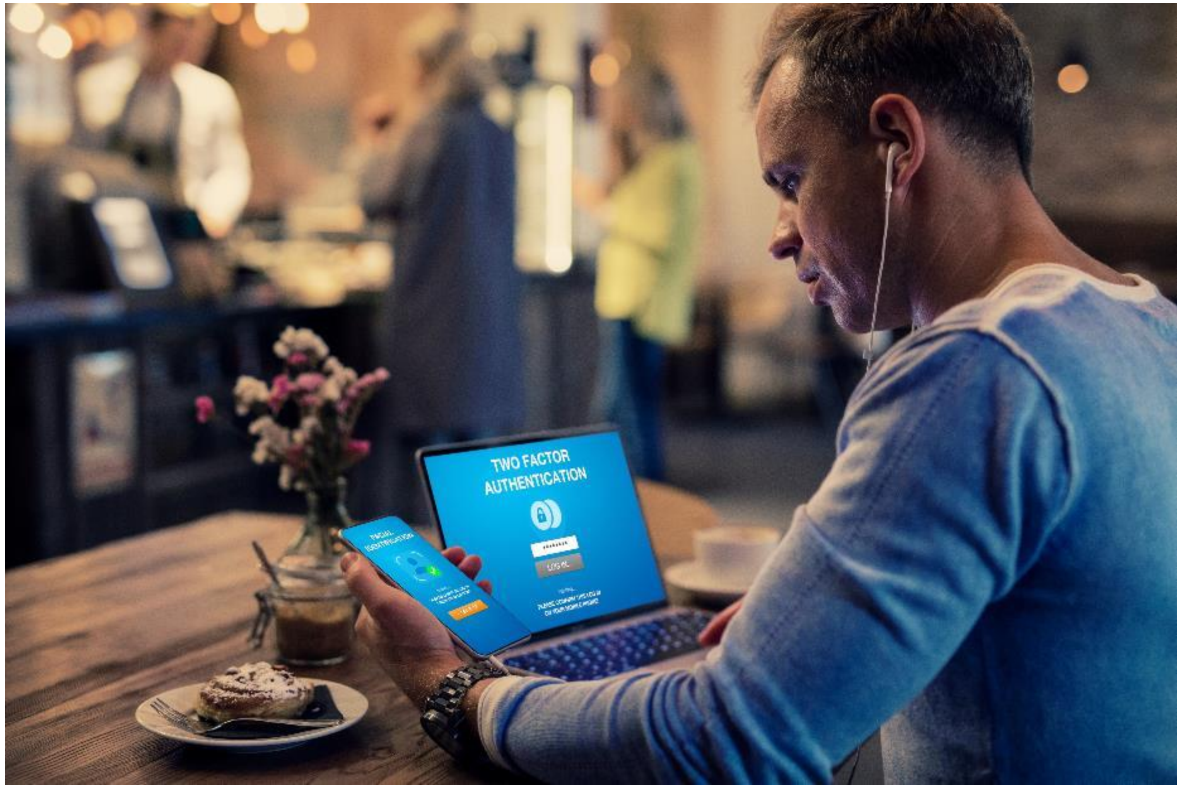
★★★★★

Mainstream MFA Offers Only “Device Assisted Authentication”

