PHONEXIA

The Essential Guide to Implementing Voice Authentication in Call Centers

1

Purpose

This document is intended for business and technology leaders in organizations considering or planning the implementation of Voice Biometrics as an authentication method in their call centers or automated systems.

2

Introduction

Voice Biometrics technology is used by hundreds of organizations and millions of callers every day to dramatically improve their call centers' efficiency, security, and customer experience. From our experience of implementing and supporting this technology in many markets, there are four key lessons from the most successful deployments that we use to shape our implementation approach.

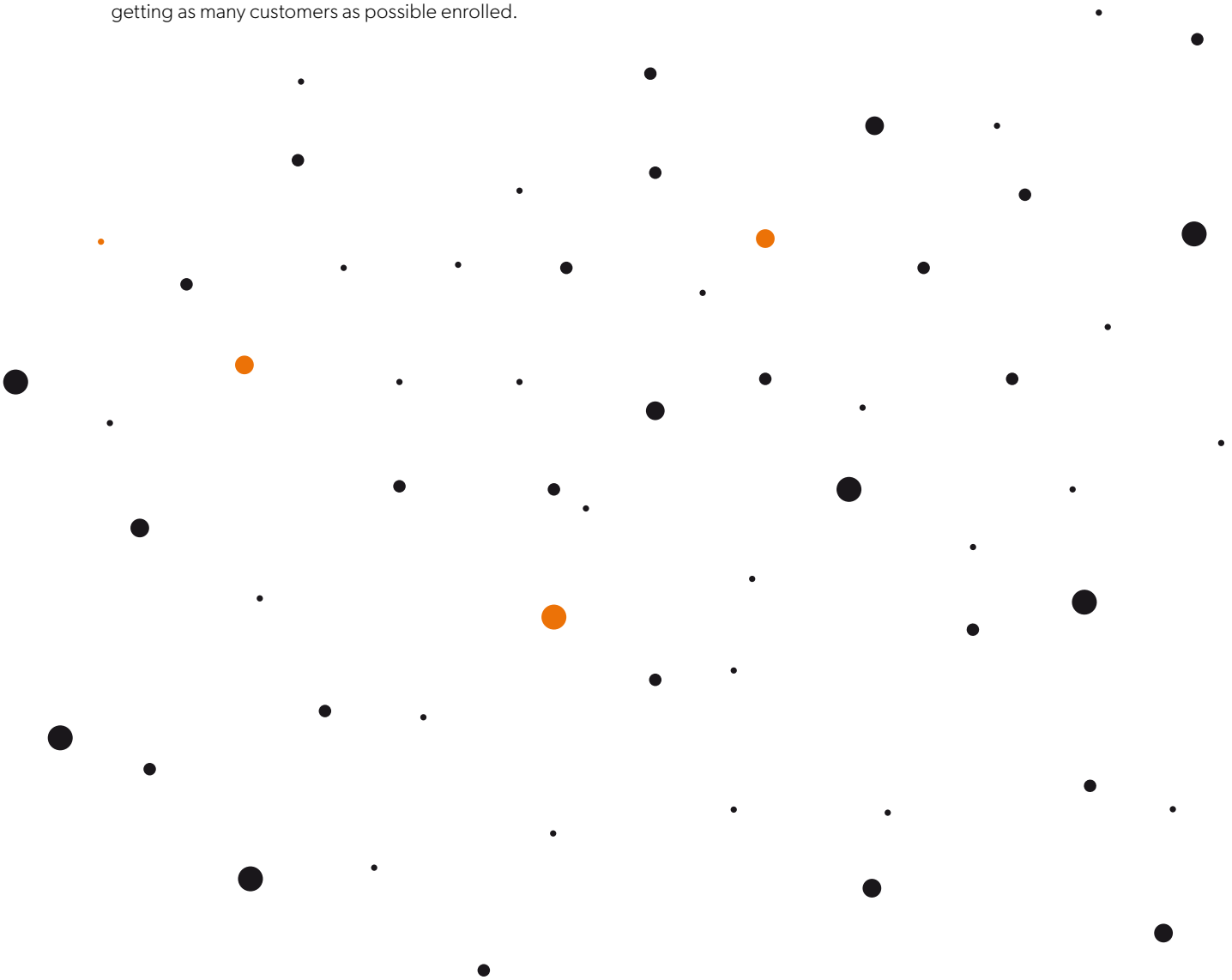
1. **Start by Understanding** – Successful organizations create cross-functional teams and engage relevant stakeholders early, ensuring everyone's understanding of the problem and technology is consistent. This reduces the time to make decisions and accelerates implementation.

2. **Focus On Enrollments** – Only enrolled customers create value, so successful organizations maximize their return on investment by optimizing their registration process and getting as many customers as possible enrolled.

3. **Start Small and Iterate** – Every organization's customers, business processes, and context are different. The most successful organizations reflect best practices from others in their processes, but they initially implement them with small user groups. They then iterate their process and increase confidence before expanding to their whole customer base.

4. **If You Don't Measure It, You Can't Manage It** – There are many steps in the process of creating value with Voice Biometrics, and the most successful organizations understand how each step performs and use data to inform their decision-making.

This guide takes you through a high-level implementation process that is shaped by these lessons.



3

Start by Understanding

3.1. Establish Baseline Performance and Opportunity

Before starting any project, you need to understand the problem you are trying to solve and the opportunity for improvement. Traditional call center authentication processes use knowledge-based authentication to confirm a caller's identity based on something they and the organization know. While this process has evolved over many years, it has several challenges:

- **Customer Experience and Usability** – It is easy for callers to forget the information they need. Even when they don't, the process has several steps that get in the way of solving the customer's problem. It's not unusual for between 20% and 25% of callers to experience some difficulty completing authentication. It's also hard for agents as it's unlikely that they work in customer service because they enjoy interrogating people, but the pressure is often on them to get the process right and not let any fraudsters through.

