AUTHENTICATION IN THE CONTACT CENTER

INDUSTRY PERSPECTIVES AND BEST PRACTICES

INTRODUCTION

Customer authentication is a critical process in protecting customers and the enterprise against the increasing threat of fraud that is targeting the contact center. However, this time-consuming process adversely affects operational efficiency, comprising more than 25% of average handle time (AHT). Customers also don't appreciate being subjected to a barrage of security questions at the outset of each call. Moreover, current authentication methods, such as knowledge-based authentication and caller ID are proving inadequate against ever more sophisticated fraudsters.

To that end, enterprises are faced with the significant challenge of making the authentication process quick and easy, yet more secure.

This white paper discusses customer authentication and how voice biometrics presents a unique solution that addresses the business needs of all key stakeholders in the authentication environment – customers, customer service reps, risk managers, regulators and those measured on operational efficiency and customer experience.

AUTHENTICATION TECHNIQUES

Three factors predominate when authenticating the claimed identity of an individual:

> **Something you know** – Most often refers to PINs or passwords used in association with a personal ID (like a proper name, account number, email address) in order to support access to a system or service.
>
> **Something you have** – A "physical token" such as a dongle or electronic device that is known to be in the possession of the individual with the claimed identity. Examples are RSA SecureID tokens, but increasingly mobile phones can be used in association with a system that delivers "one-time-passwords" (OTPs) as a text message.
>
> **Something you are** – Unique attributes of an individual can be used as a strong assertion of identity. The most accepted forms are fingerprints, photos, iris scans, palm and vein patterns, and voiceprints.

It is widely accepted that something you are is the most robust in terms of authentication and security, however using multiple factors in parallel constitutes best practice.

REGULATORY ENVIRONMENT & IMPLICATIONS

The move to layered, multi-factor authentication pays homage to regulatory bodies and industry standards boards, such as the Federal Financial Institutions Examination Council (FFIEC), the European Banking Authority and various anti-fraud task forces around the world. In many countries, these bank bodies mandate that multi-layer, multi-factor authentication be in place to protect privacy and prevent fraud. Yet the idea of employing more than one factor toward authenticating customers is a matter of common sense.

> ***".. Institutions should no longer consider such basic challenge questions (like mother's maiden name) as a primary control, to be an effective risk mitigation technique… "***
>
> *Federal Financial Institutions Examination Council, June 22, 2011*

Unfortunately, the focus on multi-factor authentication leads to increased complexity as more layers are employed. Financial institutions use device profiles (operating system, location and other unique in characteristics), out-of-band authentication and behavioral analysis to define the level of risk associated with a new caller. The result only further exacerbates previous pain points, with multi-factor authentication extending the length of a call or adding to a customer's workload.

Industry analysts have also weighed in on the delicate balance between multi-factor authentication and customer convenience and are espousing the inclusion of voice biometrics as a secure and convenient business tool.

> ***".. Focus on improving caller authentication, and don't rely on easily exposed data, such as dates of birth and account numbers, to identify callers. Instead, consider using a combination of PINs, biometric voice recognition and reliable caller ID.. "***
>
> *Gartner, Nov 2011*

CUSTOMER PERCEPTIONS & PAIN POINTS

This increased complexity challenges enterprises to strike the right balance between security and convenience when authenticating end-customers. However, until now service providers have struggled to solve the challenge of the increasing need for security and convenience. This has resulted in some key pain points for enterprises and consumers alike.

Customers don't like the authentication process

Research conducted by Opus Research found that of 1,000 consumers who had made recent calls into customer care contact centers:

- 85% of customers don't like the current authentication processes
- Most customers want to talk to a person – 80% of all callers prefer to go straight to a human operator
- In comparison to live authentication respondents found IVR authentication highly impersonal (77%), frustrating (74%) and slow (71%)

In summary, the most common forms of caller authentication are the ones that people find most annoying.