Phone Apps

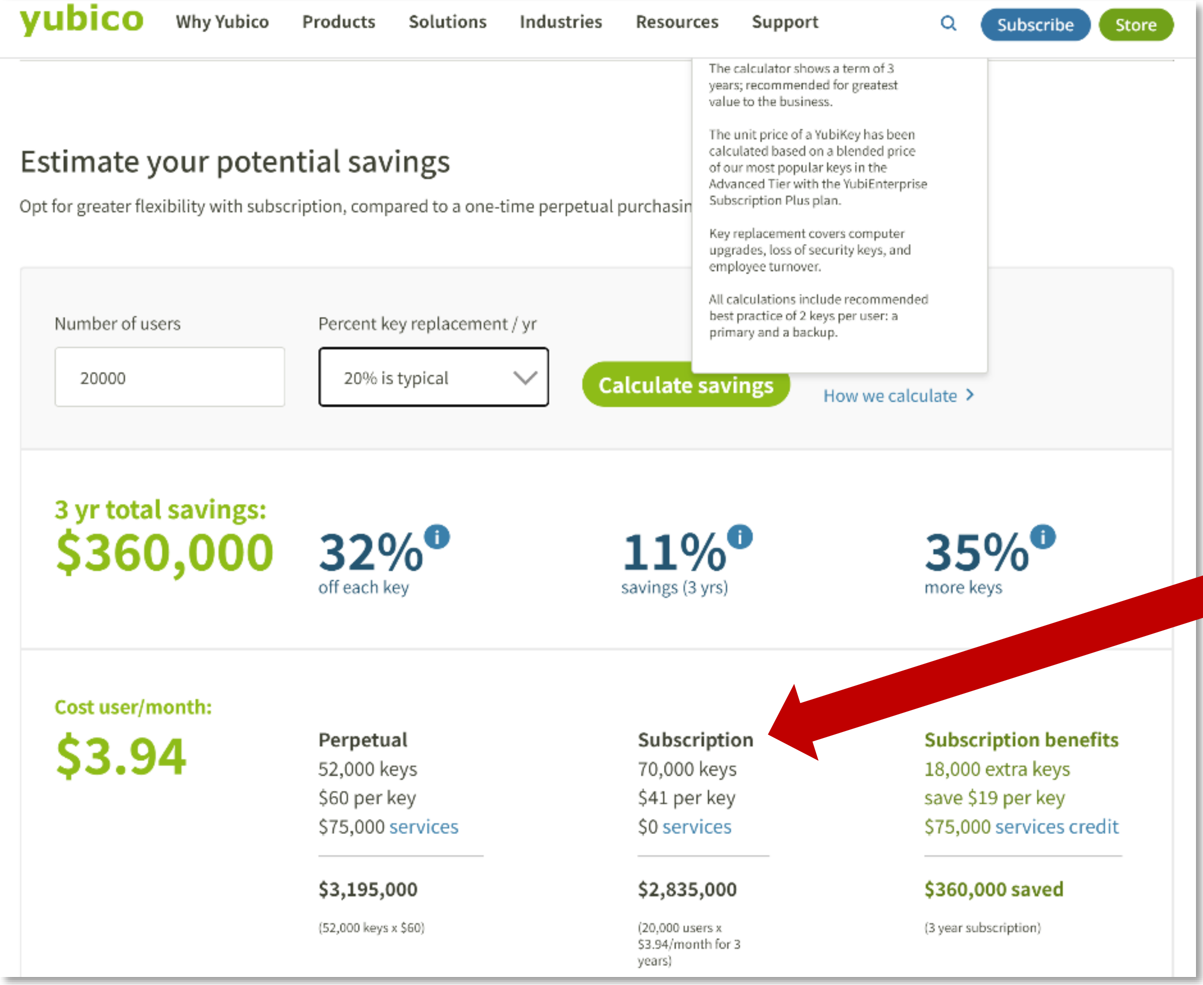
OR

User tokens



Significant Recuring Token Deployment Costs

20K users = $2.8M every three years



The calculator shows a term of 3 years; recommended for greatest value to the business.

The unit price of a YubiKey has been calculated based on a blended price of our most popular keys in the Advanced Tier with the YubiEnterprise Subscription Plus plan.

Key replacement covers computer upgrades, loss of security keys, and employee turnover.

All calculations include recommended best practice of 2 keys per user: a primary and a backup.

