The 2023 US Contact Center Decision-Makers' Guide

The Customer Identity Verification & Fraud Reduction chapter

Did you know 92% fraudsters pass KBAs while only 54% of valid customers do?

How?

Fraudsters are able to pass KBAs using the dark web

- 2021 was a record breaking year for data breaches
- Data dealers are now more sophisticated, offering more services, more organized information, and even returns!
- With all this information available, how can Knowledge
- Based Authentication questions still be utilized?

What's next?

Customers are ready for a change

- Consumers are more willing to use advanced authentication technologies
- Consumers who use advanced ID verification are more positively inclined towards the brand
- 39% say advanced ID verification methods would positively impact their trust in the organization offering them
- 70% of those interested in technologies for data security and asset safety report that these methods improve customer satisfaction

For a deeper look at this study, download Pindrop's 2022 Voice Intelligence and Security Report

Source: All facts and figures are sourced from the 2022 Pindrop® Voice Intelligence and Security Report. *92% of calls, later validated as fraudulent, showed KBAs had been passed, while 46% of customers were unable to answer the KBA or unable to be matched with an ID Claim.

Enterprise-grade fraud defense, caller authentication, and call verification for Contact Centers.

Voice Security Platform

Pindrop combines best-in-class audio, voice, and AI technologies with a comprehensive risk database to provide added protection across the phone channel. Pindrop's multifactor anti-fraud and authentication solutions work together for enhanced protection and more detailed cross-channel intelligence. The solutions available include:

- **Pindrop® Protect Anti-Fraud**: Enterprise-grade multifactor fraud detection and intelligence for the contact center that utilizes a combination of best-in-class audio, voice, metadata, and AI technologies to help defend your contact center against threats.
- **Pindrop® Passport Caller Authentication**: Passive multifactor authentication tool that utilizes device, behavior, network, risk and voice to improve contact center customer experience, average handle time, improve self-service, and reduce operational costs.
- **Pindrop® Call Verification**: Simple, easy-to-integrate solution to improve IVR authentication and customer experience via enhanced phone number (ANI) authentication, spoof detection, STIR/SHAKEN ingestion, and identified fraud risk.

Exceptional Client Services

At Pindrop, we're invested in setting the industry standard for customer service and access to experts. Pindrop's Client Services team is founded with true authentication experts and certified fraud examiners, representing over 200 years of experience. Client Services delivers tailored authentication and anti-fraud advice to provide the best possible impact to your business, and help you stay ahead of the ever-evolving fraud tactics and authentication guidelines.

Security, Identity, and Intelligence for Every Voice

As humans, our most intrinsic communication method is our voice. Pindrop's advanced audio and voice analysis technology recognizes this distinct and unique human quality with the kind of precision and certainty that's needed when access to information is essential. Protecting some of the world's biggest banks, insurers and retailers, Pindrop® Solutions enable companies to prevent fraud and deliver exceptional customer experiences in call centers, obtain information from smart devices and even activate cars. A privately held company, Pindrop is venture-backed by Andreessen Horowitz, Citi Ventures, Felicis Ventures, CapitalG, GV, IVP, and Vitruvian Partners.

Visit pindrop.com for more information.

Contact: info@pindrop.com

Customer identity verification & fraud reduction

Customer security processes are about two factors: are you who you say you are, and are you allowed to do what you are trying to do?

Until a few years ago many businesses relied on trust that the caller was who they claimed to be, asking only for a name and address. Today, identity verification processes are now seen as critically important and most calls that are not initial enquiries will need to verify a caller's claimed identity by asking for additional information that only the real customer should know (knowledge-based authentication, or

KBA). However, fraudsters have often gained access to personal information such as mother's maiden name and date of birth, along with payment card details that have been stolen from websites, and research has shown that knowledge-based questions are answered correctly by fraudsters the large majority of the time.

The increasing focus upon fraud detection, strengthened by the need to comply with regulations, has meant that identity verification continues to become more important year-on-year, yet businesses have been slow to take up alternatives to the traditional challenge/response method.

Identity theft is high-profile, and businesses have tightened security and been seen to do so by their customers: fraud prevention is a brand issue, as well as a regulatory one. While fraud certainly causes losses to a business, along with the threat of regulatory fines, risk of losing customers' confidence by being seen as lackadaisical about security is at least as great a risk. Criminals' methods and the technology used have become more sophisticated, and businesses responded by introducing ever more complex identity verification processes.

In many cases, customer identity verification has become intrusive and inconvenient for the customer, who is expected to remember an increasing array of IDs, passwords, PINs, memorable information, or details of their last transactions. Customers can undergo a 'Spanish Inquisition' before being permitted to make their inquiry or place their order – not only reducing customer satisfaction, but also costing businesses time and money. It takes an average of around 40 seconds to verify a customer's identity manually, and this mounts up considerably: the US contact center industry spends billions of dollars each year, just to verify the caller is who they claim to be, and are permitted to do what they are asking.

