A New Authentication Paradigm:

Call Center Security without Compromising Customer Experience

Financial institutions can reap significant financial gains by using voiceprints to authenticate through the phone channel. By our calculations, a large money center bank will see over $100 million in economic benefit from reducing fraud loss in the contact center, lowering operating costs, and providing a more pleasing customer experience.

Courtesy of

Dan Miller, Senior Analyst – Conversational Commerce

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

Table of Contents

Table of Figures

Key Findings:

- **Passive voice biometrics is poised to disrupt traditional "active" multi-factor authentication in contact centers** – Many past attempts to popularize voice biometrics subjected to unnatural, opt-in dialog sequences. Not surprisingly, callers rejected these attempts at forced enrollment. Passive voice biometric platforms, like Verint's, allow callers to proceed in a comfortable call flow dialog with an agent while being passively enrolled and, later, authenticated in the background.

- **Dual-screening against "blacklist" as well as "whitelist" is key enabler** – The historic approach – tuning a single voice biometric system for high detection of fraudsters – could give rise to a high "false-reject" rate, leading to caller frustration. By contrast, tuning for higher acceptance rates allows access to fraudsters. Verint has adopted an approach that separates the screening process for customers and fraudsters, and eliminates the crucial failure of single-screen biometric systems.

- **Field results show that passive voice biometric authentication leads to significant savings from reduced fraud and operating costs** – Verint has built case studies that demonstrate an 80% reduction in call center fraud and an average 25-second reduction in call duration. These benefits can translate into over $100 million in annual savings for large institutions with significant call center operations such as major banks.

- **Passive enrollment and authentication has a positive impact on customer satisfaction as well** – In studies conducted by Opus Research, customers indicated frustration with the cognitive load required by current authentication processes

The Power of Positive Authentication

In industries where contact centers are important touchpoints between the company and the customer (e.g. financial services, healthcare, utilities), managers face a paradoxical challenge. They must protect their customers' data and promote mutual trust while providing efficient and friendly customer service. Historically, these two goals have existed in a zero-sum equation — high security translated into poor customer experience. Today, passive authentication solves this riddle.

Today's Dilemma: Relying Too Much on "Something You Know"

When customers call a contact center, each is subjected to two important processes: identification and authentication. As part of identification, call center agents ascertain *who* it is they believe is calling regarding *what* account. Authentication comes next. It refers to the process of verifying that the individual on the other end of the line is who he or she claims to be. The most common types of authentication questions fall into three categories:

1. **In-wallet questions** – The 3-digit security code on a credit card or birthdate of an account holder.

2. **Static Knowledge-Based Authentication (KBA)/Shared Secrets questions** – Verbal password or security questions and answers established upon account set-up.

3. **Dynamic KBA/Out-of-Wallet (OOW) questions** – Generated in real-time from public records (i.e. make and model of car leased in 1995, last previous address, etc.).

At first glance, these types of questions do not seem too onerous to the caller. However, a survey commissioned by Opus Research in mid-2012 revealed results to the contrary. Of 1,000 individuals who had recently carried out business over the phone:

- About 65% found authentication processes to be frustrating

- Nearly 50% considered the process too time-consuming

The overall results of the survey reflected significant levels of dissatisfaction with the process of caller authentication. Those who were "frustrated" cited the reason as having to make multiple attempts at authentication. As call centers are typically cost centers of an organization, any time-consuming practice is an issue for concern, especially if the customer has to place several calls to resolve an issue or if the customer service agent is a highly compensated individual such as a clinician, technician or financial advisor.

For a low-risk transaction, such as checking an account balance, entering a PIN typically takes a few seconds. By contrast, authenticating a caller for a high-risk transaction, such as a wire transfer, can involve multiple challenge questions and take several minutes. With fully loaded personnel costs averaging $1.00 per minute and standard third-party KBA fees ranging from $0.15-$1.00 per call, the industry-wide cost of authentication is staggering; and companies see reduction of authentication time as ripe for cost savings.