- **Cost Efficiency** – The process takes both caller and agent time to complete, even when there are no issues. Even the most straightforward process will take at least 20 seconds, and it's not uncommon for the average duration to be closer to 90 seconds when things go right. If the customer doesn't know the answer to the questions or needs to find a document, it can often be several minutes. You could use this time to solve more customer problems or release capacity for other organizational priorities.

- **Security** – Finally, it's not that secure. It's easy for fraudsters to find the answers to many questions used in call centers from social media, public records, or stolen data sources. When they aren't easy to get elsewhere, it's reasonably trivial to socially engineer many customers into giving out their PIN or password.

These issues affect every call center, but one is likely a higher priority for your organization than the others, so make sure you are clear which. When you are certain, identify one or two key metrics to measure now and track through to completion.

3.2. Identify and Engage Key Stakeholders

Call center security and the implementation of biometrics touch many functions in an organization, so everyone must have a good understanding of both the problem (above) and how Voice Biometrics addresses it. The individuals and teams that are important to engage include:

- **Contact Centre Operations** – Responsible for the contact center and its people. They will experience the pain of traditional security processes daily, so they are also the greatest beneficiaries of any improvement. These teams have vital insight into how the current security process performs and, critically, how customers and agents react. This insight is essential in designing future processes. They will also be responsible for the performance of the customer registration and enrollment process.

- **Security and Fraud Teams** – Responsible for investigating fraud and security incidents and setting or advising on authentication policy. These teams will be intimately familiar with the security challenges of the current process and are, therefore, vital in ensuring Voice Biometrics processes are sufficiently robust. They will also play a key role in establishing the appropriate security posture and thresholds for the technology.

- **Technology** – Responsible for the voice technology platform and Agent Desktop applications. Voice Biometrics must integrate with the underlying call center platform to receive the audio and the Agent Desktop to accept claims of identity and display results to agents. The registration and authentication business processes are also, usually, orchestrated by the Agent Desktop.

- **Customer Experience or Business Proposition** – Responsible for the customer proposition, sales, and/or marketing. These teams will have a broad understanding of the business to guide how Voice Biometrics fits in. From their position, they will also understand all the other things that may be changing for customers, so they are vital during implementation planning to avoid any conflicts.

- **Legal and Compliance** – Biometric technology is incredibly powerful but also has the potential for misuse, and as a result, many jurisdictions have introduced specific regulations for its use. While the risk of this with Voice Biometrics in the call center is low, your implementation may still be covered by regulations designed to protect individuals. We always recommend that organizations are open and transparent about its use as we find this increases adoption. Still, it is essential to ensure that the letter of the law is followed and its spirit. As there is little or no precedent on these issues, your legal teams will be vital to ensure your processes are consistent with your organization's risk appetite.

3.3. Ensure Understanding

As a result of coverage in the media and popular press, it is easy for stakeholders to have a different understanding of how Voice Biometrics technology will work in your organization. We recommend that everyone understands these critical concepts from the outset of any project.

- **Authentication, Not Identification** – The call center security process has two components. The first step is for a caller to claim an identity and the agent or automated system to find the customer's record and corresponding voiceprint in your systems. This is Identification and is still required with Voice Biometrics. The second step is to test that claim to make sure they are who they claim to be. This is authentication, and a Voice Biometric system can fully or partially replace existing methods by comparing the caller's voice with a previously enrolled sample.

- **Probabilistic, Not Deterministic** – Traditional, knowledge-based authentication has a binary response. Either the caller got the questions correct or they didn't. When a Voice Biometric system authenticates a caller, it returns a score representing the probability that the caller is the same speaker who provided the enrollment sample. It's up to you to determine the appropriate threshold above which you consider the customer to be authenticated.

- **False Accept and False Reject Risks** – Based on our experience with traditional knowledge-based authentication, sometimes as many as 20% of real customers fail because they can't complete the process. These are known as False Rejects. The same risk exists with Voice Biometrics, albeit it is usually in the 1-5% range, primarily because of audio quality issues or changes in the customer's voice over time. The opposite risk is of a False Accept, incorrectly allowing an imposter through the process. With knowledge-based authentication, we often observe that more than 25% of imposter attempts are successful, and the same risk exists with Voice Biometrics, although, usually at fractions of a percentage point. These two risks are directly related, as represented in the curve to the side. While Voice Biometrics systems produce significantly lower levels of False Rejects, at every level of False Accept, you must decide on the appropriate operating position for your organization. The most significant difference with Voice Biometrics is the opportunity to choose this position and change it over time, depending on the nature of the call, without changing the business process.

