



# Voice Biometrics for Contact Centers

A Call for Things to Come

voice

FORG+

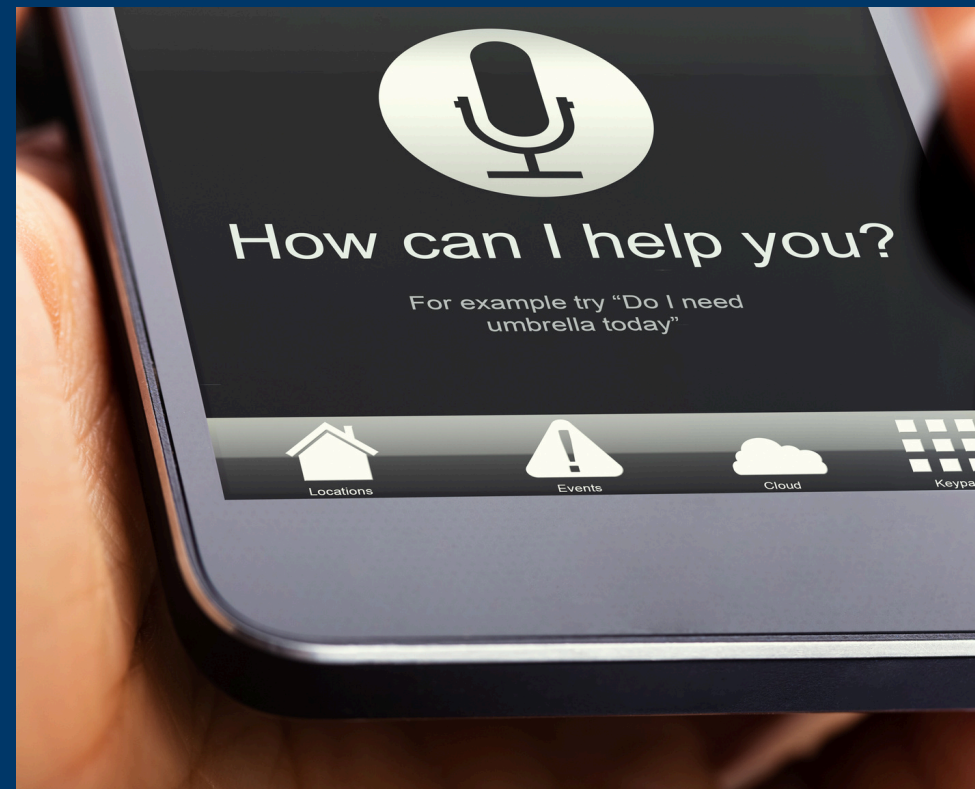


# PERSPECTIVES

## Biometrics: A Long History of Security

By James Cox, NRG Senior Consultant


Throughout history, humans have relied on physical characteristics for identification. Fingerprints, for instance, were utilized in ancient Babylon for business transactions. Today, biometrics encompasses a broader range of unique traits, including fingerprints scans, facial recognition, iris scans, and voice patterns. These biological markers, or "something you are," provide a more secure and convenient alternative for identity authentication compared to traditional methods such as passwords, PINs, or physical tokens.



# Voice Biometrics in the Contact Center

Voice biometrics is a technology that analyzes various aspects of a person's voice, such as vocal cavity shape, pitch, and dialect, for authentication purposes. In the contact center industry, this technology offers faster and smoother customer experiences along with enhanced security. For example, a customer contacting their bank can use their voice as a password, eliminating the need to answer multiple security questions. The system analyzes the unique attributes of their voice in real-time, thereby saving time and reducing the risk of fraudsters gaining access to accounts through stolen passwords or other personally identifiable information (PII).

**In Contact Centers, there are two primary approaches to voice biometrics:**



## Active Voice Biometrics

Customers actively participate by reciting specific phrases into the phone when prompted, establishing their voice print for future authentication.

## Passive Voice Biometrics



This advanced method operates subtly in the background, creating the customer's voice print during natural conversation with an agent. Authentication occurs automatically and in real-time during future calls, without requiring any specific action from the caller or agent.

This advanced method operates subtly in the background, creating the customer's voice print during natural conversation with an agent. Authentication occurs automatically and in real-time during future calls, without requiring any specific action from the caller or agent.