Reliance on "something you know" adds time and expense

Opus Research uncovered a general consensus that there is an over-reliance on "something you know," when it comes to customer-facing authentication.

> ***"..This "last century thinking" that adds both time and expense has led to dissatisfaction both by customers and by security professionals, who have found such systems to be susceptible to fraudulent access by increasingly determined criminals .. "***
>
> *Opus Research, April 2013*

Similarly, the US Contact Center Decision Makers Guide found the authentication process contributes to increased handle time

> ***"..While the authentication process can take up to two minutes, most leading enterprises looking to protect their contact centers and their customers will typically report authentication times of 45 to 60 seconds .. "***
>
> *US Contact Center Decision Makers' Guide, April 2013*

Customers have too much to remember

Customers have interactions with multiple service providers, with each one having different and increasingly complex authentication processes and password requirements. As a result, customers are overburdened with too many passwords and too much to remember. The increasing complexity of the authentication process is further contributing to this phenomenon and false reject rates of legitimate customers continue to rise, which drives significant negative impact on customer experience.

Too many dongles, key-chains and tokens

Customers are also being burdened with having to carry multiple tokens ranging from dedicated dongles, to key chains or mobile phones. The "nuisance" factor of having to carry them around and "choose the right one" when it is time to deploy continues to drive negative customer sentiment. Furthermore, one-time passwords have also been found to be susceptible to hacking and fraud.

Still not secure

Despite all of the aforementioned pain points, fraudsters are still managing to circumvent current authentication techniques and carry out their fraudulent schemes. Conversations will leading analysts indicated that fraudsters will successfully to bypass traditional knowledge based authentication between 20% - 50% of the time.

VOICE BIOMETRICS AS AN ALTERNATIVE

What is voice biometrics?

Voice biometrics uses voice patterns to produce unique identification for every individual, using both more than 50 physical and behavioral factors. Behavioral characteristics include pronunciation, emphasis, speed of speech, accent, while physical characteristics include the unique physical traits of your vocal tract, mouth shape and size, nasal passages, etc.

Text-independent voice biometrics also allows a voice print to be identified in real-time through natural conversation without being reliant on a specific phrase to accurately identify an individual.

Voice biometrics as an alternative for secure and convenient authentication

Simply put, voice biometrics allows enterprises to leverage each customer's unique voiceprint as their identifying credential for secure authentication. In fact, a voice verification's strength lies in its ability to work in remote channels, such as over the phone or mobile, making it a viable identity verification solution for contact centers.

From a technological standpoint, while voice biometrics is by no means a new technology, it has now reached the tipping point where it is now viable for business critical authentication

> ***"..Voice verification systems are now delivering levels of accuracy and security that have proven robust enough for banks and insurers.. "***
>
> *US Contact Center Decision Makers' Guide, April 2013*

In support of this, respondents to a 2013 survey conducted by Opus Research recognized that voice biometrics technologies have "matured" significantly in the past year. Based on trials or pilots, they were well aware that accuracy had improved and experienced individuals (both employees and customers) were expressing an appreciation of the convenience that voice-based authentication presented.

Previous challenges to voice biometrics implementations

As previously mentioned, voice biometrics is not a new technology and in fact the major impediment to its widespread adoption has been the requirement for customers to actively enroll in the program. Savings from voice-based authentication are only derived from enrolled customers. However, actively enrolling customers is expensive and operationally challenging. The development of Seamless™ Passive Enrollment has overcome these challenges, so now voiceprints for the vast majority of customers for can be unobtrusively obtained in the course of a conversation -– all with no customer effort or impact

VOICE BIOMETRICS VIS-À-VIS KNOWLEDGE-BASED AUTHENTICATION

It is important to assess the impact of voice biometrics vis-à-vis the status quo that is in place today regarding customer authentication. To that end, voice biometrics should be assessed in light of its performance with comparison to knowledge-based authentication (KBA) across the dimensions of convenience, security and accuracy.