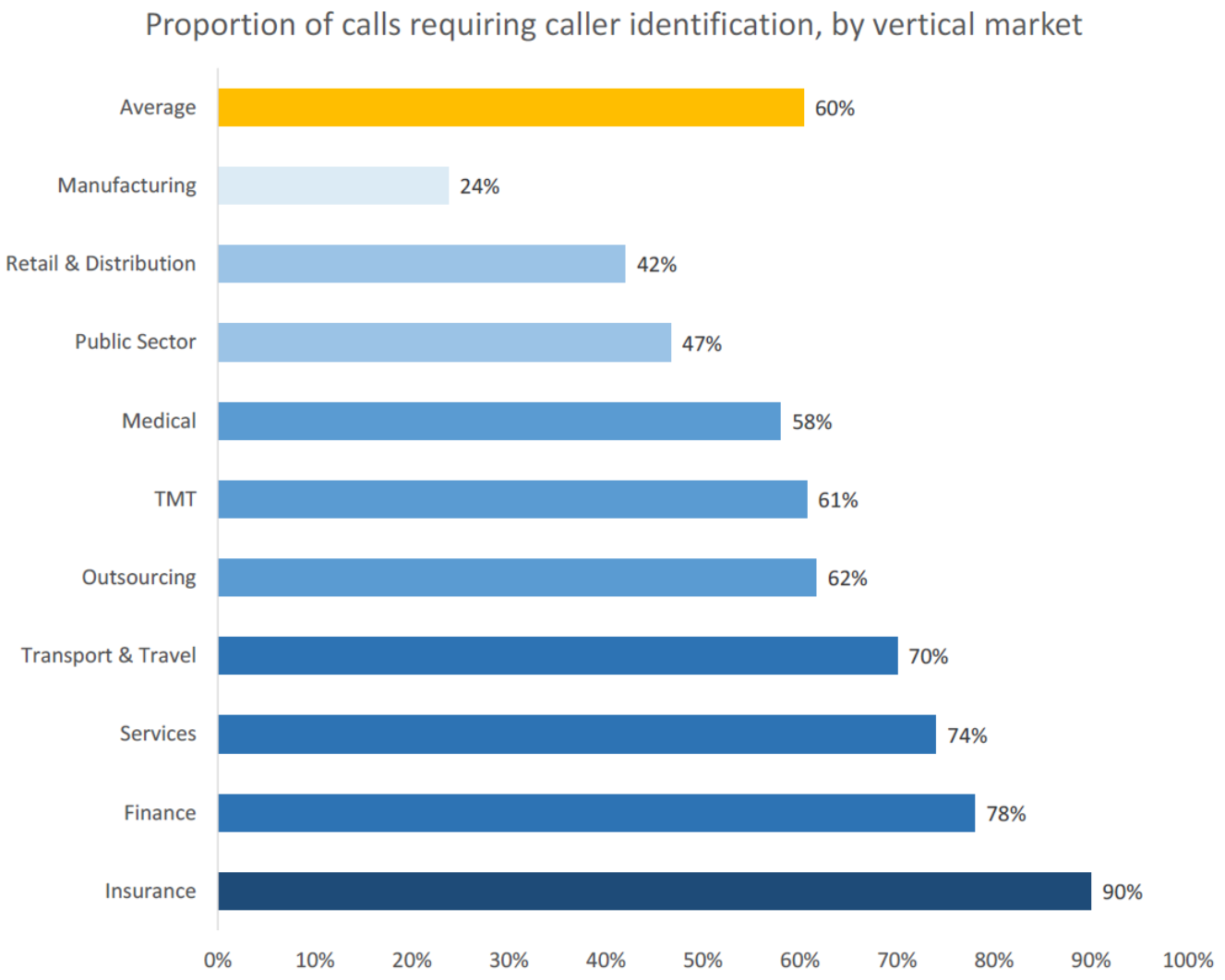
Identity verification processes are typically based on one or more authentication factors that fall into the following generally-accepted categories

- something you know - e.g. password, PIN or memorable information
- something you are - a biometric such as a fingerprint, retina pattern or voiceprint
- something you have - a tangible object, e.g. a PIN-generating key fob, the 3- or 4-digit security code on payment cards or a registered phone to which an SMS or other authentication code can be sent.

Combining these factors creates a more complex, and potentially more secure two-factor or three-factor authentication process (2FA / 3FA), although this is often quite inconvenient and time-consuming for customers. Being able to rely upon previously enrolled voice features or having the calling device, location and other factors assessed pre-call (rather than have to remember various pieces of information or carry round a code-generating device) can make identity verification far quicker and easier for the customer.

Industry-wide, a mean average of 60% of calls require caller identity verification this year. 37% of respondents state that all callers go through identity verification, with 21% stating that they never do so. Insurance and finance operations are the sectors most likely to require identity verification. Public sector respondents (which include information lines), and retailers and manufacturers (often sales and product support) are the least likely.

As we would expect, service-oriented operations are far more likely than sales-focused contact centers to require authentication, as access to user accounts is required.

