Omilia
Conversational Intelligence

Omilia Contact Center Security

Intelligent Verification & Anti-Fraud Solutions

Service That Customers Can Trust

The emergence of Generative AI has many positive uses but has also attracted fraudsters that exploit the technology for nefarious means. Fraudsters are taking advantage of easily accessible voice spoofing and deepfake technologies to attack contact centers with increasing frequency and success.

The time is now to invest and implement the appropriate systems that streamline customer authentication to maximize self-service and keep your customers' data and your contact center safe.

80% of financial industry respondents were very concerned with fraud originating in their call centers.[1]

Reduce fraud risk and prevent malicious attacks from breaching your contact center with our anti-fraud mechanisms and intelligent verification solutions, that are multi-layered acting at telephony, speech and behavioral layers.

Many new voice cloning solutions, Text-to-Speech (TTS) and Voice Conversion (VC) technologies, with synthetic speech that resembles a real person's voice, aid fraudsters in creating incredibly human-like speech. Deepfake detection technologies must keep pace with these innovations as they present new threats in the hands of fraudsters.

33% believe access and takeover (ATO) starts in the call center (60% for financial institutions).[1]

Our solutions integrate with enterprise transaction monitoring and alerting platforms, and can be incorporated into your broader anti-fraud ecosystem. This enables Omilia to detect suspicious transactions or behaviors and facilitate immediate fraud intervention across both voice and chat channels, to:

- Increase Agent and IVR Fraud Detection Effectiveness
- Increase Fraud Detection and Prevention Rates
- Decrease Customer Fraud Claims Rate
- Decrease Fraud Losses as a Percentage of Revenue

Liveness Detection

Fraudsters are increasingly using recordings or voice cloning for targeted impersonation attacks. Liveness Detection from Omilia enables call centers to actively detect and safeguard against:

- Synthetic voices - artificially generated through TTS or voice conversion technology based on the voices of the victims.
- Replay attacks - which use pre-recorded audio of the victim's voice.

Despite the fact that modern synthetic voices sound perfect, in essence they contain artifacts, which are imperfections or unnatural elements that can be present in the sound. These artifacts might be subtle, but they are still detectable by Omilia's well-trained neural networks and sophisticated AI systems designed to analyze and identify these imperfections in synthetic speech.

Omilia Voice Biometrics leverages a next-generation neural network of more than 100M parameters. Analyzing audio every two seconds, it detects synthetic and replayed speech with state-of-the-art precision, such as the 98% accuracy attained in the ASVspoof 2021 LA set benchmarks (see Figure 1).

Omilia's TTS detection system is continuously refined. After the training set is created, Omilia's Liveness Detection solution is tested against a wide range of TTS vendors, using samples that were not part of the model's training. We don't just test based on known factors; we also anticipate the unknown. Even if a new TTS system enters the market and our model hasn't been trained on it yet, we can still identify its synthetic speech production.

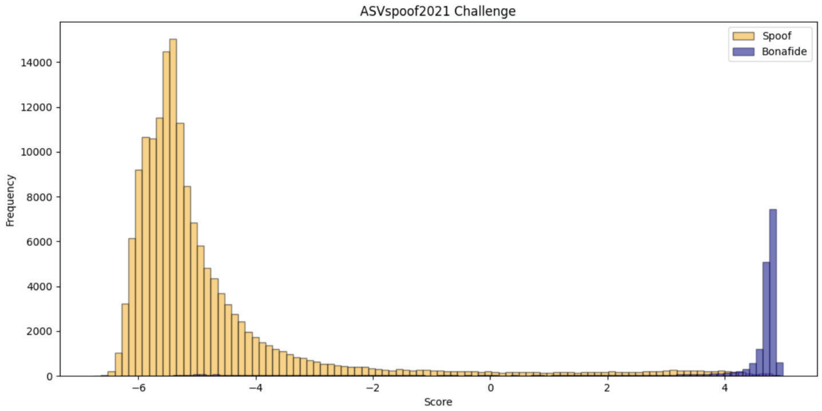


Figure 1. Histogram of scores in ASVspoof 2021 (LA set, combination of TTS and VC systems). Our model attains 2.67% Equal Error Rate.