# The Rise of AI and the Challenge of Voice Cloning

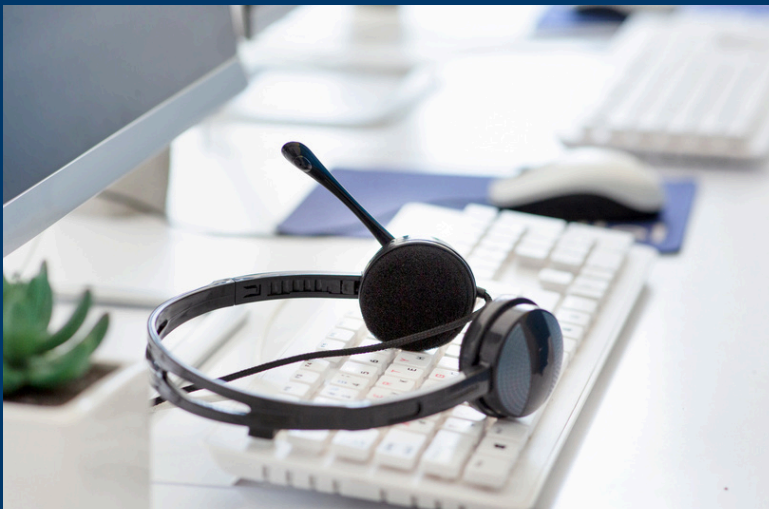
Despite the advantages of voice biometrics, the emergence of Artificial Intelligence (AI) and deep learning presents a new challenge. Fraudsters can exploit AI to synthesize voice prints, mimicking real individuals' voices for malicious purposes such as account takeover.

This risk underscores the importance of continuous improvement in voice biometric technology and the necessity of layering additional authentication methods on top of voice biometrics.

## Weighing the Benefits and Challenges of Voice Biometrics for Contact Centers

### Pros, Cons, and Considerations for Your Call Center

In continuation from Part One, exploring the potential of voice biometrics in enhancing customer experiences, saving time, and mitigating fraud risks remains essential for contact centers.



### Real Savings

Recent studies highlight the significant time savings associated with voice biometrics. Manual authentication by agents in sectors like insurance or finance averages about 40 seconds per caller.

For a contact center handling 100,000 inbound calls monthly, each requiring authentication at \$1.00 per minute, this translates to potential annual savings of approximately \$800,000.

## Cost and Implementation Efforts

It's crucial to recognize that the cost and implementation of voice biometrics can vary based on the chosen solution and its features. Contact center leaders must conduct a thorough analysis to determine if the potential savings justify the investment and effort involved.

## Identifying Suitable Candidates

Voice biometrics proves particularly valuable for contact centers managing sensitive information, such as financial, insurance, or healthcare institutions, where the risk of fraudulent account takeovers is high. Additionally, centers experiencing high call volumes from the same users may benefit from implementing voice biometrics.

---

**For a contact center handling 100,000 inbound calls monthly, each requiring authentication at \$1.00 per minute, this translates to potential annual savings of approximately \$800,000.**

---

## The Numbers Game: Fraud vs. Voice Biometrics

A recent survey across vertical markets indicates varying proportions of inbound calls requiring caller authentication, averaging at 60%. Notably, the finance and insurance sectors top the list, necessitating caller identification in over 78% of inbound calls. Source: The 2023 US Contact Center Decision-Makers' Guide (15th edition)" sponsored by NICE CX One.

While publicly available data on account takeover attempts may be fragmented, primarily due to security and companies not wanting to advertise vulnerabilities, industry reports indicate a substantial decrease in fraud rates for institutions utilizing voice biometrics compared to traditional methods. For instance, a 2020 study by Javelin Strategy & Research revealed that financial institutions leveraging voice authentication experienced a 30% reduction in fraudulent account takeover attempts.

# Addressing Emerging Threats

Account takeover attacks are not new and stem from data breaches that reveal Personally Identifiable Information (PII) on customers. This is a basic cybersecurity threat that has been around for decades. According to the Federal Trade Commission, between 2020 and 2022, pieces of PII on more than 300 million people became available to hackers and led to \$8.8 billion in losses.

Account takeover attacks are getting more sophisticated. With PII in hand, hackers analyze this information, matching it to real people. Technology is easily available that allows these hackers to spoof their phone number. Couple that with recordings of voices, more and more often found on the internet and mix in widely affordable and accessible generative AI systems, a voice deep fake can be generated that says whatever a user wishes.

Despite the potential risks posed by AI voice cloning, voice biometric suppliers actively develop countermeasures. These include:

**Liveness Detection:** Analyzing voice patterns to differentiate between live individuals and recordings.

**Continuous Authentication:** Monitoring vocal characteristics throughout a session, not solely during login.

**Challenge-Response Systems:** Requiring unexpected responses to further verify identity.



# Layered Authentication for Enhanced Security

Contact center leaders in high-risk markets, such as finance, insurance, and healthcare, should consider adopting layered authentication technologies. Options include geolocation (using a mobile phone's GPS coordinates), phoneprinting (detecting and analyzing background audio, source, and channel features), and other methodologies to notify agents of successful authentication and guide them to ask alternative questions if needed.

This layered approach can be strengthened by seeking solutions that enable the gathering and sharing of fraudster information among businesses, flagging potential fraudsters.

Voice biometrics presents compelling benefits for contact centers, including heightened security, improved customer experience, and cost savings. Although challenges exist, the technology continues to evolve to address them. Optimal security is achieved through multi-factored authentication layered with voice biometrics. By carefully considering the pros, cons, and additional considerations outlined here, contact center leaders can determine the suitability of voice biometrics for their operations.

**For more information about this topic, or to schedule a 15-minute discovery call, contact us today.**