Estimate your potential savings

Opt for greater flexibility with subscription, compared to a one-time perpetual purchasin

Number of users: 20000

Percent key replacement / yr: 20% is typical

3 yr total savings: **$360,000**

32% off each key

11% savings (3 yrs)

35% more keys

Cost user/month: **$3.94**

Perpetual	Subscription	Subscription benefits
52,000 keys	70,000 keys	18,000 extra keys
$60 per key	$41 per key	save $19 per key
$75,000 services	$0 services	$75,000 services credit
$3,195,000	$2,835,000	$360,000 saved
(52,000 keys x $60)	(20,000 users x $3.94/month for 3 years)	(3 year subscription)

Subscription
70,000 keys
$41 per key
$0 services

$2,835,000

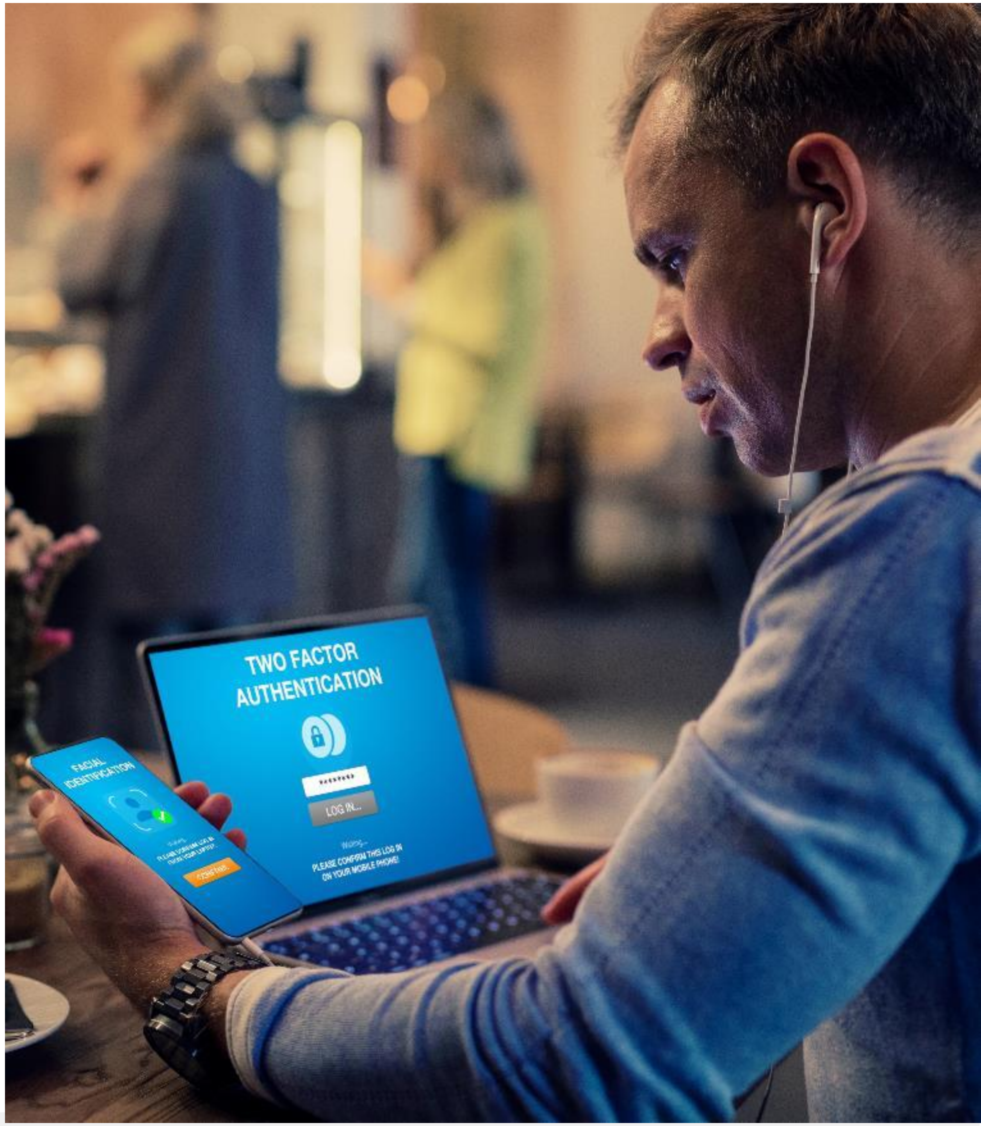
(20,000 users x $3.94/month for 3 years)

The Future is:

Phone-less. Token-less. Passwordless.

