Authenticating Customers with Nuance Voice Biometrics Solutions

Understand how authentication impacts call center interactions

Explore the value of voice biometrics in customer care

Gain insight into voice biometrics technology

Redguides for Business Leaders

Brett Beranek
Russell Warren
Executive overview

You already know that you need to deliver consistent, effective customer service (over various channels) that is secure and cost effective. But how? Today various customer care channels are available, such as web portals, smartphone apps, interactive voice response (IVR), and contact centers. These channels tend to begin with a negative experience for both the customer and the business. In addition, to broaden their services, businesses want to extend access to mobile customers and their workforce by taking advantage of mobile device capabilities to improve operational efficiencies and reduce costs. However, the growth and diversity of mobile platforms adds to the complexity of managing and securing endpoints.

The need for secure interactions by using an authentication process often leads to complex alphanumeric passwords that are challenging to remember and enter. Within the IVR, personal identification numbers (PINs) pose a similar challenge for users. For example, callers to a contact center must often answer several security-related questions from agents (interrogation process) to verify that the callers are who they say they are. Beyond an inconsistent and unpleasant experience for the customer, these authentication methods directly affect the bottom line. Also, failure to gain access when using such authentication pushes customers to use the business call center to avoid providing their personal credentials. This additional traffic to the call center increases overall operational costs.

In many situations, traditional authentication methods fail to deliver on their primary purpose of securing customer accounts and confidential data as demonstrated by rising losses because of fraud. Voice biometrics offers an easy, quick, and positive experience for customers, in addition to reducing costs and fraud risk. IBM®, jointly with Nuance Communications, Inc., can provide your business with voice biometric solutions that offer consumers a single credential. You apply this single credential across customer service channels, such as implementing it within the enterprise contact center transformation, a customer care and insight solution, or a mobile initiative.

Nuance Voice Biometrics products meet the dynamic security needs of your business, government agencies, and other organizations. These products rely on the most advanced and accurate speaker verification technology that is available. By using these products, your organization can improve security, ensure regulatory compliance, reduce costs, and deliver increased convenience to the customers you serve, regardless of the communication channel.

This IBM Redguide™ publication highlights the challenges of providing automated customer service and the value of the Nuance Voice Biometrics solutions. It describes the Nuance Voice Biometric solutions and identifies key features of the solution. In addition, it includes case studies and scenarios that provide insight into real-world usage of the solutions.
## Business challenges of authentication

Many businesses have the perception that their existing automated customer service channels provide a low-cost solution to servicing their customer. In reality, these approaches are costing them in lost opportunities and revenue. Also, supporting and maintaining these approaches have significant tangible costs. In many cases, businesses believe that their existing channels are sufficient and that additional investments in this area are not warranted, yielding low returns.

However, businesses must consider the following key issues:

- The cost of operating call centers
- Damage to a customer's experience and potential damage to the customer relationship
- Cost of web and mobile application authentication
- The trend to mobility

## Costs of operating the call center

The costs of authentication can be significant in a call center. The ContactBabel report *The US Contact Center Decision-Maker’s Guide* states: “It takes an average of 26 seconds to verify a customer’s identity manually, and this mounts up considerably: the US contact center industry spends around $20 billion each year, just to verify that the caller is who they claim to be”. In cases where customers do not prepare for the interrogation process by having all of the pieces of information at hand, the Identification and Verification (ID&V) process can take several minutes.

Frequently, the ID&V process delivers poor security value because it is vulnerable to social engineering and information attacks. This issue provides malicious individuals with an opportunity to access confidential information and to commit fraud. Call center agents are under pressure to reduce average call-handling time. To accomplish this benchmark, they often help legitimate customers to successfully authenticate. This practice also helps malicious individuals to compromise accounts and access confidential information.

## Damaging the customer experience

The contact center ID&V process can be costly and provides limited security support. Even more damaging to the business and its bottom line are the negative affects on the customer experience. Customers that call the contact center want a question answered or a transaction fulfilled. The ID&V process delays or prevents callers from achieving their objective, making them frustrated. Each interaction with the contact center starts with a negative experience for the customer. These interactions unintentionally make doing business difficult, time consuming, and unpleasant.