- **Text-Independent (Passive) vs. Text-Dependent (Active)** – You can make a comparison between an enrolled speaker and the caller in one of two ways. Traditionally, this has depended on the caller saying the same phrase during enrollment and authentication, such as "My Voice Is My

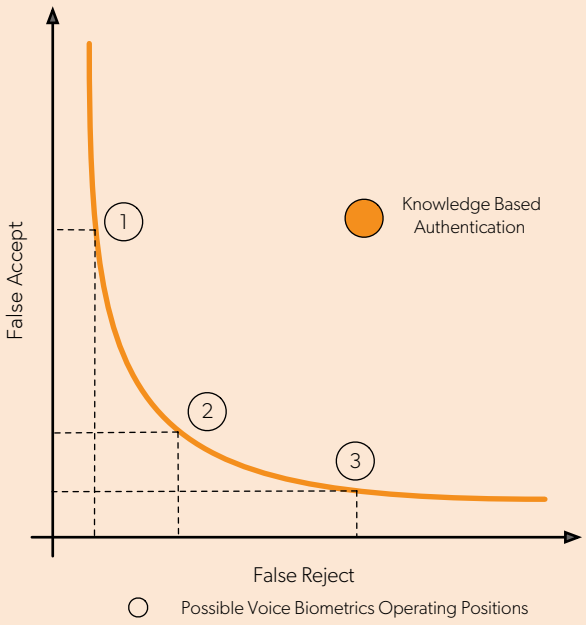


Figure 1 – A graphical Representation of the False Accept and False Reject Relationship

The chart above shows that as the False Reject rate reduces, the False Accept rate increases. The curve continues around point 1, where even the most minor of further reductions in False Rejects leads to an exponential rise in False Accepts. The same is true in reverse, with reductions in False Accepts leading to increased False Rejects up to a point around 3, where the increase becomes exponential.

During implementation, organizations will determine the specific curve for their unique situation using actual customer data but must select the appropriate operating position for their use case. Most organizations prefer somewhere around 2, where increases or decreases in either rate are more or less proportional but can vary depending on the organization's priorities.

It's important to note that at every operating position between 1 and 3, Voice Biometrics is both more secure (False Accept) and more convenient (False Reject) than Knowledge-Based Authentication. In all but the highest-risk use cases, we therefore expect Voice Biometrics authentication to be sufficient to complete the customer request.

Password." This text-dependent approach is also known as active because it requires the customer to actively repeat the phrase several times during enrollment and say something they wouldn't otherwise have said during authentication. Advances in machine learning and computation power mean that it is possible to enroll and authenticate a caller regardless of what they are saying. This text-independent approach is also known as passive because the caller doesn't have to do or say anything they wouldn't otherwise have done during enrollment or authentication. This approach has far higher levels of adoption and customer satisfaction than active and is our recommended approach. Phonexia Voice Verify is optimized for this method and we expect that most implementations will use this approach in the future because of its better customer experience and higher security. As authentication often occurs while speaking to an agent, passive authentication is also far less vulnerable to attack by pre-recorded password phrases.

3.4. Technical Integration Mechanism

Understanding the critical technical integration mechanisms is also vital for the initial phase of the project. The core Voice Biometrics technology is well proven, but it requires two integration points, which will vary significantly from one organization to another.

Audio Acquisition – Passive Voice Biometrics works by listening to the customer side of the call as they talk to the agent. This audio is usually streamed to the Voice Biometrics server using a similar mechanism as recording a call. Still, it may require additional licenses or a specialist integration effort depending on the platform vendor. Most cloud-based platforms have the means to create this stream, and on-premises systems increasingly use standards-based techniques to reduce the work required, but you should confirm this with your platform provider as soon as possible.

Agent Desktop Integration – The Agent Desktop or Customer Relationship Management system provides the user interface for the agent for the Voice Biometric system. It is responsible for telling the Voice Biometric service which customer this caller is claiming to be and orchestrating the required business processes depending on the response. The Agent Desktop is, therefore, responsible for guiding agents through the enrollment process for unregistered customers and authentication for registered customers and handling the inevitable exceptions to this process. While deploying a standalone "widget" to manage these processes is possible, the most successful organizations integrate Voice Biometrics features with their existing business processes to failure-proof agent interactions. This is likely to require custom development by your own or partner's teams.

