Identity Authentication and Fraud Detection Solution Brief

Faster Authentication and Better Security in the Contact Center with Passive Voice Biometrics and Predictive Analytics

Table of Contents

Contents

Summary

Contact centers are challenged with securely authenticating customers while providing a client-friendly experience. Most contact centers authenticate callers by asking security questions, also called "knowledge-based authentication" (KBA). Today, KBA is increasingly compromised by the growth in cyber data breaches and online social media: security questions do not stop professional fraudsters who have unauthorized access to consumer card information and other personal data. Moreover, customers are often frustrated by the extra 45 seconds or more of talk time required for authentication. Of course, contact centers pay costs in agent handle time even when KBA is not successful.

Verint provides a new solution for authentication, using passive voice biometrics to reduce the need for security questions. Verint Identity Authentication and Fraud Detection (IAFD) screens a caller's voice in real time against a database of known customer or fraudster voices, and reports matches to the agent desktop. Verint IAFD provides frictionless authentication and fraud detection by operating silently in the background of a call. Verint IAFD has the potential benefits of reducing call duration and average handle time (AHT), and improving fraud detection. Verint IAFD is embedded in the Verint recording platform. It is important to note that organizations are expected to comply with their obligations under applicable laws and regulations when using Verint technologies and/or services, including obtaining any requisite consents in relation to the collection, use, disclosure, creation and processing of data.

Caller Authentication by Security Questions / KBA

Knowledge-based authentication (KBA) is a process asking a series of security questions, either static (e.g. mother's maiden name), or dynamic (e.g. last mortgage payment).

Call centers apply KBA to every call, with the intent of stopping fraudulent access. This requires legitimate customers to answer security questions, even while fraudulent calls may represent only a fraction of total call volume.

Security Questions Face Major Issues Today

The KBA process faces major challenges today:

- **Customers are frustrated by longer calls and difficult questions:** Consumer surveys report growing frustration with multiple security questions that make calls longer and difficult. In the online age, customers expect quicker interactions and are frustrated by the talk time required to answer security questions, which may last 45 seconds or more. Moreover, some customers have difficulty answering questions. Security questions are perceived as "authentication by interrogation."

- **Fraudsters are often able to answer KBA:** Professional fraudsters can often answer KBA today. With widespread cybersecurity breaches in the payment system, hundreds of millions of stolen personal and card records have become available to professional fraudsters in the black market.

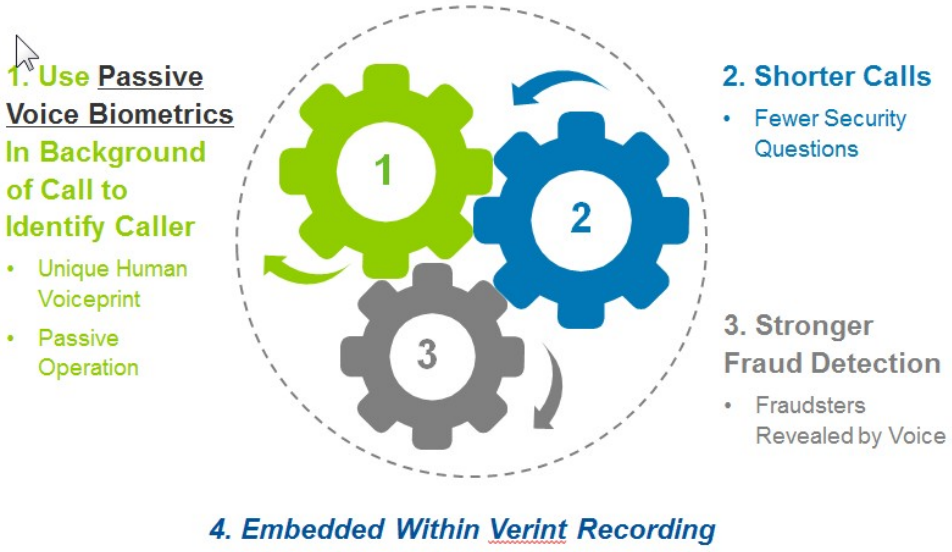
Fraudsters also acquire personal data, like date of birth, from social networks. The U.S. Office of the President stated in 2014 that "Identify theft is now America's fastest growing crime." (Source: The White House Office of the Press Secretary - Remarks by the President on Protecting American Consumers, October 17, 2014)

- **KBA adds to call handle time:** Each security question that is asked adds to call duration. The total authentication process can take 45 seconds or more for certain industries. This makes security questions a significant cost factor.

