opusresearch

Enterprise Readiness Series:
The Case for Passive, Voice-Based Authentication

Today's customer authentication methods are from another age. Opus Research interviewed security and customer care professionals in Global 100 companies to learn about their perception and attitudes toward passive authentication of customers using voice. Respondents provided insights into the value of multi-factor authentication and provided "key success factors" for implementing strong, context-aware authentication without burdening customers with passwords or answers to challenge questions.

April 2013

Courtesy of:

Dan Miller, Senior Analyst – Conversational Commerce

Opus Research, Inc.
350 Brannan St., Suite 340
San Francisco, CA 94107

For sales inquires please e-mail info@opusresearch.net or call +1(415) 904-7666

Table of Contents

Authentication: Stuck in the Last Century

Every day, people are finding new and better ways to carry out online or mobile transactions because new technologies make it easier and faster to enter payment instructions, update personal information and do their general bidding. There is, however, one very conspicuous speed-bump: customer authentication.

In spite of (or perhaps because of) higher network speeds, faster data processing and message handling, and more conveniently designed devices, dialogue models and user interfaces, the deficiencies and general inconvenience involved with customer identification and verification (ID&V) is more glaring than ever. The problems of cumbersome authentication are exacerbated by the growth of mobile computing and communications and the closely related need for strong authentication, balanced with equally important endeavors to enhance the customer experience.

Asking the Influencers

In this document, Opus Research shares the perspectives of customer care and security experts from financial institutions around the world. In late 2012 and early 2013, Opus Research carried out a series of interviews with key influencers in the space to better understand their perspectives of developments in this arena.

The answers to the questions above are included in this report, along with *verbatim* responses. Opus Research provides additional perspectives and insights drawn from over a decade of conducting research in this field.

Pain Points with Current Authentication

New personal communications and mobile technologies have given rise to increased customer activity involving a wide range interactions and transactions utilizing more and more communications channels. This increased complexity challenges enterprises to strike the right balance between security and convenience when authenticating end-customers.

There was widespread consensus among survey respondents regarding the importance of taking a holistic view of security and customer authentication; offering a consistent methodology across all channels through which a customer contacts people or resources in the financial institution.

The fact that customer authentication is still stuck in last century, coupled with the increasing need for security and convenience has resulted in some key pain points for enterprises and consumers alike.

Customers Really Don't Like the Authentication Process

In July 2012, Opus Research issued a report on "Caller Authentication: Likes, Dislikes and Preferences," based on a survey of over 1,000 consumers who had made recent calls into customer care contact centers. In response to questions posed by the respected survey house, Coleman-Parkes, they indicated that:

- 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 sum, the most common forms of caller authentication are the ones that people find most annoying.

Reliance on "Something You Know" Adds Time and Expense

The most common practice for customer authentication, across all channels, involves an individual providing his or her user name, personal identification number (PIN) or password. Most organizations also employ knowledge-based authentication (KBA) or "challenge questions" to verify a customer's identity through either personal questions or "out-of-wallet" information.

There was a general consensus that there is an over-reliance on "something you know," when it comes to customer-facing operations. 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.

Interviews revealed that authentication takes between 10-40 seconds in an IVR. Once transferred to a live agent with challenge questions it often takes over two minutes.

Customers Have Too Much To Remember

The problem with any popularly used authentication measure is that it becomes more vulnerable over time as impostors figure out how to defeat security mechanisms. Inevitably companies escalate the measures they undertake to prevent fraud and promote trusted communications, thereby making the authentication process much more complex.

"Dissatisfaction correlates with failure to get through."
Sr. IT Manager-Global Brokerage House

Customers appear to have grown especially forgetful as more strictures are put on passwords and firms are requiring increasingly complex knowledge-based information. All this leads to more false rejection – customers failing authentication on their own accounts – which gives rise to customer frustration and a spiral of more complex and time-consuming authentication.

"Failed authentication is definitely one of the things that people don't like."

Sr. Virtual Banking Manager-Large Credit Union

Multi-Factor Authentication Drives More Complexity

The move to layered, multi-factor authentication (MFA) is an 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.

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 MFA extending the length of a call or adding to a customer's workload.