The following results can occur:

- Customer loyalty is decreased.
- Customer up-sell potential is lost.
- Brand perception is damaged.
- Passwords are complex.

Providing a subpar customer experience can significantly affect your business revenue.

---

1. The US Contact Center Decision Makers' Guide; Fifth Edition 2012, page 145 (registration required for access): http://www.contactbabel.com/login.cfm?txt01=Please%20Login%20or%20Register&accessdenied=%2Fdownloads %2Ecfm
Costs of web and mobile application authentication

Web and mobile application authentication, traditionally password based, represents an equally daunting business challenge. Recent media stories highlight numerous high-profile cases of hackers who access account credentials on a massive scale.

As malicious users compromise customer accounts and confidential information, the enterprise bears the cost of fraud losses, damaged reputation, and litigation. Unfortunately for the enterprise, several trends, such as the following examples, are converging, which will inflate these costs further for the foreseeable future:

- Increasing complexity of passwords
- Proliferation of accounts
- Consumer preference for smartphone and tablet as computing platforms

Complexity of passwords

Although well-intended, increasingly stringent password requirements reduce successful authentication rates and are an advantage for malicious individuals. These passwords might require at least one special character and a combination of nonrepeating letters and numbers, making them difficult to create and to remember.

To deal with this complexity, users often revert to storing complex passwords in easily compromised repositories, such as unsecured text files. Users also tend to reuse the same password in all accounts, meaning that compromising one account provides a malicious user access to all their accounts. For the user, complex passwords lead to an increase in failed authentications, due to the inability to remember or to properly type complex passwords. The proliferation of accounts, because business is increasingly conducted on the web, compounds this problem further.

Use of mobile computing platforms

Consumers are moving to smartphones and tablets as their computing platform of choice, where the use of complex passwords is impractical. To shed light on this issue, Nuance conducted research that revealed the following key statistics:

- 74% of mobile users were unable to access important information because of failed authentication.
- 67% of mobile users must reset a PIN or a password at least once a month.
- 96% of mobile users make mistakes while typing passwords.

The alphanumeric password, originally conceived for a world with desktop computers that are equipped with full-size keyboards does not adapt well to the new technology paradigm, where keyboards are rapidly fading away. With the introduction of voice-activated personal assistants, and voice-activated mobile apps, voice is increasingly becoming prevalent as an interaction method with technology.

The challenges for the enterprise are clear. But how can a business deliver an easy, quick, and positive authentication experience to customers, enhance security, and minimize costs?
Business value of voice biometrics

Voice biometrics offers organizations a compelling authentication solution. It has the following key advantages over traditional question authentication methods:

- Improved user experience. Voice biometrics is preferred by most users over alternative methods.
- An increased success rate of user authentication. Voice biometrics provides users with a greater probability of accessing their accounts.
- Consistent experience across channels. Voice biometrics can be used as a single credential across all channels.
- Reduced costs. Voice biometrics is shown to reduce the costs related to authentication.
- Diminished fraud risk. Voice biometrics delivers a higher security rate.

When combined, these benefits translate into a strong business case that often delivers an aggressive return on investment (ROI) within months after deployment.

Improved user experience

When users were asked in a Nuance Research study if they prefer voice biometrics over existing authentication means, 90% answered in favor of voice biometrics. This result is not surprising when considering how frustrating existing methods are. In each channel, Nuance Voice Biometrics offers an improved experience:

- In the IVR, instead of providing a PIN that is difficult to remember, callers can authenticate within seconds with a simple passphrase, such as “At IBM, my voice is my password.” The successful use of a PIN also provides a quick authentication method. However PINs tend to have a failure rate in the range of 60% – 80% because callers forget the PIN that they originally provided. This situation leads to frustration and requires the customer go through an interrogation process handled by an agent.

