Best Practices

Authentication and Anti-Fraud Technology Deployment
This whitepaper is designed for executives and managers considering voice biometrics to identify fraud callers and legitimate customers in call centers. In this document, we will discuss the advantages and challenges of voice biometrics and then describe Pindrop Security’s phone printing technology, which provides similar benefits but has additional advantages. We will then show how deploying phoneprinting first will alleviate the issues raised by voice biometrics - and perhaps meet all the needs of the call center and fraud teams.

After years of relying solely on increasingly ineffective Knowledge-based Authentication (KBA) to screen callers, enterprise call centers are exploring new technologies to help authenticate customers and identify fraudsters. Not a moment too soon – call centers are under renewed attack as increasingly effective controls in the online channel drive attackers to the phone.

Attackers use a smorgasbord of social engineering research and technology to accomplish account takeovers. They hide their origin and mimic their victim using Caller ID or Automatic Number Identification (ANI) spoofing. They steal (or purchase on the black market) personal data from customers and KBA service providers to impersonate their victim and fool call center reps. They jump back and forth from the online channel to the phone channel to get data they can use to authenticate. They call in spurious vacation requests to get call centers to put lower controls in place.

The problem is significant – Pindrop Security research shows that for every call into a financial service call center, $0.57 is lost due to fraud. For a call center receiving 10,000 calls a day on average, that’s $1.5m a year in losses. In addition, fraud calls cause a significant loss to productivity and time by forcing call centers to screen every single call. This is driving the search for technologies to help identify customers and fraudsters in enterprise call centers.

Call center and fraud executives have focused on advanced authentication technology to solve the problem. By positively identifying legitimate customers, advanced authentication would keep all the “good guys” in while keeping all the “bad guys” out.

One such advanced authentication method that is appropriate for the phone channel is voice biometrics, where characteristics of a speaker’s voice are used to authenticate him or her. Voice biometrics is focused on speaker verification, which means confirming the claimed identity of a speaker from his or her voice. In other words, a caller claims to be someone, and the technology then matches the voice to an existing voiceprint. (This is as opposed to speaker identification where a voice print database is searched for a match – this is a much more difficult task.)
Voice authentication is attractive for several reasons. A positive voiceprint can verify a customer, saving time and providing a higher level of security than KBA. And a negative voiceprint can be used to “blacklist” callers, alerting on them or blocking them when they call. And capturing the voiceprint should be easy - customers make calls and talk to call center agents anyway when they need to complete a transaction over the telephone, making their voice available to the call center without having to do anything other than talking. Despite this process, deployments have been limited – only 11% of financial institutions surveyed by the Aite Group indicated they intended to deploy voice biometrics in 2013. What are the challenges that have kept enterprises from deploying these systems?

- **LOW CUSTOMER ADOPTION:** Gartner notes that only about 60% of customers will call into a call center in a given year. Of those, a significant group will be resistant to having a voiceprint created due to privacy concerns. This means that voice biometrics will likely be applicable to 50% or less of customers and that a majority of customers will never be enrolled.

- **POOR CALL QUALITY:** Gartner observes, “10% to 25% of caller voices will fail verification because of poor recording quality.” Pindrop’s own analysis of calls has observed at least 10% of all calls falling below the minimal signal to noise ratio required for voice biometric authentication. When combined, this means that only 25%-40% of calls will be available for voice biometrics scrutiny. This forces call center leaders to leave all the current measures to protect callers in place, eliminating cost benefits. And, it provides a large cohort of unprotected calls for fraudsters to “hide” in. We already see fraudsters act to have themselves routed through the least rigorous process available – either through intentionally missing answers to be sent to the exception queue or through vacation requests that trigger an escalation of privilege.

---

1. The Aite Group, *“Look Who’s Talking: Financial Institutions' Contact Centers Under Attack”* by Shirley Inscoc, April 2013
In addition to the problem of limited applicability, these issues also impact adoption:

- **FALSE NEGATIVE:** Voice biometrics systems are very accurate at verifying a caller, with Gartner claiming that they do not “generate a false-positive or true-negative between 87% and 97% of the time, depending on the quality and consistency of the voiceprints.” But even at those levels of accuracy, the system will falsely authenticate a fraudster more than 1% of the time. Since voice biometrics is a single-layer protection system, this means that once the fraudster successfully authenticates, they have complete access to the system. In other words, there is no other mechanism to detect the fraudster and they will have unfettered access to accounts for a time period that typically is measured in months.

- **DETECTION DELAY:** This delay in time for detection of fraudsters is also a liability with the blacklisting capability of voice biometrics. Blacklisting simply blocks a caller based on voiceprint that has been deemed “bad”. Since voice biometrics is not capable of detecting a fraudster, some other mechanism is required. Typically this is post-incident forensics – often occurring months after the fact – that attach a voice print to a fraudster well after they have stolen from the institution, usually multiple times. “Some credit card

---

**The Lab vs. The Real World**

Voice biometrics performs very well in a lab environment. Typically, voice biometric system detection rates are based on testing using NIST call samples. The NIST sample set is composed of high quality audio with long sample length.