Too Many Tokens, Dongles and Key Chains

Another headache from use of physical tokens was articulated by one of the interviewees taking the consumer's point-of-view. He noted that tokens are like passwords in that they are associated with a single business or service. Therefore, many individuals have multiple tokens ranging from dedicated dongles, to key chains or mobile phones. It is a nuisance to have to carry them around and "choose the right one" when it is time to deploy.

Furthermore, one-time passwords have also been found to be susceptible to hacking and fraud. For example, a catastrophic hacking of the algorithm that RSA employed for one-time passwords, which led to 40 million physical tokens having to be replaced. Accordingly, organizations are looking for suitable alternatives.

Voice Biometrics Meets Today's Challenges

Opus Research found that the executives we interviewed showed higher levels of awareness and understanding of voice biometric-based authentication than we had observed in prior years, especially in the broader contexts of multi-factor authentication, fraud reduction and passive authentication.

Simply put, voice biometrics allows enterprises to leverage each customer's unique voiceprint as their identifying credential for secure authentication.

Several respondents 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.

Ideal for Remote Authentication in the Voice Channel

There was widespread consensus across both technologically focused respondents and those directly accountable for customer satisfaction that voice biometrics is an ideal solution for remote authentication in the voice channel.

Interviewees saw voice biometrics as addressing each of the previously discussed pain points, with one executive particularly appreciative of the technology's ability to "balance ease of use and security concerns".

Recap of Key Success Factors

Given the significant potential of voice biometrics authentication in terms of security, efficiency *and* convenience, we explored the key success factors with customer care and security experts.

Authentication Best Takes Place in the Background

The executives we interviewed were in favor of technologies that can authenticate callers "in the background" while agents or financial advisors help customers carry out their business. They expressed general dissatisfaction with PINs, passwords and the use of an agent's time soliciting account information or asking challenge questions.

"Ideally it would be good if [authentication] were passive."

Multichannel Product Manager-Commercial Bank

Enrollment Has To Be Painless

Interviewees indicated that companies might be well advised to make enrollment of voiceprints an event that takes place "in the background" as well. Many of the most experienced organizations had found procedures around enrollment of voiceprints to be cumbersome and disruptive, in that

customers were often uncertain that the process was working (since they had to repeat numbers or phrases three times) and often turned to customer care personnel for help.

"We'd like to have enrollment be automatic and happen in a seamless way."

Technology Strategist-Large Commercial Bank

Minimize Customer Effort in Enrollment and Authentication

The Customer Effort Score (CES)[1] is the rising star in contact center metrics. The focus on CES uncovered the inordinate amount of effort it takes for individuals to assert their claimed identity and entitlements. Accordingly, customer effort needs to be minimized in both the enrollment and authentication stages.

An executive at a global investment house succinctly called voice biometrics an "ease of doing business" tool.

Make It Multi-Factor

It is essential that customer authentication be multi-factor; best practice is to take into account as much information and as many factors as possible, both to prevent fraud but also to understand the level of risk that should be assigned to an individual or transaction.

"Whether it's in a call center, through mobile or to protect online activity, multi-factor authentication is not a choice; it's a must!"

Sr. IT Manager-Global Brokerage House

Deploy Risk-Based Authentication

The perceived requirement to keep security strong-yet-simple has militated toward taking a passive approach to authentication in general. Fast, simple and unobtrusive are deemed to be the best qualities.

For such a strategy to succeed, the levels of authentication required from customers must be adjusted to fit the level of risk associated with a number of factors, including the origin of the call, mannerisms of the speaker, even time-of-day.

"We have an internal risk profile for every transaction and we lean toward ease of doing business over security, except for the high-risk transactions."

Sr. IT Manager, Global Brokerage House

[1] Customer Effort Score measures how long and how many hops or transfers it took to accomplish the goal at hand

Make it Customizable and Tune-able

Over the years, both the security and contact center executives we spoke with cited the need for technology to be flexible enough to handle various confidence levels and determine different authentication policies per level. The ability to customize and tune the system can be applied to tailor the customer experience to balance security and convenience.

"It is a trade-off between security and consistency."

Sr. Virtual Banking Manager-Large Credit Union

Leverage Existing Infrastructure

Respondents also indicated that cost control is important, as is the ability to continue to use the software and systems that are already in place for both customer care and security.

"One of the 'pain points' is to be able leverage what we've got installed in the back end."