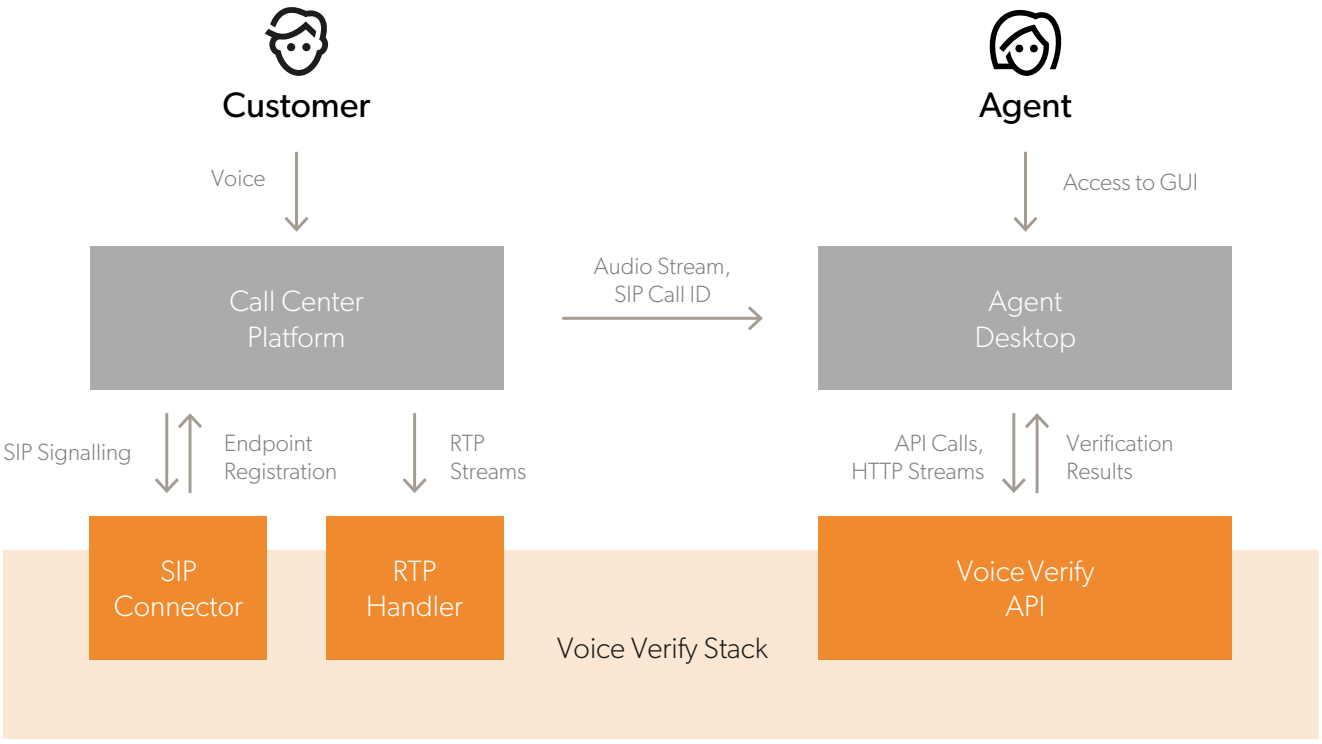


Figure 2 - Integration Points

4

Design for Registration

With the appropriate stakeholders up to speed and an agreed approach for technical integration, the focus should be on business process design and customer journeys. While the value of Voice Biometrics is delivered by authentications, these cannot occur unless the customer is enrolled. Enrollment, however, is just the technical step of creating the voiceprint, which cannot take place until several business process steps have been completed. We refer to this process as registration and optimizing this process to maximize the number of customers enrolled is key to any Voice Biometric implementation's success.

4.1. Registration Process

The registration process consists of the following steps:

- **Identification** – All voiceprints must be associated with a customer, so Identification is required before enrollment.
- **Authentication** – The value of Voice Biometric authentication is dependent on the confidence you have that the enrolled speaker is the real customer. Some level of authentication is, therefore, required for all customers before enrollment. The stronger the authentication, the more confidence you can have in the subsequent voiceprint. It is, however, possible to increase confidence in a voiceprint's authenticity after enrollment through out-of-band notifications and consistent usage. So, don't let this stop you from enrolling customers.
- **Eligibility** – In most cases, there will be a tiny subset of customers to whom you do not wish to offer the service. This could include customers whose accounts are believed to be already compromised by fraudsters, customers with voice-related accessibility issues, or children who may not legally be able to provide consent. In each case, your customer database likely contains the necessary data to identify these customers and prevent the agent from being prompted to offer enrollment. You should also use this step to avoid offering registration to the same customer too frequently. If a customer needs to call you several times in one day, for example, as a result of an emergency or problem, then they are unlikely to accept an offer on their third call of the day if they didn't enroll on the first.
- **Offer** – As the consent disclosure statement below is likely to include some mandatory legal wording, it is often better to offer the customer enrollment before asking for their consent. This allows the agent to tailor the messaging to the specific customer and handle any queries or objections before the

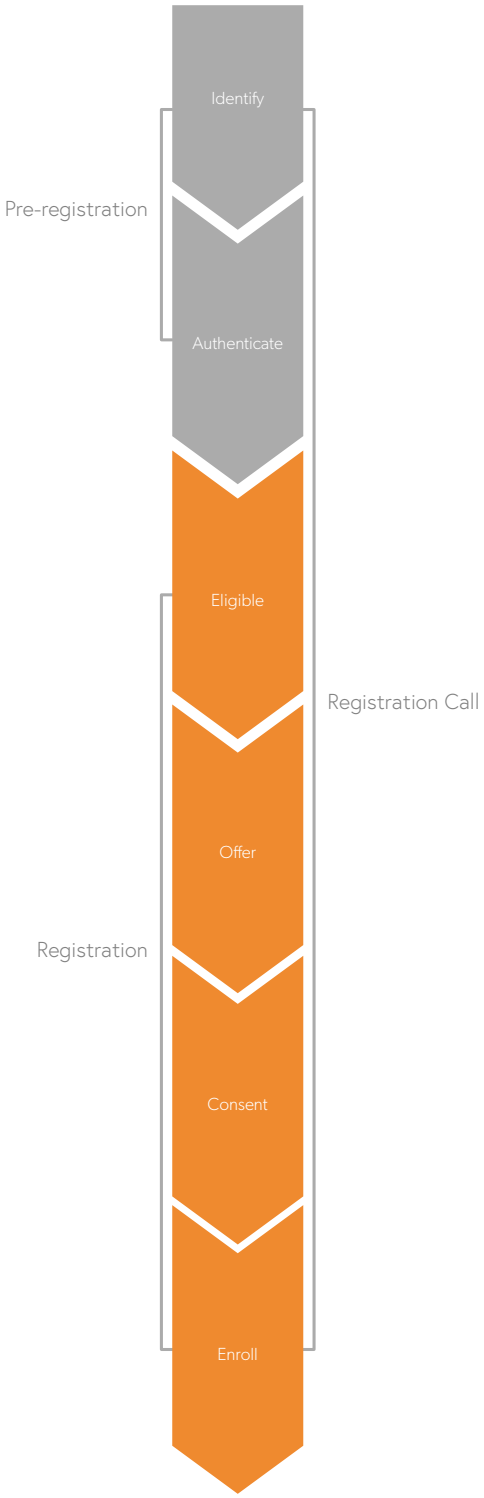


Figure 3 – Registration Process Steps

more formal consent step. It is possible to combine these steps if explicit consent is not required in your jurisdiction, for example. Still, the most successful organizations always provide an opportunity for customers to understand what is changing, ask questions about it, and object, even if few do.