- In the call center, when speaking with an agent, voice biometrics can identify the caller transparently by monitoring speech interaction with the agent. This way, the caller entirely avoids the interrogation process, and can start a call in a positive and personalized manner. Not only does this method save the caller time, it also favorably improves the customer’s perception of the quality of service provided by the organization.

- Within a mobile app, users can authenticate to the app or validate identity to perform transactions with their voice. This approach is the most natural interaction method on a phone and avoids the entry of complex alphanumeric passwords on a tiny keyboard. Beyond escaping the frustrating experience of typing a password on a keyboard, where a majority of users make mistakes, the implementation of voice biometrics eliminates the need to remember passwords in the first place.

- On the web, users no longer need to remember user names and passwords. Instead, they can use their voice as their credential, eliminating the hassle of keeping track of multiple accounts. As authentication on the web becomes increasingly complex, the use of voice biometrics can provide users with a simpler and quicker authentication process. This complexity is especially apparent on banking websites, which require multiple steps, such as answering questions based on knowledge or secret information.

In all channels, the improvement that voice biometrics provides users delivers direct financial benefits to the enterprise, through improved customer retention and new customer acquisition.
Increased user authentication success rate

Nuance Voice Biometrics offers a quicker and easier method of authenticating. However, speed and ease of use are not the only benefit for the user. Voice biometrics increases the overall usage rates for self-service by significantly increasing the success rate for a legitimate user to authenticate into their account in an automated fashion. According to analysis by Nuance, Nuance Voice Biometric deployments average successful first attempt authentication rates that surpass 95%. This solution exceeds successful authentication rates for alternative methods. Failed authentication attempts result in higher abandonment rates by users, which create frustration and prevents customers from achieving their customer care objective. Nuance Voice Biometrics increases self-service usage and successful self-care rates.

For the enterprise, increases in self-service usage, even if by a single point, can have significant positive financial impacts by reducing the usage of contact center and “brick and mortar” service points.

Consistent experience across channels

Authentication experiences tend to vary greatly when customers interact with an enterprise across multiple channels. Customers are asked to provide a user name and password on the web, to enter a PIN when calling the IVR, and to answer to a series of security questions when speaking to an agent. To the customer, these methods can lead to a frustrating and inconsistent experience.

This problem is compounded when the customer fails authentication on one platform and wants to authenticate by using the credentials used on another platform. If a set of credentials is valid to authenticate on one channel, why would the enterprise not recognize those credentials on another channel?

Nuance Voice Biometrics can be deployed as a single credential across all customer service channels, providing a secure and consistent experience to customers. Providing such an experience for customers across service channels has a direct financial impact for the enterprise through improved customer retention and new customer acquisition.

Reduced costs

Voice biometrics solutions go beyond improving customer retention rates and new customer acquisition. The deployment of voice biometrics delivers easily measurable reductions in costs, by reducing average call-handling time and reducing call volumes to the call center. This result is achieved by significantly reducing the number of unauthenticated calls that call center agents need to answer. This solution reduces the average hold time (AHT) an average of 30 seconds, because caller authentication is performed automatically by the IVR. Deployments of voice biometrics in the IVR, on the web, and in mobile apps lead to improved self-service rates, reducing the number of calls handled by call center agents. These metrics can be measured easily after the deployment of voice biometric authentication. Also, in many cases, they can deliver an ROI that is based exclusively on these cost savings.

Diminished fraud risk

Nuance has found that organizations that have deployed voice biometric solutions have experienced reduced cases of fraud. Although no technology provides 100% protection against malicious attacks, voice biometrics provides a superior authentication solution to user name and password, PIN, and security question authentication methods.
A voiceprint is unique to every individual. It cannot be shared, lost, or compromised, which is the case with knowledge-based credentials. The benefit of voice biometrics over alternative biometric technologies, such as fingerprint or iris detection, is the lack of any specialized hardware requirements. Voice is also a non-invasive biometric, unlike facial recognition, which requires a live camera to monitor the user. For additional layers of security, voice biometrics can be combined with additional methods for multifactor authentication for security of critical transactions.