Phone Apps Work for Desk Worker Employees, but…

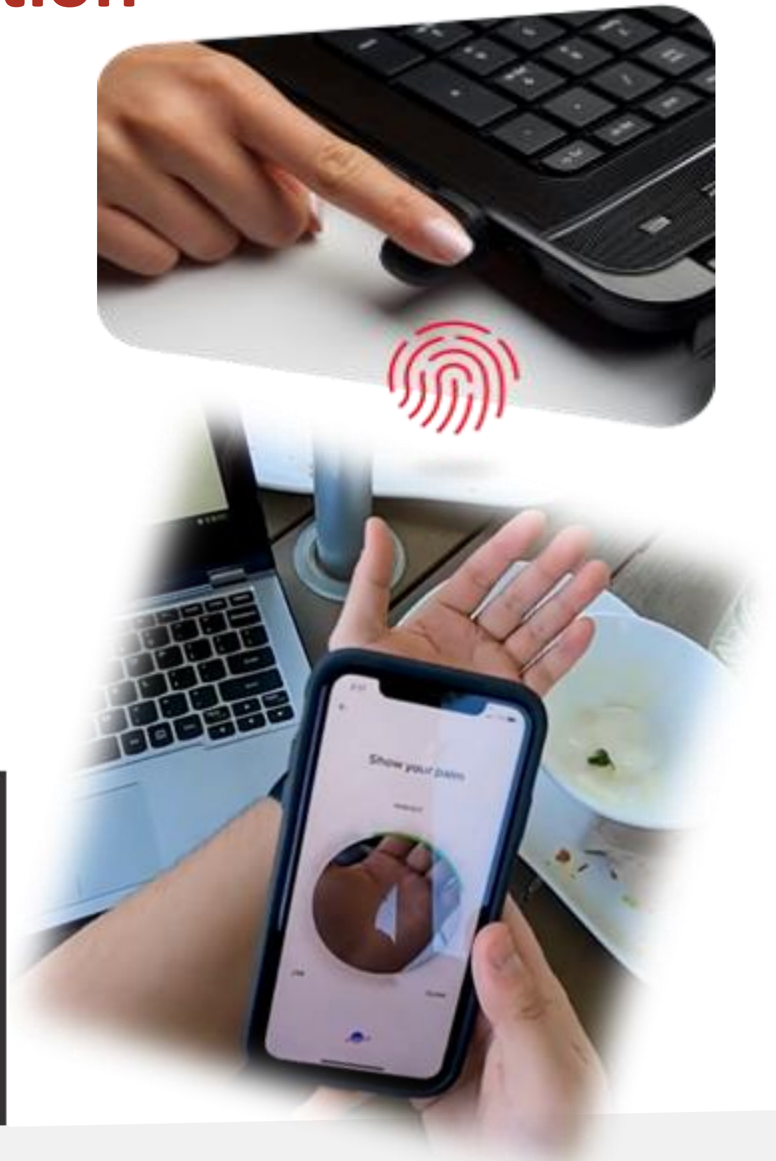
- Employees often must leave phones in a locker
  - Clean Desktop (Call Center)
  - Data Security/Privacy
  - No Distractions
  - Safety (Manufacturing, Shop Floor, Healthcare)
- Several states & EU require compensation for work-related personal phone use
  - California Labor Code § 2802(a): employer 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**.