- **Consent** – In many jurisdictions, specific regulations, such as GDPR, require explicit consent from the customer before an organization can process their biometric data. These requirements can be met in most cases by reading a formal disclosure statement to the client and receiving their positive acknowledgment. The detail of this disclosure, how it is recorded, and whether this approach is acceptable varies by jurisdiction and is open to interpretation, so it should be confirmed with your legal advisers. You should not, however, be put off by this requirement. In our experience, customers are more accepting of the technology, which leads to higher levels of adoption when they have some say in its use.

- **Enrollment** – This is the process of creating the voiceprint. All customer audio from the start of the call is held in the Voice Biometric system until it is told how to process it or the call ends. Voice enrollments in Phonexia Voice Verify require 20 seconds of customer speech (this means the customer speaking, so it is different to the duration of the call) which most calls will have. When enrollment is complete, the Voice Biometric system will update the desktop so the agent can manage the customer's expectations for what will happen during the next call.

4.2. Authentication Process

Following registration, a customer can be authenticated when they call back. You should remember that the Voice Biometrics system requires a customer's identity before completing the comparison. In most cases, you only need a few seconds of speech for authentication, which is often less time than it takes for callers to confirm their identity and reasons for calling. Agents should, therefore, receive the match outcome before they need to disclose any information or provide any services. There is, of course, the chance that the caller doesn't match the claimed identity. Either because they are not the genuine customer (True Reject) or score insufficiently against the threshold discussed above (False Reject). In most cases, Voice Biometric authentication alone should be sufficient to allow callers to complete most requests. Still, in some high-risk cases or where regulations require it, it may be necessary to use a second authentication factor such as knowledge or possession-based information.

While it's not unusual to see more than 95% of genuine customers authenticating successfully, you should ensure you handle these mismatched callers appropriately. We consciously avoid terming this outcome "failure" because most mismatches are likely to

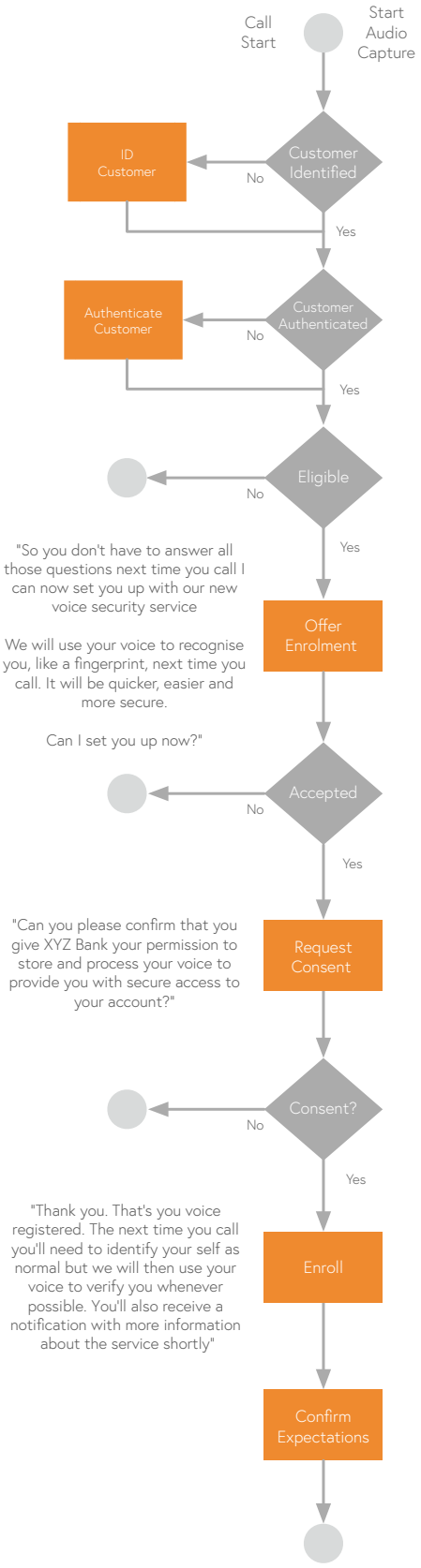


Figure 4 - Generic Registration Process

be the real customer. False Rejects can result from poor-quality enrollments (background noise, multiple speakers on the line, incorrect speaker enrolled, etc.) or the circumstances of their call today (poor quality line, background noise, multiple speakers on the line, etc.). Even when they are not genuine customers, many organizations receive calls from individuals trying to help the real customer (such as partners calling on each other's accounts or caregivers on behalf of elderly customers) and have previously authenticated using knowledge-based authentication. The implementation of Voice Biometrics is often the first time these types of calls are exposed. Most organizations do not generally receive a high volume of imposter calls; for the highest-profile English-speaking financial services organizations, we see less than 1 in 500 calls originating from fraudsters. It can be more than ten times less than that, i.e., 1 in 5000 calls for most others.

Our best practice for handling mismatches is to allow the caller to confirm whether they are who you think they are. It provides an opportunity for partners and caregivers to identify themselves and either change the claimed Identification or retry the Authentication with new audio. Only when this fails should you fall back to your legacy authentication method. Because this is the path fraudsters will also take, you should probably require stronger authentication such as One Time Passcodes for these callers or restrict the services available without it.

4.3. Supporting Processes

Of course, things go wrong, customers change their minds about using the service, or problems with their registrations prevent them from consistently authenticating. While there are likely to be very few of these occurrences, you should ensure well-defined business processes to manage them. The right to withdraw consent and have defects rectified is enshrined in many privacy regulations. Still, regardless, you should allow front-line agents to escalate issues to your team for investigation and remediation.