Beyond identity verification, voice biometrics provides a significant security benefit over traditional authentication methods. Nuance Voice Biometrics provides identification capabilities, so that a malicious user, who is attempting to compromise a legitimate user’s account, can be identified through their voice. If organizations maintain audio records of known fraudsters, by using this identification capability, fraud prevention groups can identify in real time a fraud attempt by a known fraudster.

Reductions in fraud incidents can result in significant direct financial benefits to the enterprise, by reducing fraud losses and reducing litigation costs. Furthermore, reductions in fraud increase customer confidence to conduct business with an organization, which can have significant benefits in customer retention, customer upsell, and new customer acquisition.

**IBM and Nuance Voice Biometric solutions**

IBM and Nuance Communications Inc. formed a partnership to accelerate innovation in voice technology and deliver advanced speech recognition solutions for enterprises worldwide. IBM and Nuance have demonstrated that voice biometrics is a critical component of solutions for contact center transformation and for customer care, customer insight, and for mobile initiatives.

The effectiveness of speech recognition today comes out of decades of research by hundreds of scientists and engineers who have worked on statistics, linguistics, semantics, predictive algorithms, and audio processing. IBM has been involved in speech research for many decades. IBM Research has worked with National Institute of Standards and Technology (NIST) to help drive significant recent advances in speaker verification. IBM Research includes multifactor biometrics that take advantage of smartphone capabilities to better address fraudulent attempts.

For more information about the role and involvement of IBM Research in speech recognition, see “Pioneering Speech Recognition” at:


**How voice biometrics identifies an individual**

Voice biometrics is based on the fact that every individual’s voice is unique. However, unlike other biometric technologies, such as fingerprint, iris, and facial recognition, voice biometrics uses a combination of unique physical and behavioral voice characteristics to uniquely identify an individual.

Nuance VocalPassword is a biometric system that verifies a speaker during an interaction with a voice application. Nuance VocalPassword is *Ready for IBM Tivoli® software*. It provides a secure, efficient, and convenient method to verify a speaker’s identity as a stand-alone solution or by passing credentials to enterprise systems to allow for logon, authorization of a transaction, or unlocking a mobile device.
Voice biometrics amasses hundreds of voice characteristics to create a person’s voiceprint. By using this approach, the solution can accurately identify an individual even in cases where environmental or physical variables affect a person’s voice, such as illness or background noise. Unique physical traits of an individual include such characteristics as the shape and size of their vocal tract. Behavioral characteristics include harmonic and resonant frequencies, such as accents, the rate of speech, and how words are pronounced and emphasized. Together, these physiological and behavioral factors combine to produce unique voice patterns (voiceprints) for every individual.

Identification and verification with voice biometrics

Voice biometrics provides identification and verification capabilities for each voice utterance that is received. These capabilities provide an authentication means for legitimate users and proactively search for known malicious individuals. The identification capability is most useful in cases where the voice that is being analyzed does not match the claimed identity. In this case, instead of rejecting the authentication request, the solution takes the additional step of assessing who the individual really is. With this identification capability, the technology provides security benefits that far surpass nonbiometric methods, such as user name and password or security token. These traditional methods can verify only a credential match and provide no capability to identify the user.

The Nuance Voice Biometrics solution can be used for two key purposes:

- Identification to determine who an individual is
- Verification to accept or reject a claimed identity

Key steps in performing verification

In a verification scenario, a speaker claims an identity by providing an identifier such as a user name or account number. If the identifier is spoken, the voice biometric engine can use this sample of the speaker’s voice for identification and verification purposes (illustrated in Figure 1 on page 8). If the identifier is not spoken, the user can be prompted for a voice passphrase, such as “At IBM, my voice is my password.”
To reach a decision on the speaker’s identity, the engine checks two hypotheses:

- If the voice matches the target speaker, the claim is correct.
- If the voice matches a known fraudster, the claim is incorrect.

Checking that the claim is correct is done by comparing a sample of the speaker’s voice with a voiceprint that matches the claimed identity. Checking that the claim is incorrect requires a comparison of the voice sample with voiceprints of other speakers. This process allows for the simultaneous verification and identification capability.