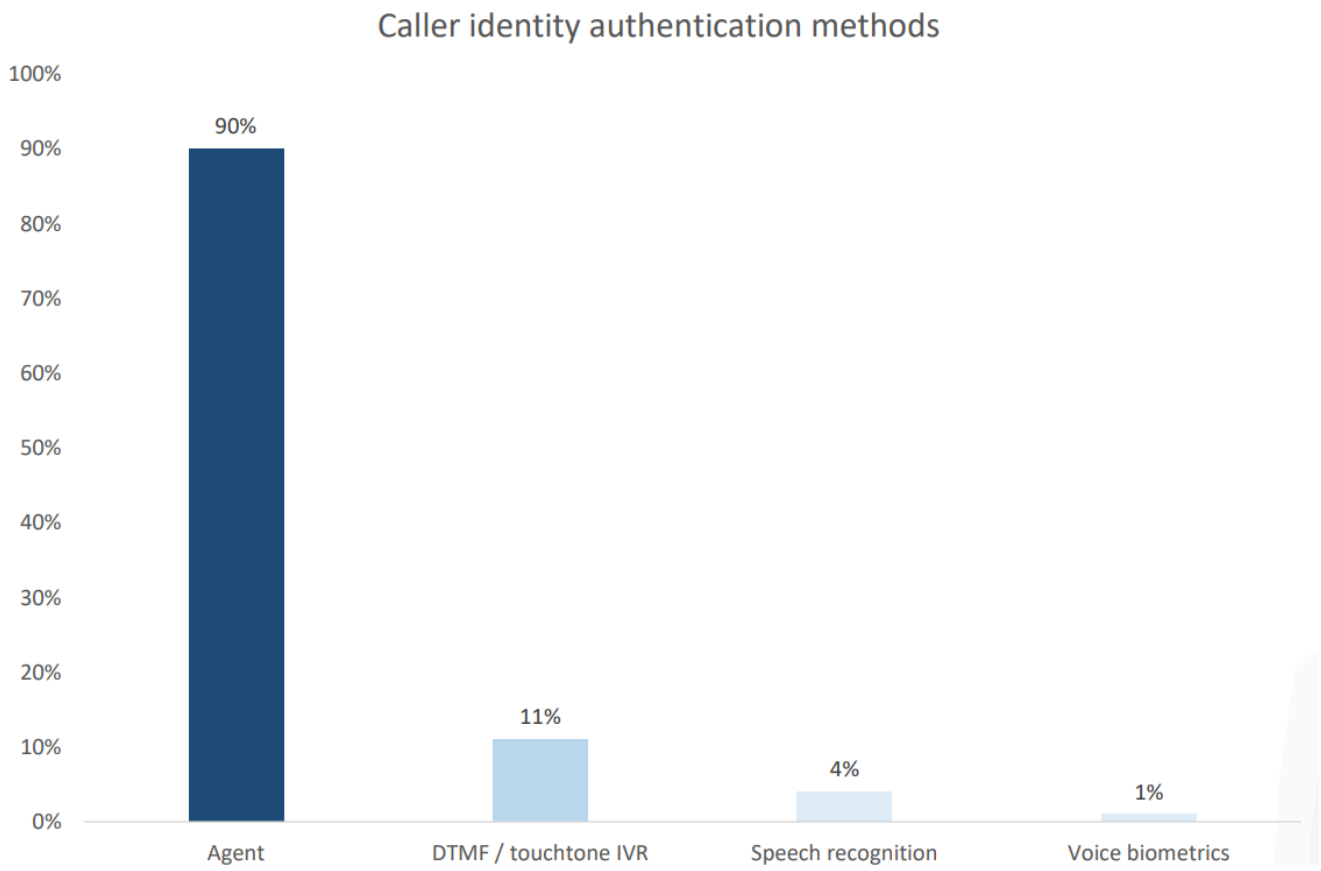


Live agent authentication accounts for 90% of calls. 11% of calls are authenticated with DTMF touchtone IVR and 4% use speech recognition to identify the caller, which itself can take around 30 seconds and 1% are carried out through voice biometrics.

In small and medium operations, the vast majority of customer identity authentication is carried out by agents, rather than automation.

Respondents from larger contact centers with far higher volumes of calls are more likely to use some form of automation – usually DTMF IVR – to authenticate customers.

However, the vast majority of respondents that use IVR or speech recognition may also use the agent to double-check once the call is passed through, wasting the caller's time and increasing the contact center's costs



NB: totals may be more than 100% e.g. all calls may be authenticated by IVR, with some of these then requiring agent checks.

The mean average time taken to authenticate using an agent is 39 seconds. The figure for authentication using an IVR is only a little less, although the main difference is that the agent's time is not used, so the call duration (from the operation's perspective) and cost per call is reduced.

Those in the transport & travel sector who use customer identity verification take an average of 62 seconds to do so. Outsourcing respondents again report taking the least time.

The unnecessary cost of caller authentication

Using figures from this report and other ContactBabel research, it is possible to estimate the industrywide cost of customer identification authentication using an agent. Please note that as respondents change each year, this figure is an indicative estimate based on this year's survey and should be read as such. We have assumed that only service-related calls for existing customers will require authentication.

60% of all calls require a security and identification process to be completed first. This year, 90% of calls were reported to be authenticated by agents. On average, it takes 39 seconds to go through security.

Using these statistics, it is possible to estimate how much US contact centers spend each year on screening customers by using agents.

- Inbound calls per year (handled by agents): 29.5bn[1]
- Proportion of inbound calls that require security and identification checks: 60%
- Average length of agent-handled security and identification check: 39 seconds
- Average call duration: 7m 6s (therefore 9.2% of the call is ID&V)
- Mean average cost per inbound call: $6.55
- Cost of time spent on agent-handled security and identification check: 60.3c per call
- Overall cost of agent-handled security and identification checking: $9.6bn per year.

Although not contact center-related, it is worth noting that at large scale, the cost of sending one-time passwords (OTPs) by SMS is considerable: it is estimated that the total cost of sending OTPs is $5bn per year which is a major cost particularly for many large banks. Added to this, customer experience is impacted as it can take several minutes for an SMS or email to be received and the code entered, and it is not always convenient for customers to do this.

To recap, there are several factors to consider when trying to predict changes in the ways in which customers are identified:

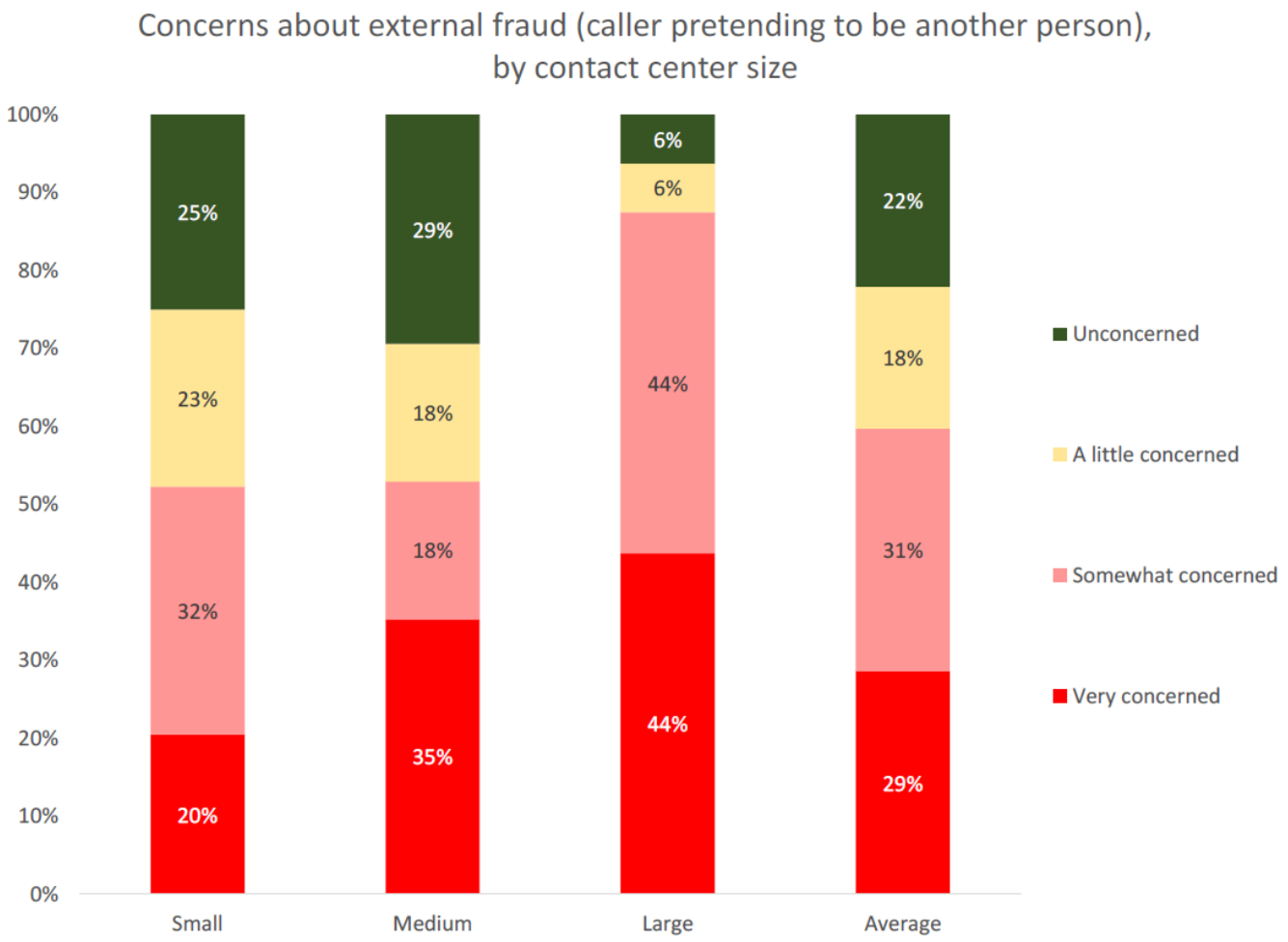
- businesses want to reduce the cost of fraud
- customers want convenience, but also their personal information and assets protected
- businesses need to comply with existing and new laws and regulations
- the contact center industry spend excessive amounts of money on identifying and verifying customer identities
- existing methods of identity verification (e.g. PIN, password, device, etc.) are not secure and/or are user-unfriendly
- knowledge-based authentication has been shown to be insecure in itself
- it is not just criminal fraud that identity verification aims to stop. The issue of privacy, especially in the healthcare vertical market, is a powerful driver for using right-party authentication to facilitate personal information sharing. This is also the case when using speech-enabled automated outbound calls, it being necessary to make sure that the person answering the call is the one to which the business actually needs to talk.

Threats from fraud

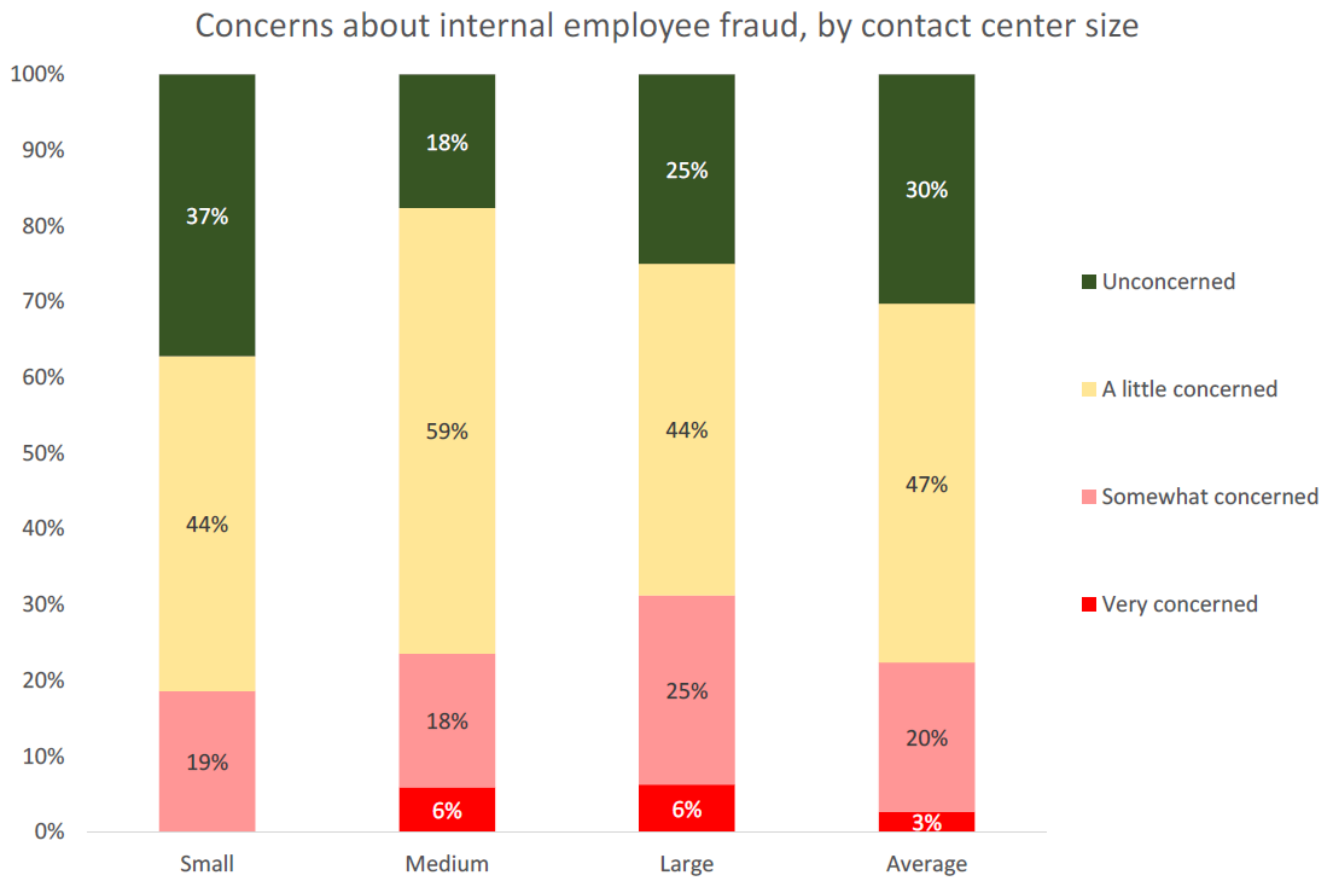
Respondents were asked to rate the level of concern they had about the possibility of fraud coming from various sources.