Omilia's unique approach to contact center fraud ensures that every caller's voice is thoroughly examined for authenticity.

Fraud Prevention Case Study at Top 10 North American Bank

A well known large North American based financial institution was having trouble managing the nearly 80 million calls per year that came through its contact center.

Fraudsters were taking advantage of the IVR and contact center agents by using social engineering to gather data, enabling account takeover, fraudulent transactions, and fraudulent exfiltration of funds.

After implementing Omilia deepVB the bank achieved a **150% ROI within 9 months**, slashing account takeovers and preventing over **$10 million dollars in fraud loss** compared to previous years.

> “By enabling [Omilia] passive voice biometrics, natural language and ANI spoofing detection we were able to streamline the contact center experience for our telephone banking customers. This technology is a key pillar in both our customer care and fraud prevention strategies.
>
> **Contact Centre Product Owner**

Voice Biometric Verification

> Seamlessly and naturally verify callers with their unique biometric voiceprint in a conversation inside the IVR or with an agent.

IVR-Side Voice Biometrics

Callers enroll seamlessly without the need to utter specific keywords. Callers are verified against their enrolled voiceprint and self-served without any additional authentication steps.

Agent-Side Biometrics

Agents enroll callers via an embedded desktop interface. Verification results are displayed on the agent's screen, providing clear confirmation of the caller's identity.

Omilia Contact Center Security also protects against fraudulent enrollments by comparing new against existing enrolled users, and reporting those exhibiting high voice similarities.

Improving Customer Satisfaction and Reducing Costs

With just 2-5 seconds of speech, Omilia can reliably verify customers so they can securely self-serve. This seamless and secure method increases customer satisfaction and Net Promoter Score.

By automating the authentication process with voice biometrics, businesses can reduce the time to verify customers, increase the number of customers who can securely self-serve and drive faster agent handling time, all of which increase operational efficiency and reduce costs.

Businesses also have full control to calibrate verification thresholds and to configure stricter or looser verification based on their specific use case.

Enroll new voiceprints with **20 seconds** of audio

Voiceprint verification with just **2-5 seconds** of audio

Known fraudster detection in less than **10 seconds**

High accuracy: False Rejection Rate **10-15%** and False Acceptance Rate **0.1-0.5%**

Speaker Change Detection

Identify instances where a different person takes over the phone after the legitimate caller has successfully authenticated.

Real-time Alerts

Omilia continuously monitors each word of the conversation and determines where speaker change occurs, providing real-time alerts to the IVR Application or an agent of a potential account takeover.

By recognizing when a different voice takes over the phone, the system can trigger additional identification measures automatically.

Known Fraudster Blocklisting

Create a database of proven fraudulent voices so every call is checked and repeat offenders are blocked.

Increase Efficiency

Having a blocklist further streamlines the process of identifying and responding to known threats and helps agents avoid falling victim to these schemes. Agents and systems can quickly identify the flagged caller and take appropriate action without using extensive resources each time, leading to increased fraud detection rates.

Reduce Agent Stress and Workload

By filtering out fraudsters, agents can focus on serving legitimate customers, improving the overall efficiency and effectiveness of the contact center. Agents won’t have to spend time handling fake claims or false complaints, which can be both time-consuming and stressful.

Fraud Deterrent

A blocklist can deter fraudsters who may avoid targeting a contact center known to have robust anti-fraud measures, like Omilia Contact Center Security, including the ability to quickly recognize who they are and block their attempts, leading to a reduction in the cost associated with these attempts.