An organization that deploys voice biometrics can maintain a list of known fraudster voiceprints. This combination of using voice biometrics and a list of known fraudsters can help to alert fraud prevention personnel that a fraudster is attempting to authenticate to a customer account.

**Active versus passive verification**

Most voice biometric applications (whether to connect to an IVR, to access a mobile app, or to authorize a web transaction) take advantage of the use of active voice biometrics. The user is prompted to say something, for example an account number or a passphrase such as “At IBM, my voice is my password.”

In some cases, passive verification is desired. Verification and identification are performed on free speech, meaning that the user is not required to say anything in particular. This method is useful in the context of a live call with a call center agent. If an organization lets callers reach an agent without going through an IVR, the opportunity for automated authentication is not present. With the use of passive voice biometrics, the caller can be identified through natural conversation with the agent. Identity verification typically occurs within the first 30 seconds of the call, because passive authentication requires more speech for verification than active voice biometrics.
The benefit for the enterprise and the customer is avoiding the interrogation process that might otherwise be used to verify a caller's identity. An additional benefit over active verification is that callers are not required to actively enroll. Their voiceprints can be created through their first interaction with the call center agent, making the use of voice biometrics by the caller transparent and effortless.

Key differentiating capabilities

Voice biometrics is unique in many respects, and the key differentiating capabilities directly impact the business and customer:

- **Accuracy**
  Numerous third-party studies have demonstrated the superior accuracy of this solution. This solution results in a higher success rate for legitimate customers to access their account on the first try. Superior accuracy also provides a more robust security system, minimizing fraud risk.

- **Scalability**
  The Nuance Voice Biometrics solution can scale to tens of millions of voiceprints. A single system has been tested with 80 million voiceprints, enabling voice biometrics to serve as an authentication platform for large-scale deployments. Beyond the ability to handle large volumes of voiceprints, this solution has multitenancy capabilities, so that multiple subsystems with separate configuration parameters can coexist within one unified deployment.

- **Universality: Language and accent independent**
  The voice biometric solution is language and accent independent, meaning that a single system can be used for a global customer base.

- **Security: Liveness detection**
  *Liveness detection* is a unique and patented capability of this solution. It is used to detect intra-session voice variation to mitigate against a change in user or a recording threat. The solution initially uses text-dependent verification, such as when a user speaks an account number or a passphrase. Then liveness detection collects a text independent voice sample by prompting the user for a random or semirandom sentence. For example, the user might be asked to say “The IBM logo is Blue, the Nuance logo is green.” Each time liveness detection is used, the user is prompted to speak a different sentence.

- **Security: Playback detection**
  To prevent malicious users from compromising an account, this solution uses voice recording techniques based on a patented playback detection algorithm. The playback detection algorithm runs as part of the verification process and identifies audio segments that unnaturally match audio segments that were previously used for verification or enrollment.

- **Manageability**
  The Nuance Voice Biometrics solution has a series of web accessible management applications and configuration tools. These tools enable customer care, IT, and fraud prevention personnel to access data and conduct operations in a manner that is easy to use.
Solution architecture

This Nuance Voice Biometric solution consists of two key servers (Figure 2):

- Processing server that handles voice verification processing
- Data repository server that stores voiceprints

![Diagram of Nuance Voice Biometrics architecture]

The processing server hosts the speaker verification engines, which perform algorithmic processing, control client services, and acquire audio through application programming interface (API) calls. Multiple servers can optionally be used in a redundancy scheme for high availability purposes or in a load balancing scheme for scalability. The processing server also hosts the web managed application.

The data repository server is responsible for storing the system and voiceprint data. It runs the database of the system, the Lightweight Directory Access Protocol (LDAP) directory, and the file system (for audio recording storage). Nuance VocalPassword supports the use of two synchronized data repository servers for high availability by using a dedicated service (Nuance data replicator).

