Contact Centers Are Increasingly Looking Beyond Traditional Multi-Factor Authentication and Turning To Biometrics To Prevent Fraud

NEWS RELEASE BY **BIO-KEY INTERNATIONAL, INC.**

Wall, New Jersey | February 22, 2023 09:00 AM Eastern Standard Time
By Gita Karunakaran, Benzinga

BIO-key International Inc. (NASDAQ: BKYI) is a trusted provider of Identity and Access Management (IAM) and Identity-Bound Biometric solutions that are refining and changing the way Multi-factor Authentication (MFA) is used within IAM. The company competes with other access management software providers such as Okta Inc. (NASDAQ: OKTA); ForgeRock Inc. (NYSE: FORG); and Cyber Software Ltd. (NASDAQ: CYBR). BIO-key is innovating within the space to offer an easier and more secure way to authenticate the identity of employees and customers while managing their access across devices and applications.

BIO-key's cybersecurity solutions are currently being used to solve unique access management challenges across a plethora of industries, including financial services, healthcare, retail, education, manufacturing, and government. With almost every industry and business having an online presence today – and cybercrime and security breaches ever on the rise – there is an urgent need for reliable authentication and access management solutions.

Take the burgeoning customer contact [or call] center business, for example. In the U.S. alone, there are **34,013 Telemarketing & Call Center** businesses as of 2023 and their numbers have been steadily increasing by 2.3% per year on average between 2018 - 2023.

The global scenario is even more active, with the cloud-based contact center market seeing significant growth from **USD 6.80 billion in 2017 to USD 93 billion by 2022** – a whopping 25.2% Compound Annual Growth Rate (CAGR).

Contact Center Fraud Under The Spotlight

Fraud has always been considered a huge area of risk for contact centers, given that there is a vast amount of personal information being handled by the customer-servicing teams as well as the fact that contact center agents handle payment transactions as well. Contact center fraud is any instance when a caller tries to spoof the identity of a legitimate customer and obtain sensitive data.

Fraudsters can also try to process a high-value transaction on behalf of the customer, routing the funds to a different account/address that they can then access. The fraudster does this by obtaining sensitive personal identification information, which enables them to mimic the customer's

identity to a very believable degree of authenticity. They become privy to passwords, answers to secret questions, and even SMS OTPs (one-time passwords) through SIM spoofing, i.e. getting access and using your phone number.

Organizations have reportedly seen a spike in fraudulent calls since the start of COVID-19. Due to their rising numbers, contact center fraud has come under the spotlight in recent years, with enterprises looking to take concrete measures to combat scammers and fraudulent entities.

As organizations become more aware of the cybercrime landscape, they are paying more attention to their identity and access management and authentication solutions. They're beefing up their cybersecurity arsenal by going beyond passwords and PINs and introducing increased security protocols like traditional and advanced multi-factor authentication.

Some of the **best practices** that are used by contact centers include 'what you are' authentication, such as a voice biometric, over traditional 'what you know' methods like PINs and passwords to securely authenticate customer identity and effectively combat fraud.

They also adopt strategies such as providing focused training to the contact center agents and giving them access to only the most necessary customer information so that they do not end up inadvertently divulging additional personal information of a customer to a fraudulent caller.

While voice biometrics are in use to prevent external frauds, there is also a risk of misuse of sensitive information by contact center agents or past employees in cases where they may have malicious intent and misuse customer information for personal gain -- adding to the need for a robust access management strategy.

Contact center agents are known to regularly handle massive amounts of sensitive information on behalf of both the company they represent, as well as the customers who require their assistance. Therefore, in most contact centers, certain electronic devices like mobile phones that could be purposely or unwittingly used to capture sensitive information and relay it outside of the contact center are generally disallowed among agents.

In such scenarios, an MFA process involving one-time passwords or PINs sent to mobile devices may not be feasible. In addition, contact center best practices involve restricting access on a need-to-know basis and are set up in a manner that requires a higher level of authorization for sensitive transactions including address changes, large fund transfers, and the like.

What is needed is a simple and elegant solution that is not time-consuming and, at the same time, able to confirm the identity of the actual individual behind the access request.

How BIO-key Can Help

This is where companies like BIO-key, which offer a variety of flexible authentication solutions, could play a key role by enabling organizations to enforce stronger security and multi-factor authentication.

For example, for contact center employees who use shared workstations across multiple locations, BIO-key offers Identity-Bound Biometrics (IBB) with fingerprint scanners. This solution eliminates the need for users to carry around individual tokens or phones to verify their identity.

In addition to the enhanced security, IBB helps employees to smoothly, efficiently, and securely carry out their daily operations, including when they're working on shared workstations in multiple shifts at contact centers. In these scenarios authentication using physical tokens and mobile devices may not be viable choices due to security policies, high cost, and inconvenience. However, organizations can quickly implement station-based fingerprint scanners and a one-time enrollment for all employees with Identity-Bound Biometrics. In which case, users can enjoy a passwordless login experience at any device across any branch location – without needing to use phones or tokens.

BIO-key's IBB authentication methodology can reliably verify a person's identity so that organizations can have confidence that only authorized people are gaining access to systems and data.

BIO-key's cloud-based PortalGuard Identity as a Service (IDaaS) platform offers flexible options for SingleSign-on (SSO) and supports a range of multi-factor authentication methods, including IBB, phone apps such as Duo, Microsoft and Google Authenticators, smartcards, OTP, and knowledge-based questions and methods.

BIO-key's customers can access the power and convenience of Identity-Bound Biometrics to ensure the highest levels of integrity, security, availability, and accuracy that enterprise security requires.

BIO-key has a long track record with fingerprint authentication, and where applicable, its one-of-a-kind mobile app, it calls MobileAuth, could be used to eliminate the inconvenience, security risks, and costs of traditional authentication methods. MobileAuth can be used for multi-factor authentication (MFA) or passwordless workflows that make it easy to sign in with a simple palm or face scan – no password needed.

BIO-key says that implementing MFA is one of the core steps to achieving zero trust – an approach that treats every person and every device as a potential threat. PortalGuard offers the greatest flexibility and choice across the three main categories of authentication factors: something you know (passwords, PIN), something you have (hardware tokens, phone-based methods), and something you are (biometrics, such as a palm scan, fingerprint or facial recognition). Because IBB authenticates the identity of the actual user, according to BIO-key, there is no stronger way to establish trust and ensure secure access across an organization.

To learn more about the business applications of BIO-key's solutions visit the company webpage **here**.

*This article was originally published on Benzinga **here**.*

BIO-key is revolutionizing authentication and cybersecurity with biometric-centric, multi-factor identity and access management (IAM) software managing millions of users. Its cloud-based PortalGuard IAM solution provides cost-effective, easy to deploy, convenient and secure access to devices, information, applications, and high-value transactions. BIO-key's patented software and hardware solutions, with industry-leading Identity-Bound Biometric (IBB) capabilities, enable large-scale Identity-as-a-Service (IDaaS) solutions, as well as customized on premises solutions.

This post contains sponsored advertising content. This content is for informational purposes only and is not intended to be investing advice.

Contact Details

Catalyst IR- William Jones, David Collins

+1 212-924-9800

BKYI@catalyst-ir.com

Company Website

https://www.bio-key.com/

Tags

BIO-KEY INTERNATIONAL TECHNOLOGY PRIVACY CYBERSECURITY