Verint Authentication Paradigm: Call Screening With "Passive" Voice Biometrics

Verint provides a new authentication paradigm based on passive voice biometric technology. Verint recognizes that a phone conversation contains audio characteristics that can be passively extracted and analyzed to uniquely verify a specific caller. This can be applied to customer verification or fraudster detection in real time.

There are 4 key aspects to this paradigm:



1. **Passive voice biometrics** is a technology which works in the background of a call that can be used by organizations to recognize a legitimate customer's voice or a known fraudster's voice using a caller's "voiceprint", which is a unique mathematical profile of that caller's vocal tract. The process involves use of a call recording to build a "voiceprint" for a caller, and then subsequently during new calls, to compare the caller's voiceprint in real time against that stored voiceprint for verification. The process can be applied towards the goal of customer voiceprint verification or fraudster voiceprint detection. Details follow for operationalizing this process:

- Voice biometrics is effective for caller identification because each human's vocal characteristics can be modeled as a **unique, identifying voiceprint.**

- The Verint system gives organizations the capability to **enroll selected callers without requiring them to speak a passphrase**:

    - The enrollment process involves an organization collecting a voice sample from an agent call.
    - The Verint system allows the organization to flag a call as ready for enrollment.
    - **For the case of customer enrollment**, the organization determines when a customer's voice can be enrolled for an account, including confirming the legitimacy of the caller.
    - **For the case of fraudster enrollment**, the organization determines when a caller associated with an alert should be confirmed as a "fraudster" before creating and enrolling a voiceprint in the database; this typically involves the organization's fraud operations team reviewing and confirming a fraudulent call.

- In **contrast with "passphrase" or active voice biometrics**, the operation of passive voice biometrics does not require customers to speak a specific passphrase during both enrollment and verification of their voice; therefore, customers are not burdened with this additional talk time.

- However, with passive voice biometrics methods, it is still important for an organization to consider and comply with any local law requirements that must be satisfied prior to the utilization of this process.

2. **A voice match is reported in seconds to the agent desktop**. Once a live call begins, within seconds of the caller speaking, Verint IAFD can perform an accurate voice biometrics match against the database of voiceprints. If there is a match with either the voiceprint on record for that customer account, or with a known fraudster voiceprint, the system can be configured to generate an alert to the agent's desktop. Organizations are expected to train their agents on how to handle alerts. For example:

    - Organizations may opt to train their agents to stop asking security questions and serve the customer's request when the agent is alerted that a caller's voice has been authenticated based on the enrolled voiceprint. This may translate to fewer security questions on average, which means reduced AHT costs and better customer experience;

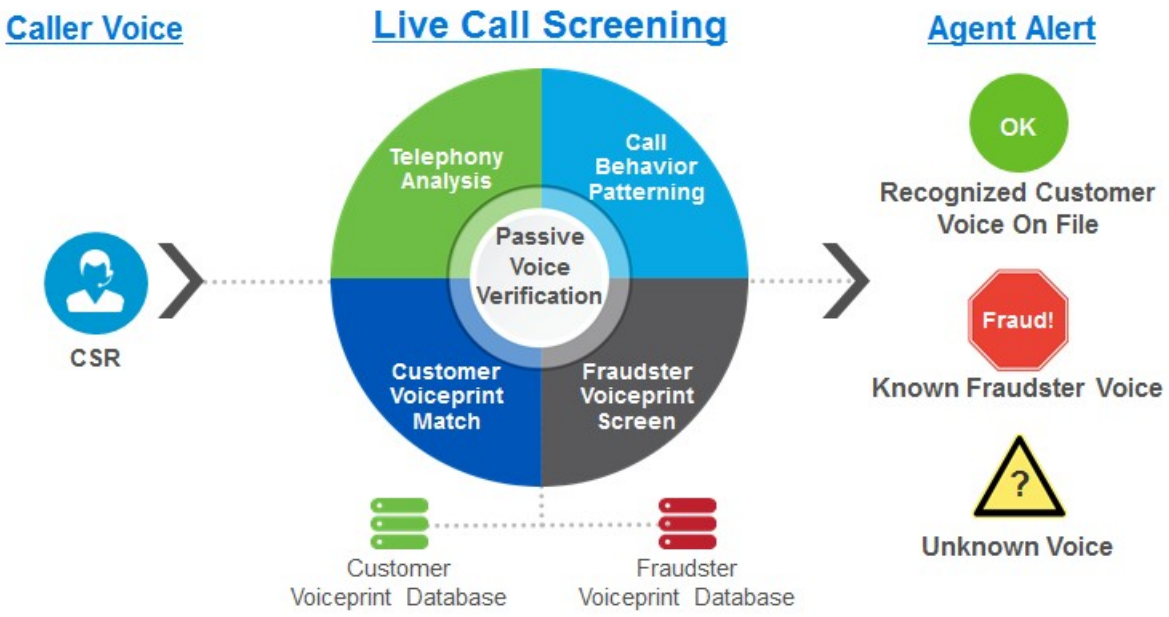
    - Organizations may opt to train their agents to transfer the call to the fraud operations team when the agent receives an alert that the caller's voice matches a voiceprint enrolled in the organization's fraudster database.