Customer care scenarios that use Nuance Voice Biometrics

Nuance Voice Biometric solutions are deployed in hundreds of organizations across the globe, consisting of over 15 million voiceprints. These solutions are used in the following key scenarios:

- Contact center ID&V scenario
- Mobile app authentication
- Website transaction verification
- Account enrollment and verification services
- High-risk credit card transaction verification
Contact center ID&V scenario

A large financial institution has various business units that include retail banking, private banking, corporate banking, brokerage services, and wealth management. Their contact centers can handle millions of calls a year, and despite years of optimization, only 55% of callers are able to self-authenticate using a PIN-based system. As a result, 45% of these calls are transferred to contact center agents who spend an average of 60 seconds authenticating callers by asking multiple personal and transactional questions.

The institution’s agents report that many customers are annoyed by having to answer several questions, especially when they are unable to provide an answer. By the time the authentication process is over, the agent rushes to respond to the customer request because the caller is already impatient. Many of the calls are for tasks that can be performed easily in the IVR, which drives up contact center costs and ties up agents on non-revenue-generating calls. Executive management is requiring cost reductions and demanding that the contact center drive more revenue.

The solution in this situation is to deploy the Nuance Voice Biometric solution to automatically authenticate callers to the IVR. Customers are prompted to say “My voice is my password” and are automatically authenticated. Automated authentication increases from 55% of calls to 95%. Callers that fail or bypass automated authentication and reach an agent no longer need to answer security questions, as the callers are passively authenticated during their conversations with agents. Average call-handling time is reduced by 20 seconds.

The greatest benefit, however, is the average increase of 40 seconds that agents can spend upselling customers. Additional revenues and a reduction in AHT deliver an ROI within 6 months of deployment. An unexpected benefit is an increase in call-center agent satisfaction, which reduces the turnover rate. Marketing can take advantage of this innovative technology in their advertising and public relations activities to position the bank as an innovative leader in delivering improved customer experiences. The financial institution sees an increase in customer retention rates and in new customer acquisition.

Mobile app authentication

A telecom provider delivers wireline, wireless, high-speed Internet, digital TV, and voice over internet protocol (VoIP) services to consumers and corporate customers. The firm is already using voice biometrics to authenticate callers to their IVR, with over 4 million of their customers who enrolled their voiceprint. Customer service executives see the mobile channel as an opportunity to reduce call volume to the contact center.

However, recent investments in customer service apps have yielded mixed results. An application was released that required entering the same user name and password that customers used on the web portal. Although the number of customers that have downloaded the app has surpassed expectations, the usage figures have been deceiving. No decrease in contact center volume has been noted.

Feedback from users indicates that entering complex alphanumeric passwords on their mobile device is inconvenient and frustrating and has been identified as the key factor that prevents increased usage of the app. A second version of the app was released without any authentication requirement, but with reduced functionality. Users can perform only basic tasks, such as checking voice and data usage rates. A lack of authentication was viewed as too risky to enable service or account changes. Executive management is demanding to see a return on the mobile app investment.
The Nuance Voice Biometric solution is deployed to enable secure and convenient authentication by users to the mobile customer care app for the telecom provider. This approach has permitted the telecom provider to enable advanced functions on the mobile app, such as ordering new services and changing address information. Usage rates have surpassed the initial targets, and the contact center has seen a decrease in call volume.

Based on these results, the telecom provider can achieve the return on investment it originally set in its mobile application strategy. Enabling voice biometric authentication also has had an additional and unexpected benefit. New customers tend to use the mobile app before they call the contact center. As a result, when they call the contact center for the first time, they already have their voiceprint enrolled, because the same voiceprint is used for both the mobile app and IVR authentication. This approach has resulted in an additional improvement in overall IVR automation rates, further reducing contact center costs.

Website transaction verification

An online payment service provider offers an alternative to entering credit card information to speed up online transactions. The firm has millions of consumers and small business users that perform transactions daily. Unfortunately, cases of fraud have been on the rise because malicious users are increasingly targeting the firm's online service to perform unauthorized transactions and money transfers. Executive management believes that the fraud issues are hampering the firm's growth potential. Incidents of fraud tend to reduce usage by affected customers and negatively impact the firm's brand through word-of-mouth and social media activity highlighting fraud cases. The firm has assessed various security technologies and rejected them because of their cost and negative impact on user convenience through the use of security tokens.