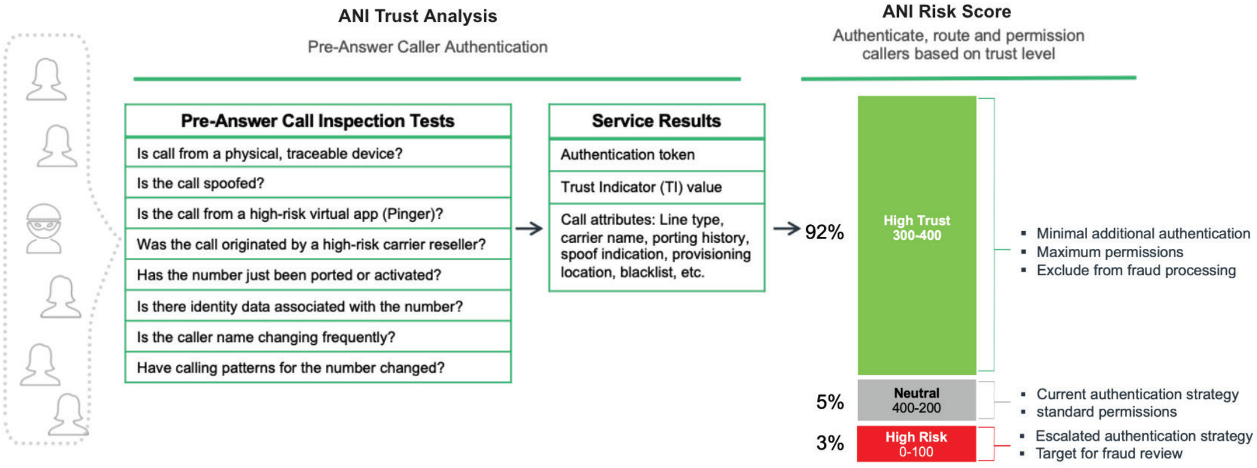
ANI Spoofing Risk Analysis

> Prevent attacks where fraudsters hide behind a spoofed phone number, one where they changed the ANI number in order to mimic the number of a real customer, or use a different ANI every time they call in order to avoid being detected.

We partner with Transunion network forensics that support 100% of carrier, mobile, landline and fixed VoIP devices, and inspect, confirm and authenticate the call, ensuring it is not virtualized, spoofed, shared, anonymously provisioned, illegitimate, altered or hacked.

Nearly **70%** of financial firms reported increased use of call spoofing into the call center.[1]

We analyze if the calling ANI number is unique, authentic and physical before a human or virtual agent even engages. End-to-end pre-call ANI inspection allows a contact center to inspect the calling device to optimize call treatment. It analyzes the phone number activity history in a database from 100+ enterprise brands, and provides access to exclusive call origin data only available to licensed carriers to detect risky or spoofed calls.


ANI Trust Analysis
Pre-Answer Caller Authentication
ANI Risk Score
Authenticate, route and permission callers based on trust level
92%
High Trust
300-400
Minimal additional authentication
Maximum permissions
Exclude from fraud processing
5%
Neutral
400-200
Current authentication strategy
standard permissions
3%
High Risk
0-100
Escalated authentication strategy
Target for fraud review

Pre-Answer Call Inspection Tests
Is call from a physical, traceable device?
Is the call spoofed?
Is the call from a high-risk virtual app (Pinger)?
Was the call originated by a high-risk carrier reseller?
Has the number just been ported or activated?
Is there identity data associated with the number?
Is the caller name changing frequently?
Have calling patterns for the number changed?

Service Results
Authentication token
Trust Indicator (TI) value
Call attributes: Line type, carrier name, porting history, spoof indication, provisioning location, blacklist, etc.

Behavior Analytics

Identify suspicious or out-of-the-ordinary behaviors that indicate fraud risk, allowing for timely intervention and prevention of an attack. For example, based on historical data, a customer always calls once a month at a certain time, but then they call and fail to authenticate multiple times within one hour.