TWO FACTOR AUTHENTICATION
LOG IN...
PLEASE CONFIRM THIS LOG IN ON YOUR MOBILE PHONE!
FACIAL IDENTIFICATION

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

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

- Centrally secured, privacy law compliant biometrics
- Patented, high security data and integrity protection
- Captured using USB fingerprint scanners or via 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
Eliminating Phones/Hardware Tokens for Restricted Environments

Huge Efficiency and Cost Savings versus Tokens

Uses BIO-key Biometric authentication as a drop-in replacement for FIDO2 hardware tokens when signing into shared workstations

Use Cases:

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

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

BIO-key Value Proposition

- Complete MFA offering with **Phoneless & Tokenless** authentication
  - Leveraging patented biometric capabilities **widely deployed/proven** in the highest-security settings in the world.
- Growing Base of Major Enterprise Deployments
  - Global Defense Ministries, Banks, Hospitals/Healthcare, Retail, Call Centers
  - Ideal for manufacturing, construction, healthcare
  - In Proof of Concept with industry leaders in:
    - Residential construction
    - Retail Grocery
    - Call centers
    - Automotive OEM

Gartner Underscores Value of BIO-key’s Capabilities

- “User authentication is fundamental to identity-first security and an imperative for security and risk management leaders responsible for identity and access management (IAM leaders). “

- “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 (UX).** Biometric traits also provide a robust basis for binding other authentication credentials to a living person via identity verification (IDV).”

- Already seeing referred leads

Gartner®

Source: Gartner Innovation Insight for Biometric Authentication, 20 December 2023

Customers Relying on BIO-key

IKEA

First National Bank LI

THE WORLD BANK

DEPARTMENT OF JUSTICE · FEDERAL BUREAU OF INVESTIGATION

Collier County

UNIVERSITY of DENVER

Henrico County VIRGINIA

NATIONWIDE CHILDREN'S When your child needs a hospital, everything matters.

SINGAPORE POLICE FORCE

DHL

NCR

du

afiniti

ORANGE Bank&Trust COMPANY

نوبكو nupco

AEON CREDIT SERVICE

UNION PACIFIC

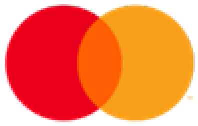
UNITED STATES SENATE

iQor

Marketron

Cleveland Clinic

vodafone



UNITED STATES COURTS

CAPITEC

CITY COLLEGE OF SAN FRANCISCO THE TRUTH SHALL MAKE YOU FREE

HERSHEY ENTERTAINMENT & RESORTS

NORTH ORANGE COUNTY COMMUNITY COLLEGE DISTRICT
Cypress College · Fullerton College · NOCE NORTH ORANGE CONTINUING EDUCATION

ORANGE COUNTY GOVERNMENT FLORIDA

BROOKDALE UNIVERSITY HOSPITAL MEDICAL CENTER

Coca-Cola Canada

Monash Health

CLEARENT

BIO-key Go to Market Strategy

Paths to Market

- Expanding Channel Alliance Partner Program with Global Reach
  - 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+

Use Cases

- Users of **Competing** MFA Solutions:
  - MFA with add-ins such as “FIDO Passkey” to eliminate the need for tokens and phones
  - **Eliminate Costs of** phone use reimbursement & tokens
- **New Prospects**
  - Value priced MFA solution with phoneless, token-less authentication options