88% of respondents from large contact centers stated that they were very or somewhat concerned about external fraud, defined within the survey as the caller pretending to be another person. This shows that customer identity verification is taken very seriously, and that many organizations do not feel that they have an acceptable level of fraud control.

Figure 5: Concerns about external fraud (caller pretending to be another person), by contact center size



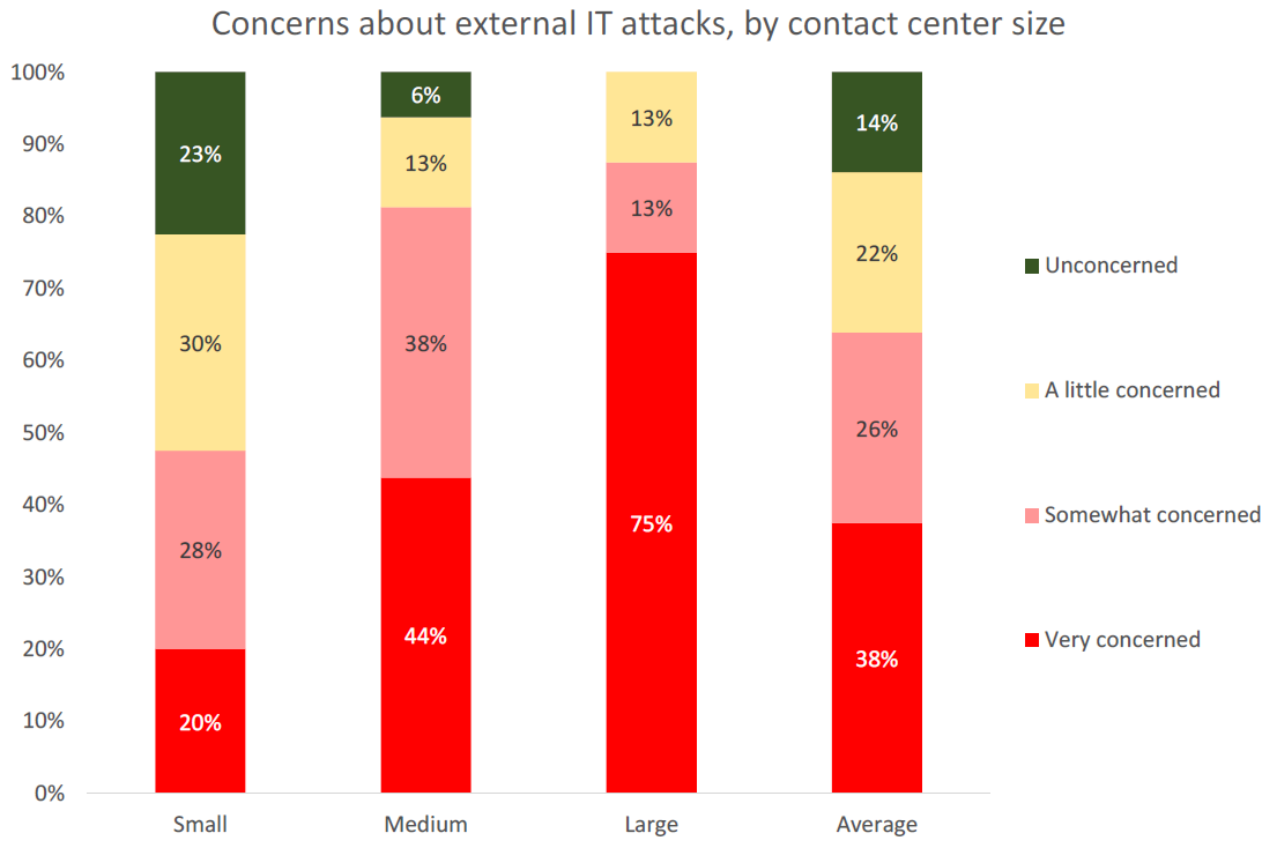
Levels of concern about internal employee fraud were much lower, although 31% of respondents from large contact centers were either very or somewhat concerned about this.



Concerns about external IT attacks were very much weighted towards larger operations, which are likely to be representing larger organizations.

Finance, insurance, outsourcing and services respondents were most likely to be very concerned, with manufacturers being least concerned.