Customer dissatisfaction with current authentication methods also has the potential to drive up costs. Our 2012 survey also revealed:

- 28% of respondents thought that the business was applying the proper level of security to the task at hand

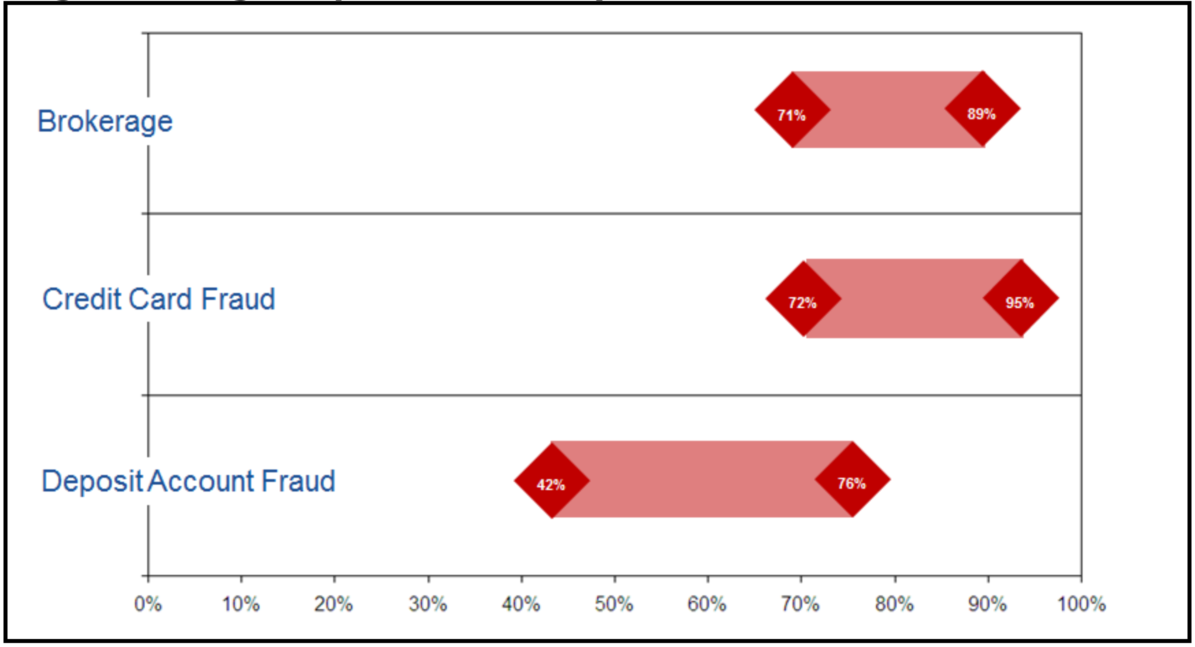
- 22% believed that it "always takes too long for me to authenticate myself before I can carry out the purpose of my call."

Thus, poor authentication practices lead to disgruntled customers and the possibility of lost business.

Questions Don't Stop Professional Fraudsters

Data gathered by security experts at RSA and at Javelin Research reveal another more serious flaw with current authentication systems. Call center-based attacks on customer data is increasing by double-digits. The contact center has been targeted by organized crime on a global basis. These crime rings have mounted persistent attacks that are likely to increase because they perceive security for the phone channel to be "weak."

Figure 1: High Repeat Attacks by Vertical



Source: Verint (2013)

The increase in fraud attempts is exacerbated by the professional nature of the attacks. As Figure 1 illustrates, skilled fraudsters are calling repeatedly and finding success.

Verint believes that professional fraudsters perpetrate 75%-95% of all fraud calls. Anecdotal evidence suggests that skilled fraudsters call multiple times to the same institution, often attacking a variety of accounts. Once authenticated, fraudsters are adept at mining the agent for answers to commonly asked authentication questions that can then be used to authenticate on future calls. These professional fraudsters beat security questions nearly 50% of the time.

> James Jackson, the self-proclaimed "Father of Identity Theft," successfully collected personal information of Wall Street and Hollywood luminaries in the mid-1990s. Most notably, he acquired detailed purchase information from Steven Spielberg's American Express account. He started with only Spielberg's name and Screen Actors Guild membership number. Jackson acquired all of this information while incarcerated, using only a cell phone smuggled to him in prison.

Case Study: James Jackson

Ironically, because contact center agents are trained to make customer experience as pleasant as possible, they often try to help callers remember the answer to challenge questions. They are easy marks for experienced criminals. Beating KBAs is not rocket science. It only takes a few phone calls for a criminal to anticipate and prepare for the types of questions asked. The answers to most questions are easily found on the Internet, leaving everyone exposed to identity theft.