3. **Voiceprint detection means much stronger fraudster detection.** Even when a fraudster successfully answers security questions, their unique voiceprint remains unchanged and can be detected. This means that stolen data or social engineering skill do not allow a fraudster to get past voice biometric screening. Once a fraudster's voiceprint is enrolled in an organization's fraudster database, the solution can be configured to generate an alert when it detects repeat calls from the same individual, which provides organizations the opportunity to take action and therefore potentially lessen the likelihood of additional fraud losses by that fraudster.

4. This voice biometric capability is **native to the Verint Recording platform**, a leader in contact center infrastructure. While the solution is embedded in the Verint platform, it can also use third- party call recordings.

Verint Identity Authentication and Fraud Detection Solution

The solution is called Verint Identity Authentication and Fraud Detection. Verint IAFD provides agents with real-time guidance on customer verification or fraudster detection.



How the solution works:

- When a call begins, Verint's voice biometric solution performs "**dual screening**" of the caller's voice for both customer verification and fraud detection. The caller's voice is screened against both the legitimate customer voiceprint on record for that account, and concurrently against a database of known fraudster voices built by the organization over time.

- If a voiceprint match is found during the “dual screening” a process, the solution can be configured to send an alert to the agent. Voiceprint matches are typically detected within approximately 10 seconds of caller talk time. The alerts are simple:

    - **Green** means a match to the customer voiceprint on record for that account. The agent is alerted to stop asking security questions and proceed to assisting the customer.
    - **Red** means a match to any voiceprint in the fraudster database. The agent is alerted to transfer the call to the fraud operations team.
    - **Yellow** means an unknown voice, so the agent can proceed with their usual security questions.

In summary, the Verint IAFD solution has the potential to reduce security questions and improving fraud detection by alerting agents of a voice biometric match, seconds into the call.

Solution Capabilities

- **Passive Enrollment – No Passphrase Asked**

  Verint IAFD gives organizations the capability to **enroll selected callers without requiring them to speak a passphrase**:

    - The enrollment process involves an organization collecting a caller’s voice sample from an inbound call.
    - The Verint system allows the organization to flag a call as ready for enrollment.

  The enrollment process can be applied to customer enrollment for subsequent authentication purposes or fraudster enrollment for repeat fraud detection purposes.

- **Dual Screening**
  Verint introduces “dual screening” to voice biometrics – concurrently screening calls against both customer and fraudster databases and cross-validates scores. This allows the contact center to reduce the number of security questions asked while providing greater security through voice biometric fraud detection.

- **Passive Customer Verification – “One-to-one” Matching against a Voiceprint on Record**
  Verint Identity Authentication verifies the caller by comparing their real-time speech against the voiceprint registered for the account number given by the caller. This is called “one-to-one” matching.

- **Passive Fraudster Detection – “One-to-Many” Matching against a Voiceprint Database**
  Verint Fraudster Detection detects the caller is a fraudster by comparing their real-time speech against the organization’s database of known fraudster voiceprints, which is built over time. This is called **“one-to-many”** matching.

- **Bulk Customer Enrollment from Call Recordings**

  Verint IAFD allows creation of campaigns to automatically enroll users/voiceprints from historical recordings. This requires minimal effort from the contact center manager. Campaigns can be created to auto-enhance enrolled voiceprints with subsequent calls made by the same caller.

Benefits to the Contact Center

The benefits of the Verint Identity Authentication and Fraud Detection solution are significant:

Benefits of Verint Identity Authentication:

- **Savings Due to Reduction in Security Questions and AHT:** After collecting 10 seconds of caller talk time, Verint Identity Authentication performs a voice biometric match against the customer voiceprint on record for that account and reports verification to the agent. Upon notification, the agent can stop asking security questions, which reduces average call duration accordingly. Given that security questions can take 45 seconds or more, this reduction can translate to significant AHT or operating expense savings.
- **Better Customer Satisfaction:** With Verint Identity Authentication, the contact center can effectively offer a "fast lane" to customers, especially frequent callers, who opt to enroll by performing enrollment and verification silently, so customers are not bothered. When enrolled customers call, they experience fewer security questions and shorter calls, which is a desired experience according to customer surveys.