Figure 7: Concerns about external IT attacks, by contact center size



The emergence of biometric technologies

Biometric technology uses physiological or behavioral characteristics to verify a person's claimed identity. Physiological biometrics includes fingerprints, iris, or retina recognition, and voice verification. Behavioral biometrics includes signature verification, gait and keystroke dynamics.

Of these, voice is the only biometric that can currently be used over the phone, making it a viable identity verification solution for contact centers. It should be noted that many businesses now allow smartphones with thumbprint- or face-recognition to be used as trusted devices to log into mobile apps.

Voice verification systems use spoken words to generate a 'voiceprint', and each call can be compared with a previously enrolled voiceprint to verify a caller's identity. It should be noted that the word voiceprint' should be used carefully, as it incorrectly implies that it creates a single element (like a fingerprint) that can be viewed and analyzed, making reverse engineering possible. This is not the case: these voice features are hashed, anonymized mathematical maps of a person's voice as it is delivered, regardless of age, language, content, etc. that are unique on delivery and measured against audio artifacts the human ear cannot ascertain. These audio artifacts of a person's voice make replay and deepfake synthetic voices score significantly lower and thus will not be properly authenticated.

Systems generate a voiceprint by using spoken words to calculate vocal measurements of a caller's vocal tract, thereby creating a unique digital representation of an individual's voice, as well as other physical and behavioral factors, including pronunciation, emphasis, accent, speech rate and other audio artifacts. These systems are not affected by factors such as the caller having a cold, using different types of phones, or aging.

A significant advantage of voice biometric verification is that both enrolment and verification can be done unobtrusively – in the background during the natural course of customers' conversations with an agent – using text-independent and language-independent technology. Real-time authentication significantly reduces average handle time and improves the customer experience by utilizing voice biometrics to authenticate customers within the course of the conversation.

With this advanced technology, contact centers can:

- Voiceprint the vast majority of customers for seamless passive enrolment: in the course of a conversation, a voiceprint is created for that customer which lies on record for them to be authenticated against on the next call
- Securely authenticate customers with zero customer effort: the first few seconds of a call will be enough to match the customer's voiceprint against those on record
- Cut seconds off average handle time: no need for customers to answer numerous security questions as the conversation they are having provides enough information to identify them
- Significantly reduce fraud risk for all customers, and deter fraudsters when combined with other layers of security, for example, phoneprinting, which analyzes the background audio of the call.

However, voice biometrics, while an excellent authentication tool, is not enough to deter fraud attacks. In fact, researchers at the University of Alabama[2] have found that a fraudster armed with just a few minutes of recordings of a person's voice could build a model of the victim's speech patterns and successfully pass voice biometric security. While technology has advanced since then, as voice is a characteristic unique to each person such attacks essentially give the attacker the keys to that person's privacy, which strongly suggests that voice biometrics in itself is not always enough to create the highest levels of security.

The customer's experience of voice biometrics

Since speaking is natural and intuitive, a well-planned implementation can result in a better customer experience that reduces the need for PINs or passwords. For example:

- In the case of text- and language-independent authentication, the customer's voiceprint (collected on previous calls) is authenticated in the background during the natural course of conversation with an agent while simply outlining their service request, minimizing both customer effort and time-to-service. There is no need to remember PINs or passwords, which greatly improves the customer's experience, although if further authentication is needed, the agent can revert to KBA
- 'Account Number'-based voice verification: the caller is asked to speak their account number. The account number identifies the caller, and the spoken words are used to generate a voiceprint that verifies the caller is the account holder
- 'Challenge Response': typically, the customer is asked to repeat a series of numbers, e.g. "Please say 'one seven three four'". The spoken words are used to generate a voiceprint. The numbers spoken are usually different each time the caller phones.

In cases where a two-factor authentication process is required, voice verification can be combined with a 'something you know', such as an answer to a memorable question. Real-time agent guidance can prompt agents to ask a further security question within the call if the process requires it.

The business benefits of voice biometrics

Businesses benefit from two types of savings. These can be illustrated in the following example:

A contact center receives 10 million inbound calls per annum with the existing identity verification procedure taking on average 39 seconds and being performed by an agent:

- Eliminating the time taken by an agent to verify a caller's identity can save 60.3c per call ($6.03m per annum)
- Secure automated identity verification enables a broader range of fully automated services to be offered, reducing agent cost.

The potential benefits for the business are huge, and the customer also gains through a better experience, longer opening hours and greater identity protection.

Similar savings will also be found in the case of text-independent authentication, where the caller's voiceprint is authenticated within the natural course of the conversation. The agent begins each call by immediately asking how they can help the customer, and the authentication process is carried out by voiceprint verification at the same time that the agent is listening to the caller and preparing to help them.

It is also possible to use contextual analysis, such as the caller's geolocation (as detailed from their mobile phone's GPS coordinates, or their ANI) to add another layer of confidence in the security process, automatically notifying the agent whether the caller has been identified successfully, and guiding the agent to ask alternative questions if further verification is required.

Contact centers wishing to deter fraud should consider combining voice biometrics with phoneprinting technology for a multi-layered solution. Phoneprinting relies on background audio, source, and channel features that are more difficult for an adversary to manipulate than voice. Phoneprinting can detect CLI spoofing, voice distortion, and social engineering-based fraud attempts, which voice biometrics by itself would have missed.

Voice verification can also be used to protect the enterprise against repudiation (where the customer says at a later date that they did not do it) as it can verify the physical presence of an individual at the other end of a phone line. Interestingly, this capability is already used by various US law enforcement agencies to check that released offenders are where they should be.

For procedures such as internet password resetting, the higher level of security achieved with voice verification can enable businesses to offer real-time password resets or reminders. This benefits both customer and business and can reduce up to 70% of helpdesk calls.