Authentication Based on "Something You Are"

Biometric-based authentication solutions are making inroads into contact centers. Managers recognize the need to employ multiple authentication factors in order to reduce susceptibility to fraud. Obviously, voice biometric-based solutions are best suited for the phone channel.

In 2012, Opus Research began to observe voice biometrics moving to the next stage of its maturity model and adoption curve. The number of individuals who had enrolled voiceprints increased dramatically, moving from fewer than 10 million to over 20 million over the span of 8 months. This progress was the result of two overall factors: 1) improvements in the accuracy of the underlying biometric engines and 2) growth in large-scale implementations at telecommunications companies, financial institutions, healthcare providers and government agencies, where dozens of companies deployed systems supporting over one million enrollees.

Overcoming the First Impediment: Enrollment

The first wave of implementers deployed solutions that require ‘active enrollment.’ Callers are prompted to say and repeat a passphrase or series of numbers during the course of a call. Each caller’s voice is recorded and distilled into a “template” or “voiceprint.” The voiceprint was then stored as the baseline to be used for comparison against the same phrase from the caller on subsequent calls.

As evidence that enrollment is a barrier to adoption, through our surveys, callers have indicated that active voice biometric enrollment is a negative, time-consuming experience. In addition, enrollment often requires assistance from customer service representatives, who are normally incentivized to do other things, such as keep handle time low or ensure the caller’s issue is resolved on the first call. What’s more, early implementations were not ready for prime time. Empirical evidence suggests that a subset of customers and critics tried to break the system – not for criminal or malicious reasons – but for sport.

However, the landscape has changed. Over the past decade, voice biometrics technology has evolved to enable a better experience for the user and better results for the institution.

> ***Voice biometrics can now be implemented as a passive solution running in real-time in the background of the call.***

In contrast to an active solution, which requires the caller to walk through the creation of a set passphrases, a passive solution does not require the IVR or agent to administer enrollment questions or the caller to repeat specific passphrases. Passive enrollment does, however, require either opt-in or opt-out explicit consent.

With a text-independent passive solution, the caller’s audio is separated from the agent’s by the system software. It does not matter what the caller is speaking as long as a minimum of 20 seconds of net caller audio is gathered to create the voiceprint. This length of audio can be sourced over multiple calls if necessary.

The voiceprint is initially stored as part of a “graylist” subset of the database for a period of time, determined by the institution’s business parameters. During this time, the activity on the account is monitored closely for actions that indicate fraud. When the pre-enrollment period has elapsed without incident (and other pre-established business policy requirements are met), the voiceprint achieves fully enrolled “whitelist” status and is then used as the valid voiceprint for the account for authentication on future calls.

Obviating the Need for Active Authentication

In the passive solution, authentication of a previously enrolled voice occurs in the background of a call. Approximately 7-10 seconds of net caller speech is captured and then matched to the enrolled voiceprint associated with the account. The voice biometric system analyzes the vocal characteristics of the caller's voice in addition to associated metadata. An ID Confidence score is returned to the call center agent platform. As the call progresses and more caller speech is captured, the ID Confidence score becomes more certain. The institution can set score thresholds based on the type of transaction requested, account history, account value or other parameters. The agent can then determine whether to validate the caller, request more information, or transfer the call to Fraud Operations.

In fact, the passive solution greatly minimizes the need for the traditional method of asking multiple security questions. A passive solution is text-independent and requires only several seconds of caller audio to authenticate a caller. What the caller says doesn't matter – only that he or she speaks long enough to provide an audio sample. Studies of live deployments have shown that the minimum amount of caller speech needed to authenticate a caller is typically captured during the account information gathering process.

The passive solution fundamentally alters the customer care interaction by allowing the caller to get to his or her request many seconds – even minutes – sooner than with traditional security questions. The agent-caller dialog can flow conversationally without being interrupted for extended KBA questions because the authentication process is running in real-time in the background of a call. In trial deployments, Verint has observed that by the time the caller has finished speaking his request, the agent has already seen the ID Confidence score and can proceed to resolution without further authentication.