The Nuance Voice Biometric solution is used to secure at-risk transactions such as first time payments to a merchant, first time money transfers to new payees, and any transaction over $1,000 in value. When such transactions are performed, an automated outbound call is placed to the account holder's mobile phone that describes the transaction. If approved, the user is prompted to speak the passphrase: “My voice signature authorizes this transaction.”

After deployment, the firm experienced a significant reduction in fraud, providing a rapid ROI for the voice biometric implementation. The reaction of the customer base has been so positive. Because of this reaction, voice biometrics is now used as an alternative authentication method to the user name and password combination to access both web accounts and all transactions that involve using a microphone. The firm also tracks increases in social media posts that pertain to the firm's online payment services. The firm is planning to invest in a broad marketing campaign to highlight the user-friendly and secure nature of their service, around the theme of “No more passwords.”

Account enrollment and verification services

Financial services firms must constantly refine their security approaches to protect their customers from criminal elements. Fraudsters are constantly searching for ways to breach protections and to gain illegal access to account information and money. Unfortunately, many safeguards that are put in place to protect customers are frequently inconvenient to them. Account numbers, PINs, secret passwords, and authentication questions are used in electronic interactions to validate that the person who is trying to access the account has legitimate authorization. Customers must remember these unique authentication steps, which can be difficult and time consuming. An unauthorized person with the right information can pose as a customer to gain access to accounts.
Nuance and IBM, through their partnership, show how voice biometrics can enable financial services to improve their customer’s experience and lower cost. The new financial services scenario showcases the integration of Nuance Voice Biometrics and outbound notifications in with IBM financial solutions.

This next generation solution has been extended to include the following features:

- Voice enrollment and voice verification
- Event driven multichannel alerts with voice
- Email and Short Message Service (SMS) to speed calls with increased customer convenience

The overall solution provides multimodal verification, integrated event detection, and proactive notification. It uses the customer preferred method to speed customer care, improving customer satisfaction and reducing inbound call center volumes.

This comprehensive solution increases the satisfaction of banking customers, decreases call times, and reduces costs with natural verification. Voice verification helps customers securely satisfy their requests at their convenience, decreasing customer frustration and increasing loyalty. Secure inbound voice-based verification reduces fraud and increases legitimate transactions.

**High-risk credit card transaction verification**

The credit card division at a leading financial institution provides services to millions of consumers and commercial credit card customers. Credit card fraud is an ever-increasing problem. The switch to credit cards with built-in chip technology has had a negligible impact on overall fraud as malicious users increasingly commit fraud online rather than in brick and mortar stores.

The institution’s predictive transaction risk analytics solution has delivered mixed results. In the past, the system has been tuned too aggressively. Legitimate transactions were blocked when cardholders traveled or performed transactions that did not follow their historical purchasing patterns. Executive management decided the impact on the customer experience did not justify the reduction in fraud. As a result, the analytics system was tuned to be more lenient, resulting in increased successful credit card fraud incidents.

The Nuance Voice Biometric solution was deployed to combat fraudulent credit card transactions. When the risk analytics solution detects a high-risk transaction, a request to verify that the transaction is sent to the credit card holder. The request is sent through an automated outbound call to the cardholder’s mobile phone or through a message on the user’s smartphone for cardholders who have downloaded the mobile app. The credit card holder is then asked to speak a common passphrase, such as “My voice signature authorizes this transaction.” If the credit card holder is unable to verify the transaction at the time of purchase, and their card is locked, the card holder can automatically unlock the card through voice biometrics. This unlock activity can be done either through the IVR or the mobile app, eliminating the need to speak to a contact center agent.