Convenience

KBA is time-consuming and customer effort intensive, as customers are put through a series of questions regarding the account details or previous behaviour. Voice-authentication simply requires the customer to converse naturally with the agent to be authenticated.

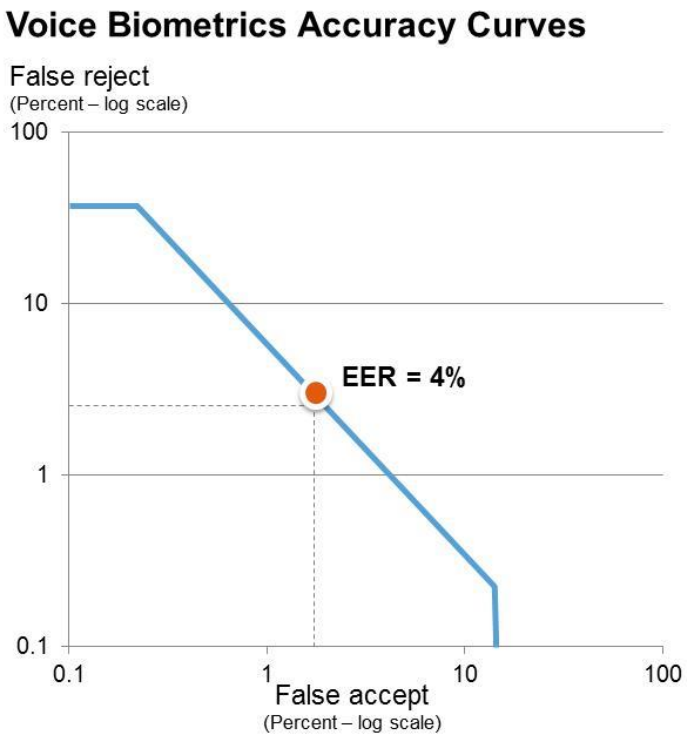
Security & Accuracy

The key measures for accuracy are *false accept* and *false reject* ratio:

- **False reject –** engine wrongly identifies a legitimate caller as illegitimate
- **False accept** – engine wrongly identifies an illegitimate caller as legitimate

While KBA is the standard authentication method across a large majority of enterprises, it is by no means failsafe. Leading analysts estimate that fraudsters will successfully to bypass traditional knowledge based authentication between 20% - 50% of the time. In the most optimistic scenario this translates to a false accept ratio of 20%. Conversely, the average agent has one failed authentication every hour (false reject), meaning that on average one of every eight calls (or 12.5% of calls) are false rejects.

Voice biometrics has an equal error rate of 4%, meaning that on average it will give the correct determination 96% of the time. However, this can be calibrated for lower false accept tolerance at the expense of false rejects, and vice versa. For example, setting the false accept ratio to below 2% will result in false reject ratio of approximately 10%. Significantly better than traditional KBA for both false accepts and false rejects.



IMPLEMENTATION OPTIONS

Given that NICE Seamless™ Passive Enrollment has solved the challenge of enrolling millions of customers into voice-authentication programs, enterprises have several options regarding how to rollout the system:

- **Switching to voice-authentication only** – once the system is tuned and calibrated, voice-authentication can completely replace traditional authentication methods, such as KBA
- **Employing voice-authentication as a primary factor** – employing the voice-authentication solution as the primary factor and leveraging additional security tokens only on high risk interactions
- **Employing voice-authentication as a secondary factor** – employing voice-authentication as an additional factor to the current verification process of PINs, passwords and authentication questions

Of course, enterprises have also employed a gradual deployment strategy where only certain lines of business and customer segments have been involved in early stage “pilots”, to ensure key learnings and best practices can be applied to the wider rollout.

The following section will discuss case studies of different rollout from previous deployments around the world.

CASE STUDIES

Leading Financial Institution in the United Kingdom

Deployment overview

The system was rolled out on 600 seats focusing only on wealth management customer segment. This focused customer group were asked to opt-in into the system, which would enabled them to skip the ID&V process to emulate the same experience that the client would have in a face-to-face meeting with their banker.