It should be noted that some US states have privacy laws that require express consent and special handling capabilities to protect consumer privacy, which impact upon the cost and effectiveness of collecting, using and storing voiceprints, meaning that some businesses may not be able to use voice biometrics.

According to Jenny Neubeck, Director of Remote Services, Affinity Plus was focused on a few major obstacles. Before Pindrop, wait times for members averaged 10 minutes and abandon rates were high, making it difficult to staff properly. Agents were getting burned out and were required to manually authenticate every member calling in, adding an additional burden on the agents' shoulders to identify if the caller was actually a bad actor. Their overall goals were to improve member experience and agent experience by reducing abandon rates, hold times authentication time, and agent stress, all while reducing fraud and overall costs.

By implementing both of Pindrop's Caller Authentication and Anti-Fraud products in their contact center, Affinity Plus saw value for their customers directly after implementation. Spending extra time on the design and plan for the rollout helped tremendously with adoption delivering outstanding results. And they didn't have to do it alone—Neubeck stated, "Pindrop provided additional insights into fraud cases that showcased how the system was working. That assistance and education gave us confidence in the system. We took Pindrop's best practices and then adjusted them based on Affinity Plus' needs."

In addition, Affinity Plus benefited by tracking first-party fraud. This spurred the growth of their fraud management team and Affinity Plus is now investing in new areas of fraud protection after the success they had with Pindrop's solutions.

Average 20%	80	45 seconds	82%
Drop abandon rates	Improved average hold times	Reduction in average handle time	Authentication rate

Their Challenges

Reducing

- Abandon rates
- Hold times
- Time for authentication
- Voice & cross-channel fraud
- Agent stress
- Costs

Improving

- Member experience
- Agent experience

Their Results

- Abandon rates dropped from 25-30% to just 5-10%
- Average hold times improved by 80%
- Average handle times reduced by ~45 sec.
- No need to replace 3 FTE (lost to natural attrition)
- Members reported increase in prompt service satisfaction
- Agent stress levels improved

Future use of voice biometrics

The interest in using voice biometrics for customer authentication is tipped more towards larger operations, which are more likely to have high call volumes, meaning that 40 seconds or more cut from each call would add up to a very considerable saving, without affecting the customer or agent experience negatively.

Finance, medical and TMT respondents were most likely to look favorably on voice biometrics, and although the argument has certainly not yet been won, there has been a significant increase in interest in recent years, especially in large contact centers.

However, 35% of respondents do not yet have a firm view on whether or not voice biometrics is a solution they would even consider implementing.

Inhibitors to voice biometrics

One of the main inhibitors to voice biometrics is the perceived expense of the solution, with around half of respondents stating that this was a very important reason not to implement it. This was particularly the case for both small and medium operations.

Another issue with voice biometrics is the question of low customer adoption. Only around 60% of customers will call into a contact center in a given year and of those, a significant group will be resistant to having a voiceprint created due to privacy concerns or will experience poor call quality. This means that voice biometrics may be applicable to 50% or less of customers and that a majority of customers will never be enrolled, leaving them vulnerable to fraud attacks.

It is still possible to give some protection to these non-calling customers' accounts, as criminals often try to mine the IVR in order to gather and using the stolen information to socially engineer agents and take over accounts across the enterprise. Fraudsters identify and take over legitimate accounts by using automated bots in the IVR to test large numbers of stolen credentials and credit card numbers. Some solutions monitor inbound calls for IVR bot activity, suspicious phone numbers and accounts that have had multiple attempts to be accessed, flagging these accounts as requiring particular attention when a caller then tries to access that account on a call. As every caller exhibits unique behavior patterns when engaging with a call center, by classifying the cadence of each keypress, a pattern can be established for every genuine caller.

In terms of usability, some issues have been reported with callers using speakerphone or cordless phones, leading to false negative responses, which means the caller then has to go through a very long and stringent manual ID&V process, taking far more time than is usually the case for agent-led identification.

Although the reliability of the technology was a concern, almost half of respondents admitted that they did not know enough about this to even form on opinion. Worries about managing the solution were also present in smaller operations and there are concerns over customer sentiment for contact centers in all size bands.

As might be expected, respondents in small contact centers are far more concerned that call volumes are too low to make the solution worthwhile: for large operations, it is not the case that the commercial benefit isn't there, but concerns over the use of the solution and its cost are far more important.

Beyond voice biometrics

Voice biometrics can be a useful tool, especially for larger contact centers through cutting call lengths and costs, and improving customer experience. However, it may not always be enough against a fraudulent attack or series of attacks.

Solutions that focus on identifying potential fraudulent callers don't rely solely on matching the voiceprint, which is not an infallible method of authentication, as can be seen below.

Biometric security fooled by twin's voice

The BBC carried a story[3] about an experiment that a BBC reporter and his twin had tried on a UK bank. The reporter had enrolled in a bank's voice identification system, but his twin was able to access the account after ringing the bank and pretending to be his brother.

The security breach did not allow the twin to withdraw money, but he was given access to some of the account's functionality. The twin took eight attempts to access the account, which is a failing in the implementation process rather than the technology – most typed passwords will allow perhaps three failures before the user is locked out.

Experts stated that although each voice is unique, if the system has been implemented to allow too much leeway when detecting some of the hundreds of characteristics of the voice, then it would not take an exact voiceprint match to access the account.

The expert noted that if the voiceprint was hacked or copied, the genuine account holder would not have the option to change their voice like they would change their password.

Voice replication software was also noted to be becoming increasingly sophisticated, and the general feeling was that alternative methods of security would be required alongside voice biometrics.

[3] http://www.bbc.co.uk/news/technology-39965545

Call signaling analysis & ‘phoneprinting’

An alternative – or rather, additional method of customer identity verification is ‘phoneprinting’ or call signaling analysis, which is perhaps focused more on identifying and preventing fraud than on simply authenticating genuine customers.