Unfortunately, this is not representative of a real call center. In an actual call center, quality is degraded as the signal originates on a cell phone or VoIP phone over long distances. In addition, call center conversations tend to be short and broken into small snippets, such as “yes” or “no”.

Pindrop analysis of typical call center voice samples showed that only 54% of calls met the minimum speech length for enrollment and 10% did not meet the minimal signal to noise ratio requirements.

---

issuers say that over 70% of fraudsters who call their call centers, call multiple times in any given month. That percentage can go as high as 95% in certain months."

- **NO INTERACTIVE VOICE RESPONSE (IVR) PROTECTION**: Voice biometrics rely on a voice and therefore cannot be used to detect callers in the IVR, were an estimated 40% of calls go and where fraudsters can social engineer account data without speaking a word.

- **FALSE VOICEPRINTS**: Voiceprints can be spoofed by crude methods such as voice distorters or simple mimicry. Or they can be “stolen” by recording someone and piecing together the words. More advanced technologies such as voice conversion, which digitally reproduce a voice, are emerging. While the incidence of these events is still low, advances by adversaries in this area could render current systems vulnerable. In fact, we already hear fraudsters playing television or music loudly in the background in an attempt to mask their voice.

This combination of issues has given deploying managers pause. The Aite Group's research indicates that call center execs' first priority is operational efficiency followed by customer experience. Deploying a solution that adds complexity and cost, without reducing hassle somewhere else, is not compelling.

Pindrop's Enterprise Fraud solution features Phoneprinting™, an audio analysis technology. Phoneprinting was developed by Pindrop Security with an intention to discover just how much information could be gleaned from a phone audio signal. As opposed to voice biometrics, phoneprinting focuses on the entire audio signal of the call. This includes the voice, as well as noise, compression, loss, spectrum, etc.

Phoneprinting measures 147 (and counting) characteristics of the audio signal in order to form a unique signature for the call. In addition to using the phoneprint to identify callers, phoneprinting can identify the region the call originated from and determine if the call was from a landline, cell phone or specific VoIP provider. These additional pieces of information allow us to go beyond blacklisting and whitelisting to assess the riskiness of the call, even when the caller is new or unrecognized.

Phoneprinting complements voice biometrics by addressing these gaps:

- **DETECTION DELAY**: Since phoneprinting can provide caller location and device type, it can identify ANI spoofing. This is an immediate red flag for anyone running a call center that the caller has malicious intent. By detecting call anomalies such as spoofing, phoneprinting can detect a fraud call even if the caller has not been detected previously.

---

• **WORKS ON ALL CALLS:** Phoneprinting functions regardless of call type or call quality. In fact, low quality calls actually make it easier to do analysis - the more noise and distortion in a call, the better phoneprinting performs.

• **NO VOICE REQUIRED:** Phoneprinting does not require voice content and therefore can be used to detect fraud callers in the IVR, where ~40% of pre-attack activity occurs.

• **TRANSPARENT TO CALLERS:** Phoneprinting requires no enrollment and captures no caller voice or content.

• **ACCURATE & EFFECTIVE:** Phoneprinting detects over 80% of inbound fraud with false positive rates below 2%. Phoneprinting provides a score on every call and that score is based on a variety of factors, eliminating the risk of authenticating a bad caller into your environment.

• **SPOOF PROOF:** As opposed to a voice print, which is “portable”, i.e., it can be collected outside of the voice channel or reproduced, a phoneprint contains artifacts which are created by it’s path and is therefore not reproducible without changing the signal. This makes spoofing much more difficult.

According to Gartner, “using voice biometrics combined with phone printing provides the strongest method for authenticating callers and detecting fraudsters”. Phoneprinting and voice biometrics offer a multi-layered solution because they can reinforce each other. Phoneprinting relies on source and channel features that are more difficult to manipulate by an adversary. On the other hand, voice biometrics can provide improved accuracy when good quality audio from the call source is available. When you put them together, you can ensure you identify the right caller, from the right phone, in the right location.

---

**ABOUT PINDROP SECURITY**

Pindrop Security, headquartered in Atlanta, Ga., is a privately-held company that provides enterprise solutions that help prevent phone-based fraud. Its breakthrough phoneprinting technology can identify phone devices uniquely just from the call audio thereby detecting fraudulent calls as well as authenticating legitimate callers. We have helped enterprises eliminate financial losses and reduce operational costs on their phone channel. Pindrop’s customers include two of the top five banks and one of the leading online brokerages. Recently named a Gartner “Cool Vendor” in Enterprise Unified Communications and Network Services for 2012, and recognized with an SC Magazine Excellence Award, Pindrop’s solutions help companies feel more confident in the security of phone-based financial transactions. pindropsecurity.com

Pindrop’s solutions help companies feel more confident in the security of phone-based financial transactions.