Diverse Prevention Toolset

Behavior analytics operates independently of telephony. Because of this, it complements the tools and technologies you’re already using at the ANI and speech levels.

Streamline User Experience

Leverage comprehensive caller behavior blueprints to anticipate fraud attempts by understanding customer patterns. Identify risky behaviors and apply safeguards in advance to improve security and enhance the overall user experience.

Summary

Real-Time Alerting & Preventative Actions

Omilia anti-fraud analytics and real-time AI-based alerting mechanisms are built on top of our natural language model so the system can notify the human agent if there is an active ongoing pattern of malicious behavior and dialog engagement, or direct the bot to manage the dialog with a customer differently based on the risk score, for example, instructing it to route the call to the fraud specialist team.

Continuous Model Updates

Under continuous development and improvement release cycles, Omilia’s models remain up to date with the latest advancements in Generative AI and synthetic speech.

By thoroughly verifying the actual person behind every interaction, and reassessing the voice for the entirety of the interaction every time a caller speaks, Omilia achieves higher levels of confidence and accuracy in detecting synthetic voices. Omilia helps organizations protect their contact centers, their reputations and provide a more efficient and secure service for customers that ultimately increases trust, improves the experience and drives loyalty.

[1] Source: **2023 State of Omnichannel Authentication Report Mitigating Call Center Account Takeover Attacks, TransUnion**

The Role of Liveness Detection in Voice Biometrics: An Evolving Security Landscape
Omilia's Voice Biometrics (VB) technology, enhanced with liveness detection, remains a powerful authentication factor, providing a robust layer of security against fraudulent access attempts. Liveness detection is specifically designed to counter emerging threats such as deepfake audio, recording/replay attacks, and synthetic voice fraud, ensuring that authentication is based on a real, live human voice rather than a manipulated or pre-recorded sample.

However, as with all security measures, authentication technologies exist within an ever-evolving threat landscape. The rapid advancements in artificial intelligence and voice synthesis mean that adversaries are continuously developing new techniques to bypass biometric security. As deepfake technology improves, new forms of attack will inevitably emerge—some of which may initially evade detection until our models are updated to recognize these novel threats.

Omilia is fully committed to staying ahead in this ongoing arms race. Our liveness detection technology is continuously trained and updated to recognize new patterns indicative of synthetic speech, enabling our system to adapt to the latest fraud techniques. Nevertheless, as with any cybersecurity measure, there is no such thing as an infallible system. At any given moment, a previously unseen attack vector may momentarily surpass existing defenses until countermeasures are developed and deployed.

This reality underscores why Voice Biometrics—despite its strength—is not and should not be the sole factor of authentication. Instead, it should be part of a multi-factor authentication (MFA) strategy, combining other security layers to provide the highest level of protection. This approach mirrors the broader cybersecurity landscape, where encryption, intrusion detection, and behavioral analytics continuously evolve to keep pace with increasingly sophisticated threats.

Omilia remains at the forefront of voice security innovation, ensuring that our customers benefit from the most advanced and adaptive biometric solutions. While no system can offer absolute security against future threats, our ongoing investment in AI-driven fraud prevention ensures that Omilia VB with liveness detection remains one of the most effective and resilient authentication solutions available today.

Omilia is a Conversational AI pioneer, delivering the highest quality, automated voice and chat solutions for Customer Service. Omilia owns and provides state-of-the-art technology in Conversational AI, enabling clients to improve their customer experience, shorten response times, and reduce costs. The Omilia Cloud offering allows businesses to effortlessly identify, authenticate, and serve customers across any channel, with ready-to-go integrations, and pre-built solutions trained for specific use cases.

Omilia Natural Language Solutions Ltd. Inomenon Ethnon 50, Thekla Konteatis Court, Off. 41, 6042, Larnaca, Cyprus
omilia.com   hello@omilia.com