Call signaling analysis is the process by which the metadata surrounding a call can be looked at, for the purpose of identifying potentially fraudulent and suspicious calls that can then be handled differently by the business.

The process collects information about the call being made, such as location, the type of phone being used (VoIP is far more likely to be used in fraudulent calls), caller ID, the phone number’s history and the chances it has been ‘spoofed’, levels of voice distortion, etc. These factors can be scored, and after assessing the likelihood of the call being fraudulent will then impact upon the security processes and questions that the agent is required to ask the caller, speeding up the process for genuine callers, and focusing the tightest levels of security on potentially fraudulent calls.

For solution providers who have access to their country’s PSTN, data such as network level caller ID may be collected from the call at carrier-level compared to the presentation caller ID: a mismatch may indicate that the call is suspicious.

Call metadata may include many dozens of individual pieces of data, which are put together to form a phone print:

- presentation caller ID
- network caller ID
- geographic ID
- the type of device being used
- codec artefacts
- packet loss
- clarity.

The solution checks to see if this pattern of metadata has been seen before, and if so which account it is linked to. If it is anything other than the account of the customer that the caller claims to be, it is flagged as a potentially fraudulent interaction. If the phone print is not recognized, it will be stored and used in future interactions.

The caller’s voiceprint and phoneprint can be matched against a database of fraudsters: while this “bad voice” method of matching recorded voice against the database of known fraudsters can be effective, this is usually done as a retrospective batch process so does not work in real-time, although it can be useful to check that requests for new credit cards are authentic before the card itself is sent out. Some fraudsters call in multiple times to find an agent that they can socially engineer. Identifying and logging multiple calls from the same caller/device can identify this and allow agents to be aware and/or block calls.

Call signaling analysis can work in conjunction with voice biometrics to alleviate some of the weaknesses of the latter. By identifying suspicious phone prints, the caller can be identified as being suspicious and handled accordingly:

- IVR spear-phishing: fraudsters use the IVR to validate customer information such as recent transactions, which is then used to conduct fraud through other channels
- Fraudulent voice biometric registration: if the customer has not already registered their voiceprint, a fraudster can do so if they have sufficient static identification information about the customer (e.g. password, date of birth, address, etc.)
- 'Catch and release' fraud: fraudsters contact the bank to clear blocked fraudulent payments that they themselves have made, if they are able to successfully authenticate themselves as the customer
- SIM swap and fraudulent ports: fraudsters gain control of genuine customers' phone numbers in order to bypass two factor authentication (e.g. caller ID and another factor)
- Call signaling analysis can also reduce unnecessary customer callbacks caused by a lack of confidence about the caller ID: in cases where voice biometrics has been uncertain, meta data around the call can be used to provide a more definite answer either way.

Some solutions allow fraudulent phone numbers to be gathered and shared with other businesses, redflagging likely fraudsters. Data from various sources can be added, such as consumer complaint sites, spam calls databases, detecting attack patterns and improving suspicious call identification. Such information can also feed into fraud detection platforms which gather data from many sources often do not include flags from the telephony channel – despite 60% of forthcoming through the phone channel – causing a limited detection of cross-channel attacks.

Some solution providers offer a fraud investigation service for SMEs who may not have the resources to implement the full biometrics or call signaling analysis solution. The solution provider takes the audio recordings identifies the fraudulent activity on an as needed basis.

Sophisticated fraud detection solutions use AI and machine learning to identify fraudulent transactions and also to analyze cases where legitimate users fail the authentication attempt (e.g. due to noise variations, the ageing process, a change in devices, etc.) to amend and optimize the voiceprint so that they are more likely to be identified correctly in future.

To summarize, the strongest security will be present where there is multi-factor authentication around voice biometrics, device authentication, shared information about known fraudsters and customer behavior such as keypress analysis and call patterns.

About contact babel

ContactBabel is the contact center industry expert. If you have a question about how the industry works, or where it's heading, the chances are we have the answer.

We help US and UK contact centers compare themselves to their closest competitors so they can understand what they are doing well, what needs to improve and how they can do this.

The coverage provided by our massive and ongoing primary research projects is matched by our experience analyzing the contact center industry. We understand how technology, people and process best fit together, and how they will work collectively in the future.

If you have a question about the contact center and CX industry, please get in touch.

Email: info@contactbabel.com | Website: www.contactbabel.com | Telephone: +44 (0)1434 682244

Free research reports available from www.contactbabel.com (UK and US versions) include:

The Inner Circle Guide to Agent Engagement & Empowerment
The Inner Circle Guide to AI, Chatbots & Machine Learning
The Inner Circle Guide to AI-Enabled Self-Service
The Inner Circle Guide to Cloud-based Contact Center Solutions
The Inner Circle Guide to Contact Center Remote Working Solutions
The Inner Circle Guide to Customer Engagement & Personalization
The Inner Circle Guide to Customer Interaction Analytics
The Inner Circle Guide to Fraud Reduction & PCI Compliance
The Inner Circle Guide to Omnichannel
The Inner Circle Guide to Omnichannel Workforce Optimization
The Inner Circle Guide to Outbound & Call Blending
The Inner Circle Guide to Video & Next-Generation Customer Contact
The Inner Circle Guide to the Voice of the Customer
The European Contact Center Decision-Makers' Guide
The UK Contact Centre Decision-Makers' Guide
The US Contact Center Decision-Makers' Guide
The UK Customer Experience Decision-Makers' Guide
The US Customer Experience Decision-Makers' Guide
UK Contact Centre Verticals: Communications; Finance; Insurance; Outsourcing; Retail & Distribution; Utilities
US Contact Center Verticals: Communications; Finance; Healthcare; Insurance; Outsourcing; Retail & Distribution.

To download the full "2023 US Contact Center Decision-Makers' Guide" for free, please click here.