The solution has dramatically reduced the number of incidences of credit card fraud. It has also reduced the call volume handled by the security contact center agents. The financial institution realized an ROI after only 6 months of deploying the solution.
Summary

Through their partnership, IBM and Nuance Communications Inc. have accelerated innovation in voice technology and delivered advanced speech recognition solutions for enterprises worldwide. This joint activity delivers end-to-end contact center transformation. IBM has extensive experience in strategic business transformation, hosting, and services, coupled with a global reach, unmatched industry expertise, and decades of experience. These qualities interconnect with those qualities of Nuance, bringing unparalleled depth of experience in speech-enabled customer care. Together, IBM and Nuance have one of the largest and most experienced customer-relationship management consulting practices in the world.

By reading this paper, you now have an overview of the Nuance Voice Biometrics solution and how it is used within an IBM enterprise contact center transformation, customer care and insight solution, and mobile initiatives. This paper highlighted the advantages of this solution over traditional authentication methods that are used in customer care centers. It also highlighted the key capabilities of voice biometrics and provided customer scenarios that highlight key features of the Nuance and IBM contact center solutions.

Other resources for more information

For more information, see the following resources:

- Nuance Voice Biometrics product information
- Nuance VocalPassword
- IBM and Nuance solutions

The team who wrote this guide

This guide was produced by a team of specialists from around the world who are working with the International Technical Support Organization (ITSO).

**Brett Beranek** is a Solutions Marketing Manager at Nuance. Brett has extensive experience in security, biometric technology, and enterprise software. He has a Bachelor of Commerce degree in Information Systems from McGill University and an Executive Marketing Certificate from Massachusetts Institute of Technology.

**Russell Warren** is a Product Manager in IBM Security Product Management. Russell has 34 years of experience in security, systems, network, and applications management. He has worked in the IBM Tivoli organization and with IBM enterprise and distributed systems for application, network, storage, and security management across the full software lifecycle. In addition to working on standards definitions and partnerships programs, he has worked with sales and marketing teams on generating and presenting external and internal collateral.
Thanks to the following people for their contributions to this project:

LindaMay Patterson  
IBM ITSO, Rochester, MN

Debbie Katz  
Nuance Communications, Inc.

Ron Hoory  
IBM Israel Research

Steve Ambrose, Alliance Partner Executive  
Kay Freund, Alliance Marketing  
Paul Govoni, Software Sales  
David Nahamoo, IBM Research and IBM Fellow  
Dean Witt, Alliance Technology  
IBM US

Now you can become a published author, too!

Here’s an opportunity to spotlight your skills, grow your career, and become a published author—all at the same time! Join an ITSO residency project and help write a book in your area of expertise, while honing your experience using leading-edge technologies. Your efforts will help to increase product acceptance and customer satisfaction, as you expand your network of technical contacts and relationships. Residencies run from two to six weeks in length, and you can participate either in person or as a remote resident working from your home base.

Find out more about the residency program, browse the residency index, and apply online at: ibm.com/redbooks/residencies.html

Stay connected to IBM Redbooks

- Find us on Facebook: http://www.facebook.com/IBMRedbooks
- Follow us on Twitter: http://twitter.com/ibmredbooks
- Look for us on LinkedIn: http://www.linkedin.com/groups?home=&gid=2130806
- Explore new IBM Redbooks® publications, residencies, and workshops with the IBM Redbooks weekly newsletter: https://www.redbooks.ibm.com/Redbooks.nsf/subscribe?OpenForm
- Stay current on recent Redbooks publications with RSS Feeds: http://www.redbooks.ibm.com/rss.html
Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user’s responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing, IBM Corporation, North Castle Drive, Armonk, NY 10504-1785 U.S.A.

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs.
Trademarks

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both. These and other IBM trademarked terms are marked on their first occurrence in this information with the appropriate symbol (® or ™), indicating US registered or common law trademarks owned by IBM at the time this information was published. Such trademarks may also be registered or common law trademarks in other countries. A current list of IBM trademarks is available on the Web at http://www.ibm.com/legal/copytrade.shtml

The following terms are trademarks of the International Business Machines Corporation in the United States, other countries, or both:

IBM®
Redbooks®

Redguide™
Redbooks (logo)®

Tivoli®

The following terms are trademarks of other companies:

Other company, product, or service names may be trademarks or service marks of others.