Impact

- 84% of frequent callers were enrolled within the first 6 months
- 95% of enrolled customers successfully verified
- 93% of customers were highly satisfied with the service
- 15% improvement in handle time

> ***"..Knowledge-based authentication is disruptive and gets in the way of client interaction… intrusive security questions have now been replaced by customers simply speaking, in their natural voice .. "***
>
> *Vice President*

Leading Financial Institution in the Slovakia

Deployment overview

The system was rolled out on 600 seats in November 2013 across the entire customer base on an opt-in basis. Customers were enrolled in branches after being successfully verified by bank tellers. The voice biometrics implementation allows customers to skip a lengthy authentication process which requires multiple tokens and one-time-passwords.

Impact

- The bank launched a TV campaign to gain awareness and gain consent via branches
- 90,000 customers enrolled in the first fours month of the deployment
- Authentication time was reduced from 80 seconds to 28 seconds on each call

> ***"..As the first bank in Central Europe to deploy a voice biometrics solution in this way, we allow our clients to access our banking services with a unique security tool they carry with them at all times – their voice.. "***
>
> *CEO and Chairman of the Board*

Leading Financial Institution in the Russia

Deployment overview

NICE's Real Time Authentication solution was implemented as part of the organization's alignment for improved authentication and better customer experience. The system was rolled out in two phases, with 70 seats in

November 2013 and on 700 seats in March 2014. The solution uses NICE Seamless™ Passive Enrollment to passively enroll customers into the system on an opt-out basis by leveraging previous recording to create voice prints. The system will replace the manual authentication process, where additional security questions may be employed in high-risk interactions.

Impact

- Authentication time reduced by ~30 seconds
- Over 100,000 voice prints created in the first 2 months
- Over 90% successful verification of enrolled customers
- Over 95% of eligible calls are successfully enrolled

> ***“.. After seeing the results of the system we will only be using voice biometrics to authenticate our customers. In certain cases of high-risk, we will employ NICE’s dynamic security questions to guide our agents for an additional security layer.. ”***
>
> *Senior Executive*

Leading Financial Institution in the United States

Deployment overview

NICE’s Real Time Authentication solution is being implemented as part of the bank’s push for operational efficiency and improved customer experienced. The system is being rolled out in two phases, with 50 seats in September 2013 and on 10,000 seats in July 2014. The solution leverages NICE Seamless™ Passive Enrollment to passively enrol customers without the need for consent. The system will replace the lengthy authentication process, with additional security tokens employed only in high-risk interactions.

Impact

- 87% verification rate in a live mono environment
- Over 40,000 customers passively enrolled in the first month (Phase I)
- Authentication time reduced from 65 seconds to 27 seconds

> ***“..Voice biometrics will allow us to identify customers based on their voice characteristics, offering protection and convenience in one solution.. ”***
>
> *Customer Banking Technology executive*

Leading Financial Institution in the Brazil

Deployment overview

NICE’s Real Time Authentication solution was implemented on 200 seats in January 2014, as part of the bank’s push for operational efficiency and improved customer experienced. NICE Seamless™ Passive Enrollment is being leveraged to passively enroll customers without the need for customer consent.

Impact

- 50,000 customers enrolled in the first few weeks of the deployment
- Approximately 10,000 successful authentications

SOURCES

Caller Authentication: Likes, Dislikes and Preferences, **Opus Research**, July 2012

Identity Theft Resource Center

Look Who's Talking: Financial Institutions' Contact Centers Under Attack, **Aite Group**, April 2013

The Case for Passive, Voice-Based Authentication, **Opus Research,** April 2013

U.S Banks Are Improving Much Needed Online Security but Their Phone Channels Need More Attention, **Gartner**, Nov 2011

U.S. Contact Center Decision Makers' Guide, **Contact Babel**, April 2013