The biggest reason for opting out of this type of service is that it hasn't performed as the customer expected, probably due to one of the issues identified above. You can quickly rectify this by re-registering the customer, but some checks are likely to be required to make sure the request is not fraudulent. In a small number of cases, the customer may want their voiceprint removed, in which case you should ensure that the request is genuine, they are aware of the implications, and that you will do so promptly.

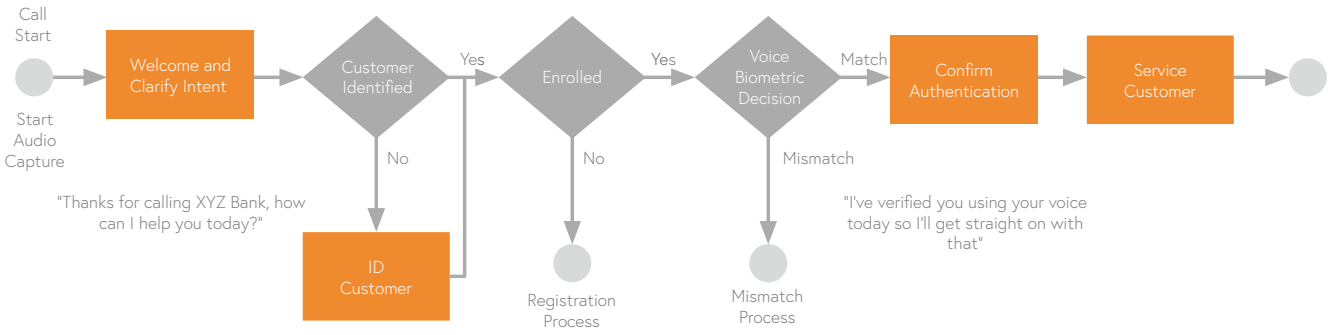


Figure 5 - Generic Authentication Process

5

Crawl Before You Walk, Walk Before You Run

Every organization is, of course, slightly different, so the best practice advice provided here will need to be tailored to your unique circumstances. While some of these modifications can be anticipated, some cannot and will only be understood when real customers and agents encounter the service. During implementation, there are three areas of focus.

- **Integration** – Ensuring that all the individual components can communicate with each other. While this will be primarily proven during testing before implementation, real customers and agents likely do not behave precisely as your tests might expect, creating unpredictable edge cases and potential issues. Identifying and fixing these issues is challenging in high-volume situations.

- **Performance** – Phonexia trains and optimizes its Voice Biometric algorithms using large and diverse data sets. While these ensure high-performance levels for all customers, it is essential to use representative data from your environment to establish appropriate operating thresholds. Until these thresholds are set, you cannot articulate the probability of a False Accept and may, therefore, require additional controls until this is complete. With sufficient data, it should also be possible to optimize the core algorithms for your environment.

- **Customer Acceptance** – Determining the most effective way to offer the service and gain customer consent is likely to require trial and error. Acceptance will also vary across the agent population, requiring team leaders and managers to support agents and manage their performance. It is far easier to learn these lessons and try different approaches with small groups of agents than with your entire center.

Our recommended implementation approach (Crawl, Walk, Run below) is, therefore, to proceed on the assumption of full implementation but with deliberate steps designed to help learn and increase confidence as you go. There are, however, some occasions when additional action before implementation may be warranted:

- **Proof of Concept** – Where there are concerns or gaps in your understanding of how the Voice Biometrics application will integrate with your technology platform, there may be some value in a lab-based proof of concept to test out and prove different integration approaches.

- **Proof of Value** – Phonexia trains and optimizes its systems using extensive data sets and is constantly seeking the highest performance levels, so you should be generally confident that technology performance will not constrain

	Crawl	Walk	Run
	Friends and Family	**Limited Poduction**	**Full Production**
Objective	Prove technology integration and establish initial operating threshold	Prove business process adoption and calibrate system with representative users	Realize business benefits
Users	100s	1,000s	10,000s +
Duration	2–4 weeks	4–6 weeks	Ongoing

Figure 6 - Implementation Steps

your implementation. If, however, your application of Voice Biometrics is in a new or novel environment or use case, there may be some value in obtaining representative sample audio and evaluating the performance of the Voice Biometric application during an offline proof of value exercise.

- **Pilot** – Customer acceptance has exceeded expectations in many markets, but when using this technology in new markets or industries, it may be worthwhile prototyping or piloting the service before committing to full implementation.

5.1. Crawl Phase

We often refer to this phase as the friends and family phase. While the service is in production and live, only a small number of known friendly customers can access it through a unique number or routing strategy. This phase aims to prove the technology integration and identify any edge cases that couldn't be anticipated in testing. While they are unlikely to be fully representative of your customer population, these early users will also provide data to allow you to establish an appropriate operating threshold for the next phase of implementation.

Depending on issues identified and the time taken to gather sufficient data for threshold setting, we generally expect this phase to last between two and four weeks. At the end of this phase, you will need to provide Phonexia with an extract from your system to complete the analysis required to inform your threshold decision.

As the threshold and algorithms used during this phase are likely to be based on third-party data, you should not expect the biometric performance of the system to be representative of the end state. You may well experience several False Rejects and Accepts so should ensure appropriate steps are taken to control access and mitigate this risk by restricting the services available or additional authentication steps.

5.2. Walk Phase

In this phase, the service will be available to a limited number of representative customers. This phase aims to validate the registration process design and obtain representative customer audio for full tuning and calibration of the Voice Biometric algorithm.