Technology Strategist-Large Commercial Bank

Keep Innovating to Match Changing Threats

Fraud loss specialists know well that imposters mount persistent threats on their security measures. Authentication needs to take place across all modes, take into account the customer "journey" and employ both active and passive methodologies for risk assessment and authentication.

"From our standpoint it would be integrated as a multimodal experience. In the contact center, we'd look at both active and passive authentication."

Technology Strategist-Large Commercial Bank

Convenient Security Becoming the Priority

Interviews with senior executives revealed the importance of maximizing both security and the customer experience through the authentication process. There was wide consensus on the unique attributes of voice biometrics for solving the paradox of balancing concerns about security and convenience.

Because voice biometrics technology is not new, many of our interviewees had evaluated voice biometric technologies, as well as multi-factor approaches, over the past five years. Several cited the need for formal enrollment as one of the major roadblocks to more widespread adoption of the technology. That need stems from the fact that past solutions (and indeed most of the implementations to this day) required repeated recitation of selected passphrases. As a result, low customer opt-in rates have diminished the promise of the technology and limited its applicability in authenticating the wider customer base.

How NICE Systems Addresses Authentication in Real Time

Opus Research is continuously searching for the latest developments in the field of voice biometrics during which we have discovered NICE Systems' offering for addressing authentication in real time. NICE Real-Time Authentication brings to market a new approach for mitigating each of the pain points experienced in the authentication process, as well as adhering to the key success factors laid out by customer care and security experts. The solution:

- **Seamlessly creates customer voiceprints** – Leverages your existing recording platform and stored recordings to securely enroll the vast majority of your customer base with no customer or IT impact.
- **Authenticates customers in the background** – Utilizes text-independent voice biometrics to authenticate with no customer effort through the natural course of conversation.
- **Streamlines the authentication process** – Integrates real-time audio management and real-time agent guidance to minimize the time spent on authentication.
- **Makes authentication more secure** – Offers multi-layered security for creating voice prints, as well as a multi-factor approach by combining voice biometrics and dynamic security questions.
- **Enables risk-based authentication** – Combines call meta data and analytics for real-time risk decisioning to customize the authentication process.

These unique capabilities enable the enterprise to significantly reduce average handle time, while improving the customer experience and the security of the authentication process.

Case Made for Passive Voice Authentication

Our executive interviews corroborated the findings of prior surveys of general consumers and customers: When contacting banks, brokerages, insurance companies or any business that has access to personal information and carries out important transactions, callers want both convenience and a sense of security/trust.

To recap the findings of our executive interviews: We're at a potential 'tipping point' with respect to implementing simple, multi-factor authentication methods. Solution providers recognize that voice biometrics stand out as an ideal antidote to the long-standing conflict between security and convenience. They also realize that overcoming barriers to authentication is a major step toward broader acceptance and adoption.

The more tech-savvy respondents also perceive that adding passive enrollment and voice authentication can overcome barriers to adoption and create a compelling ROI, especially since it augments, rather than replaces existing solutions. Based on feedback from executives, the time is ripe to re-evaluate, revisit and/or re-deploy voice biometric-based solutions.

Appendix A: Factors for Authentication

As a quick review, 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 (or more specifically the SIM card installed in a phone) 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.

Appendix B: Interview Guide

Overall purpose of discussions is to learn the following:

How your organization is currently thinking about customer authentication and how voice biometrics can add value in this area

Current authentication process and challenges

1) What is your current authentication approach and how long does it take?
2) How critical is Multi-Factor Authentication (MFA)? What factors do you find strongest or "most trustworthy"?
3) What are the current challenges / pain points with your authentication process?

Customer satisfaction (CSAT)

4) How do you measure your CSAT in relation to your authentication process?
5) What is the percent of failed authentication attempts? How does this impact your CSAT?

Operational efficiency

6) How do you balance between security concerns and operational efficiency / customer experience?
7) Do your agents currently have difficulty with your authentication process? Elaborate.

The value of easily creating voice prints for all customers

8) What value do you see from having all your customers voice printed from day one in an automated passive manner?
9) Do you consider voice biometrics active enrollment to be an inhibitor to adoption?

Project priorities

10) Have you looked at or evaluated voice biometrics-based live agent (text independent) authentication?
11) Assuming a solution with easy enrollment of the majority of customers, significant CSAT uplift and operational efficiency savings, would this rank as a top project for 2013? Elaborate.
12) What are the primary concerns that have slowed VB's progress?