Benefits of Verint Fraud Detection:

- **Reduction in Fraud Losses Due to Stronger Fraud Detection:** The Fraud Detection solution can reduce fraud attacks and losses by helping make fraudster detection capabilities stronger within an organization. The solution can screen all calls against the organization's database of known fraudsters whose voiceprints are passively enrolled by the organization over time. Once enrolled, a professional fraudster may have the stolen data to answer KBA, but there is a higher probability that fraudster will be stopped because their unique voice triggers detection.

- **Mitigation of Fraud Losses Following Security Breaches:** Financial institutions can use Verint Fraud Detection to mitigate the fraud attacks that follow leaked card and consumer information from data breaches in the payment system. By using Verint Fraud Detection to monitor incoming calls to exposed accounts, the call center can identify which accounts are compromised and take corrective action. This screening can lead to preemptive fraud reduction and customer notification, a significant advantage. This gives the organization a preemptive defense to lessen fraud losses and customer fallout from data breaches.

- **Visibility and Discovery of New Fraud Patterns:** Because the Verint Fraud Detection solution can recognize an individual fraudster's unique voice by detecting a match against a voiceprint enrolled in an organization's database, the contact center can track the fraudster's activity across time, calls, and accounts. This gives the contact center the opportunity to mine that data for useful and actionable insights into changing behavior and method of attack.

Solution Options

Verint's voice biometric solutions for customer authentication and fraud detection are available in these three options:

Verint Identity Authentication Solution:

Verint Identity Authentication is an out-of-the-box solution atop the Verint Interaction Recording Platform that provides customer authentication services. Key aspects:

- **Native to the Verint Interaction Recording Platform –** This voice biometric capability is embedded within the Verint Recording Platform. This enables easy integration with call center infrastructure, and faster time to deployment.

- **Customer Voiceprint Database** – Organizations have the ability to build a database of legitimate customer voiceprints, which can be passively enrolled over time. Each voiceprint record includes an identifier to a customer account. The solution matches an incoming voice against the voiceprint on record for that specific account.

- **Real Time** – Verint Identity Authentication operates in real time. After collecting about 10 seconds of caller talk time, the system can detect a customer or employee match against the voiceprints then-currently enrolled in the organization's databases, upon which it can alert the agent.

- **On-Premises** – The Verint Identity Authentication solution is deployed on the organization's site.

Verint Fraud Detection Solution:

Verint Fraud Detection is an out-of-the-box solution atop the Verint l Interaction Recording Platform that provides fraud detection services. Key aspects:

- **Native to the Verint Interaction Recording Platform –** This voice biometric capability is embedded within the Verint Recording Platform. This enables easy integration with call center infrastructure, and faster time to deployment.

- **"Blacklist" Voiceprint Database** – Organizations have the ability to build a database of known fraudster voiceprints, which can be enrolled into the database over time. This database may be seeded over time by extracting fraudster voiceprint from known fraudulent calls. The solution screens the incoming voice

against a watch list fraudster voiceprints.

- **Real Time** – Verint Fraud Detection operates in real time. After collecting about 10 seconds of caller talk time, the system can detect a customer or fraudster match against the voiceprints then-currently enrolled in the organization's databases, upon which it alerts the agent desktop.

- **On-Premises** – The Verint IAFD solution is deployed on the organization's site

Verint Identity Authentication and Fraud Detection (IAFD) Solution:

Verint IAFD is an out-of-the-box solution atop the Verint Interaction Recording Platform that combines both identity authentication and fraud detection services. Key aspects:

- **Native to the Verint Interaction Recording Platform –** This voice biometric capability is embedded within the Verint Recording Platform. This enables easy integration with call center infrastructure, and faster time to deployment.

- **Customer Voiceprint Database** – Organizations have the ability to build a database of legitimate customer voiceprints, which can be passively enrolled over time. Each voiceprint record includes an identifier to a customer account. The solution matches an incoming voice against the voiceprint on record for that specific account.

- **"Blacklist" Voiceprint Database** – Organizations have the ability to build a database of known fraudster voiceprints, which can be enrolled into the database over time. This database may be seeded over time by extracting fraudster voiceprint from known fraudulent calls. The solution screens the incoming voice against the watch list of fraudster voiceprints.

- **Real Time** – Verint IAFD operates in real time. After collecting about 10 seconds of caller talk time, the system can detect a customer or employee match against the voiceprints then-currently enrolled in the organization's databases, upon which it can alert the agent.

Verint. Powering Actionable Intelligence.®

Verint® is a global leader in Actionable Intelligence® solutions with a focus on customer engagement optimization, security intelligence, and fraud, risk and compliance. Today, more than 10,000 organizations in 180 countries—including over 80 percent of the Fortune 100—count on Verint solutions to make more informed, effective, and timely decisions.