Depending on your automated identification capability, it may be possible to select customers at random for registration and route them to a specific agent group trained in registration and authentication. In most cases, however, you will need to identify a subset of your agents who generally handles the same customers and provide them with the training. If this is not possible, then you could consider training a small group for registration and everyone else for authentication.

It is essential during this phase that you have robust management information on each step of the registration process so you can understand the rates of eligibility, offer, consent, and enrollment, as well as how these vary across the agent population. There will likely be some variation in performance, and additional support may be required for some agents. This phase provides a fantastic opportunity to learn from front-line agents about which approaches deliver the highest consent rates and encapsulate the best practice in guidance and training for full implementation. Critically, this phase also provides you with the handle time assumptions necessary to model the impact of full implementation on your center. The registration process inevitably increases handle time, so this phase can also be used to get the right balance between efficiency and effectiveness.

To provide time to test and learn from different approaches to customer offers and consent and capture sufficient audio, this phase may last between two and six weeks. A further week is required at the end of this phase for Phonexia to complete the necessary analysis to inform your threshold decision and deliver an optimized algorithm. You should probably allow an additional week for this decision to be made and implemented before scaling up the service in the next phase.

5.3. Run Phase

With confidence in the technology integration, business processes, and biometric performance, you can now enable the service for more customers and agents to realize the business benefits. The speed of implementation is constrained by the time taken to train agents and the handling time impact of the registration process on your service levels.

Only at this scale is it likely that your supporting process, such as investigation, re-registration, and de-registration, will be used. So, during this phase, you should conduct a first occurrence validation to ensure that they function as intended. It is almost certain that some of your customers will seek to test the limits of your service after registration by colluding with friends or relatives, giving them a far greater chance of success than the average fraudster. When these tests are successful, they will nearly always contact you to report it, and you should, therefore, expect to react to reports of False Accepts.

6

Manage by the Numbers

Because the Voice Biometric value chain spans at least two calls, many process steps, and has natural human variation within it, you must continue to manage it by the numbers. After the excitement of initial implementation, management attention will likely shift to other priorities, so the key metrics from the value chain must be embedded in business-as-usual performance reporting.

The critical output metric should be the percentage of authenticated calls authenticated by Voice Biometrics driven by the eligible caller registration rate. At an individual level, agents should be targeted based on their eligible caller to consent rates.

To manage the performance of the Voice Biometrics decision, you should also track the reject rate (which, of course, includes both true and false rejects), which we would expect to remain constant. After 6-12 months of operation, you should also consider conducting a new tuning and calibration analysis using data from the whole period to validate that performance remains consistent with expectations set at the end of the walk phase and enable further Voice Biometric algorithm optimization.