Expanding IP Portfolio

18 U.S. Patents including three 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)

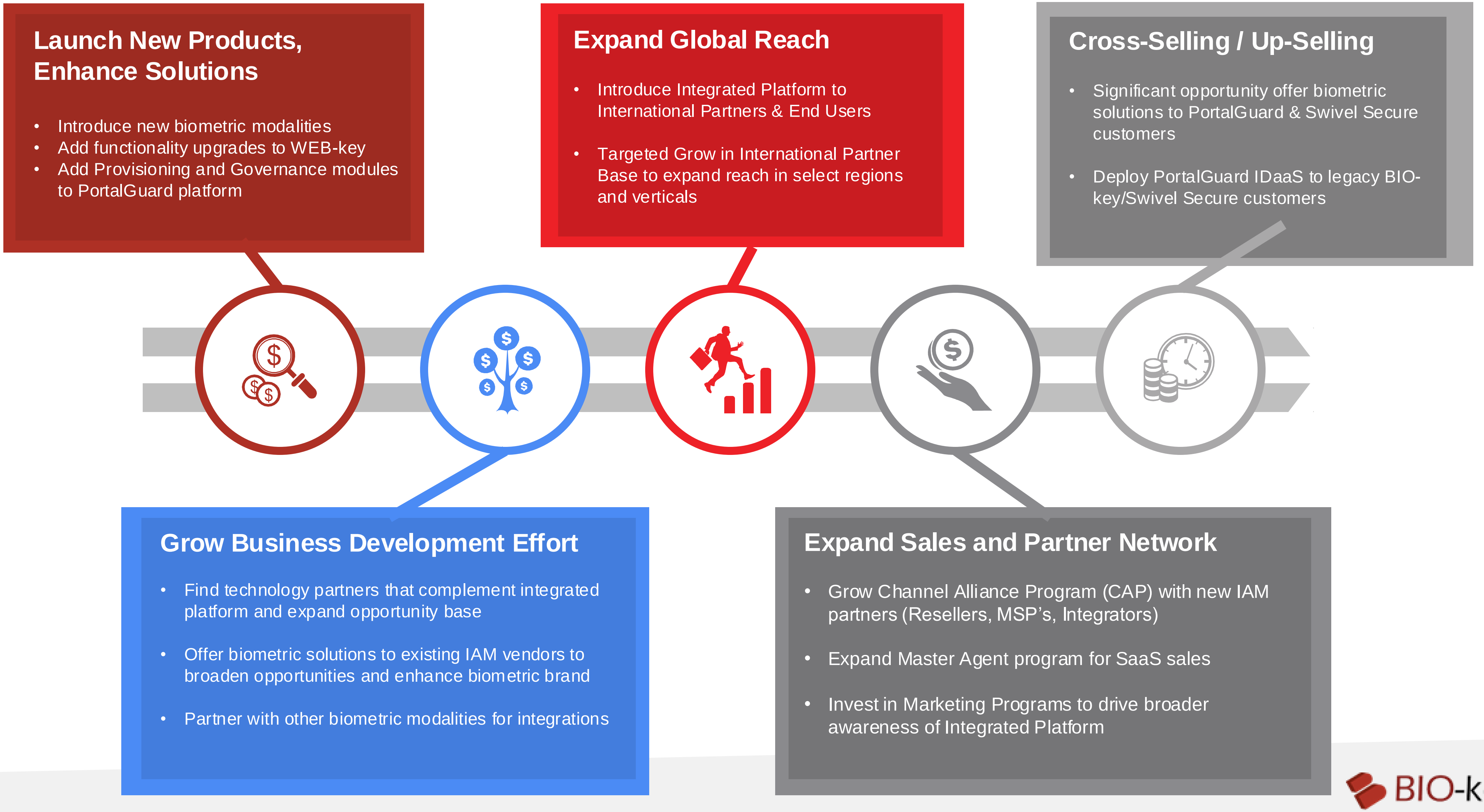
- ***Enables BIO-key to capitalize on the transition of mobile devices to in-screen, "under glass" biometric sensors*** **–** though patent is broad enough to apply to sensors anywhere on a device.
- Patent leverages continuous stream of partial fingerprint, facial or other biometric captures that occur 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

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

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 Global Reach

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

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

Cross-Selling / Up-Selling

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

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 – CEO of Swivel Secure Europe** Former sole stockholder of SSE with 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.
- **Galen Rodgers – VP Sales & Channel** 20+ years in channel program development, marketing, value selling, management, cybersecurity, process automation, coaching & team building – most recently with Ping Identity Corporation.

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®