The passive solution can also take advantage of speech utterances in a speech-enabled IVR. However, such a solution must be careful to not undermine high automation rates achieved in the IVR. For example, many financial services institutions have automation rates in excess of 85%. A poorly designed voice biometrics system can adversely impact IVR automation rates and subsequently result in increased agent handle time. However, a well-designed passive voice biometric solution does not make special requests of the caller for the sake of collecting speech input. According to Verint, one or two simple navigation commands and entry of account number information (such as a 16-digit account number) is enough to passively authenticate the customer using speech IVR input alone.

Incorporating Multiple Factors

No modern contact center operator relies on a single factor for customer identification and authentication, especially when customer data might be exposed. Large companies have CRM systems, call monitoring/recording systems and analytical resources that already make efforts to identify callers and ascertain the intent of a call. Voice biometrics-based solutions will be used in conjunction with these existing systems and in tandem with risk management resources to apply the level of security that is suited for each caller and each transaction. The 2012 Opus Research survey revealed that callers have grown accustomed to agents asking KBA questions before carrying out instructions for a stock trade or money transfer.

Passive solutions using voice biometrics should incorporate a broad spectrum of multi-factor authentication approaches to provide a holistic authentication profile. Vocal traits, behavioral analysis, account history, information regarding the telephonic origin of the inbound call, and metadata from call records all contribute to an ID Confidence score. When data from all of these sources match the expected profile, the system generates a higher confidence score. Anomalous data will trigger an alert.

Data factored into today’s passive voice biometrics solution include:

- **Velocity information** - Has this voice been observed on other recent calls associated with other accounts, or in high frequency?

- **Single institution fraud** - Is this caller a known fraudster associated with the fraudster Blacklist who has targeted this institution in the past?

- **Industry-wide fraud** - Is this caller a known fraudster already enrolled in the federated fraudster Blacklist database who has targeted a participating bank or other institutions before?

- **Vocal/signal manipulation** - Is this caller showing signs of a voice changer or ANI spoofing manipulation based on the digital signal of the line? [Note: Because fraudsters can change phone numbers, wireless devices, and VoIP services easily and cheaply, this technique cannot be solely relied upon.]

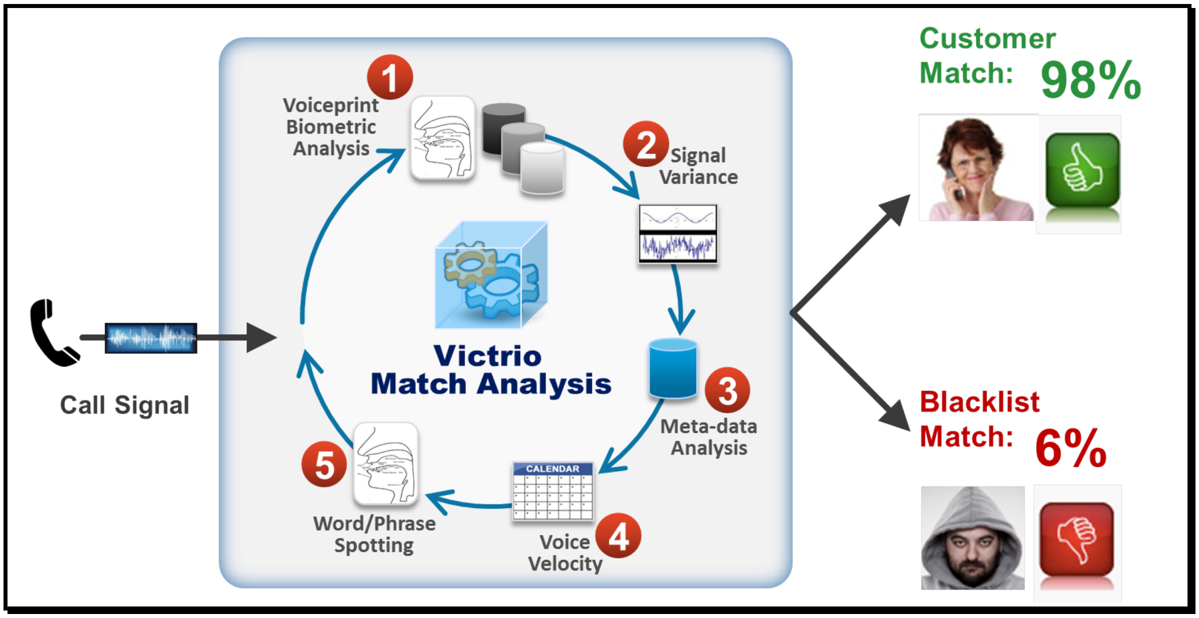
- **Device history** - Is this type of phone device known to be associated with this customer relationship based on digital signal artifacts? [Note: Because fraudsters can change phone numbers, wireless devices, and VoIP services easily and cheaply, this technique cannot be solely relied upon.]