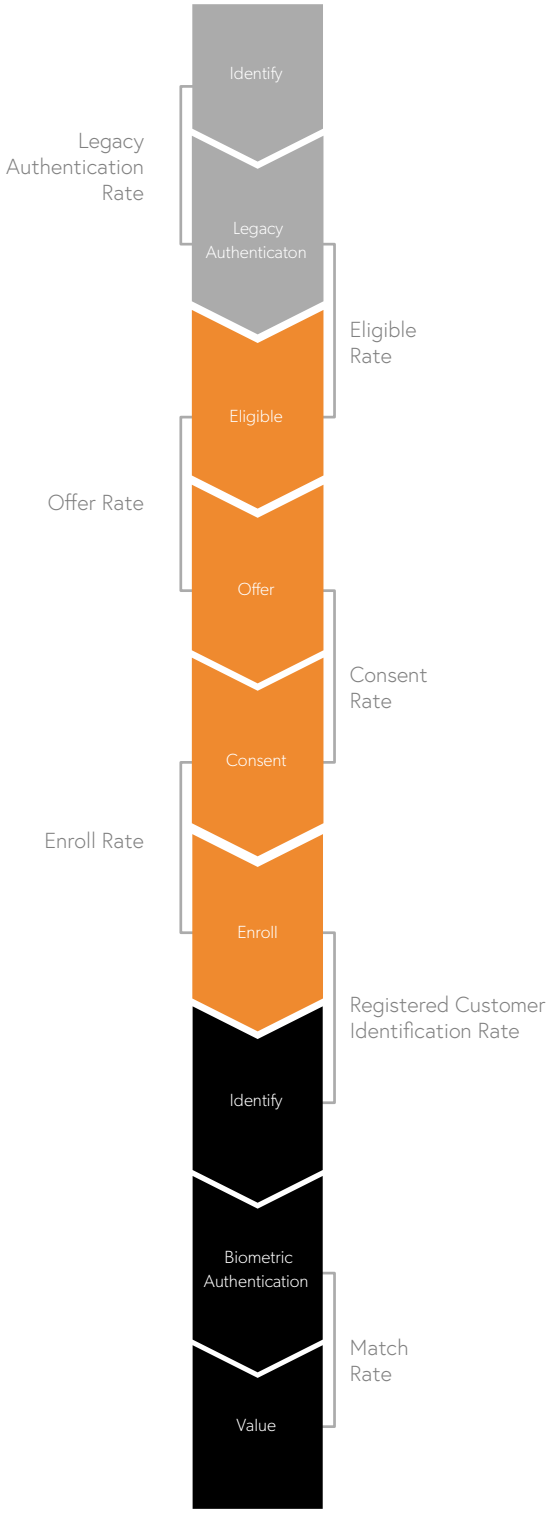
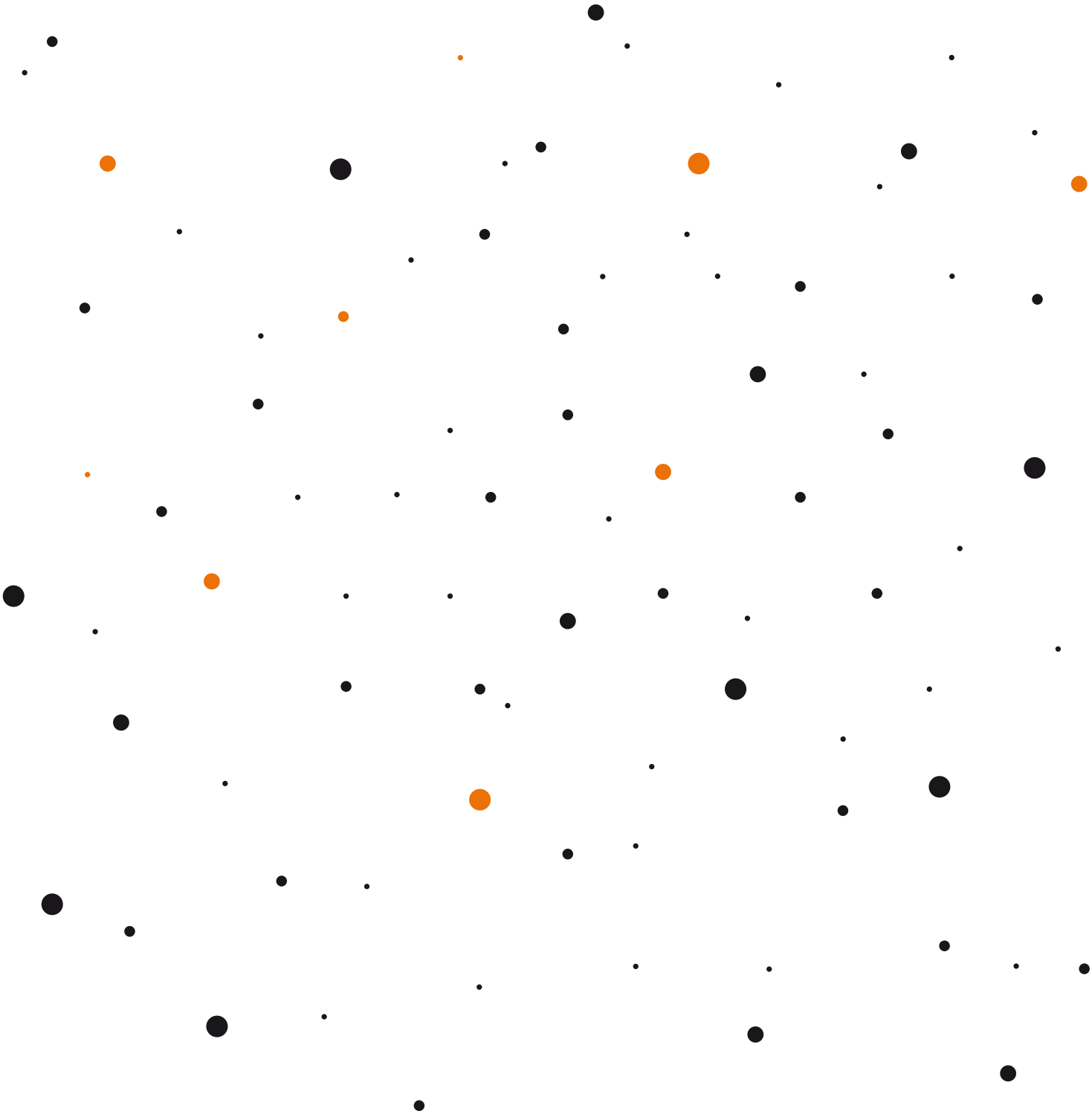


Figure 7 - Key Process Metrics

7

Conclusion

Hundreds of organizations have successfully deployed Voice Biometrics to reduce their costs and improve the customer experience of their call center authentication processes, while reducing or eliminating fraud. Realizing the full potential of these benefits requires a good understanding of the core concepts, a focus on maximizing the number of customers enrolled, an iterative implementation approach, and ongoing measurement.



Matt Smallman

Matt is the founder of SymNex Consulting (www.symnexconsulting.com), which helps organizations unlock the potential of their call centers by improving their security processes. He has more than ten years of experience with Voice Biometrics, having led the first implementation of passive Voice Biometrics for Barclays Bank, and now works with some of the most customer-centric organizations in Europe and North America, including Lloyds Banking Group and Fidelity Investments, to procure, design and implement solutions.

Today, his clients have more than 30 million registered voiceprints, producing significantly quicker, easier, and more secure authentication experiences for their customers. He is co-author of the annual Intelligent Authentication Intelliview published by Opus Research and has featured in the FT, Wall Street Journal, and BBC.

Why Choose Phonexia Voice Verify

1-2-3.

3-Second Verification

Phonexia voice biometrics technology leverages state-of-the-art deep neural networks specifically designed to provide highly accurate verification of extremely short speech.

Quick to Evaluate

Phonexia Voice Verify can be tested via a demo today, your developers can explore its capabilities through a sandbox tomorrow, and a PoC can be finished in just a few weeks.

Support That Cares

Phonexia support is not about solution-evading emails – our European-based team of experts always tackles any challenge you may throw at them, as we care about your success.

Get in Touch

To discuss any of the topics raised in this whitepaper or to arrange a free demonstration of voice biometric authentication, reach out to your Phonexia representative or send us an email at **info@phonexia.com**.

PHONEXIA

+420 511 205 265

info@phonexia.com

Phonexia s.r.o.
Chaloupkova 3002/1a
612 00 Brno
Czech Republic
European Union

phonexia.com