- **Aggregated call-in behavior** - Is this voice continuing to call into this account as expected over time? Are we becoming increasingly confident that it is a “safe voice”?

- **Word/phrase spotting** – Based on what the caller is saying, can we determine the call disposition? Is this caller using words or phrases that are commonly used by fraudsters?

Figure 2 illustrates a high-level process using multi-factor analysis:

Figure 2: Verint's Multi-Factor Approach



Source: Verint (2013)

The institution can tailor its security measures to meet its level of need for authentication based on line of business, transaction type, account type, or other criteria. The difference between past voiceprint implementations and the current passive solution with voice biometrics is that now ALL authentication scenarios can meet the highest requirements of security without sacrificing user experience.

Taking a Passive Approach to Fraud Detection

Any authentication solution, by definition, is attempting to achieve two goals:

- Validate authorized account holders
- Flag potential fraudsters

Passive authentication solutions are the same in terms of objectives. Fraud detection is integral to the passive voice biometrics solution. Yet there are some salient differences surrounding "enrollment" of fraudsters' voices and identifying them during the course of a call.

Enrollment Means Building a Blacklist

As with passive authentication, passive fraud detection runs in the background of a call in real-time. A preamble or announcement can inform callers that the call may be recorded, but unlike authentication, callers are largely unaware that fraud detection is taking place.

Enrolling fraudster voiceprints takes place in a different manner. They are typically loaded in batch mode from historical recordings of confirmed fraud calls. Companies can add to the Blacklist when confirmed fraud occurs with a new voice. As with passive enrollment for authentication, approximately 10-20 seconds of net speech time is required to create a Blacklist voiceprint. This length of audio can be sourced over multiple calls if necessary.

As mentioned earlier, most fraud is committed by professional fraudsters who call repeatedly. However, fraudsters can be detected even before they are formally enrolled in the Blacklist if they exhibit call velocity patterns that are anomalous. Such unusual behavior results in their voice being added to a "watch list" of suspicious voices.

An institution may choose to participate in a federated Blacklist database of confirmed fraudster voiceprints. With participation, the institution agrees to contribute voiceprints of confirmed fraudsters in exchange for access to other participating institutions' voiceprints. This is similar to federated efforts by credit card issuers who make it possible for merchants and other issuers to know if a card is no longer valid. In this model, all institutions in an industry benefit greatly from the ability to more quickly and accurately identify professional fraudsters who are likely to attack multiple institutions on a repeated basis.

No professional fraudster attacks just once and stopping a fraudster on a "first attempt" presumes that the fraudster will not alter his behavior and try again. A first attempt is rarely an only attempt.

Detection of Blacklist Members During Calls

As part of a Dual Screen, all calls are compared to both a Whitelist of valid customer voiceprints and a Blacklist of known fraudster voiceprints. While Whitelist authentication is underway, passive fraud detection will return an alert in real time if the caller's voice is a match to the Blacklist database. At that point, the agent is prompted to handle the call according to the institution's security protocol.

Conclusion: Moving Authentication to the Background

The passive approach to authentication brings clear advantages to both contact center operators and their customers. For financial institutions, fraud is detected and losses are reduced. The vast majority (meaning "law abiding") customers move more effortlessly through each call. Collectively, this lowers customer effort while reducing operating costs.

The passive solution allows call center agents to be more engaged and friendly with authenticated customers. The institution can maintain the management and marketing goal of a customer-focused organization, while call centers can offer personalized security options that change over time because level of required security and authorizations determined by account history, including confidence scores based on the voiceprint and existing account data and metadata.

As a net result, companies can expect an overall increase in customer satisfaction. This is especially true in instances where moving authentication to the background provides for more productive person-to-person interactions between customers and customer service agents. The institution can maintain the management and marketing goal of a customer-focused organization while sacrificing nothing in terms of security.

The passive voice biometrics solution provides greater security with multiple factors incorporated into an ID Confidence score. The new paradigm of passive voice biometric authentication truly is a win-win opportunity for both the customer and the institution.

Only the fraudster loses.