Aite PARTNER. ADVISOR. CATALYST.

Contact Center Authentication: A Mystery Shopper's Journey

MAY 2021

Shirley Inscoe

PREPARED FOR

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

IMPACT POINTS

- This Impact Report, sponsored by Pindrop, details the results of mystery calls made to a number of financial institutions' (FIs') contact centers to understand the customer journey and the authentication measures in place at each one. It also examines whether the mystery caller was able to achieve the goal of the call and how the caller felt after the call was completed.
- Methods used to authenticate callers in contact centers can make or break the customer experience—and the way customers view an FI.
- Outdated authentication methods such as knowledge-based authentication (KBA) questions—a method that has been used in many contact centers for decades—are often defeated by fraudsters.
- Every FI must devise an authentication strategy for its contact centers that balances the FI's risk tolerance with the customer experience. If the risk threshold is too high, fraud losses will rise, but if the customer experience is poor, profits and reputations will suffer.
- Forty-seven percent of U.S. adults have been victims of some type of application fraud or account takeover in the past two years; more reliable authentication is sorely needed to halt this tsunami of identity crimes.
- Multifactor authentication is imperative—there are no silver bullets, and multiple methods must be used to authenticate callers reliably.
- Long wait times were the primary complaint of mystery shoppers, followed by interactive voice response units (IVRs) that make it difficult to reach an agent even though the IVR does not provide the service needed.
- Personalized service from a representative who seems to really want to assist a caller can overcome other deficits (such as IVR navigation difficulties) when it comes to overall customer satisfaction.
- Consistently reliable authentication methods can enable an FI to offer more products and services through contact centers and through self-service IVRs, increasing the value of this delivery channel.
- A wide variety of contact center solutions can enable an FI to devise a strategy to authenticate callers without introducing unnecessary friction. More than one technology solution may be required to manage contact center authentication needs due to fraudsters' use of so many different attack methods.
- FIs and core processors (which provide contact center services to their FI customers) must review current contact center authentication processes for effectiveness and update them if they are not resulting in reduced fraud losses, improved customer experiences, and increased operational efficiency.

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

INTRODUCTION

When a customer calls into an FI's contact center, it is because he or she has a specific need for information or for a specific action to be taken (e.g., a travel alert added to a card or funds to be moved). From the caller's perspective, it is important that their particular need be met as quickly as possible. Life moves quickly, and no one wants to waste time on the phone with their FI longer than necessary. The COVID-19 pandemic created a lot of turmoil in contact centers. Many changes were required for agents to be able to work from home; incoming call volume soared due to branch closures, increased cardholder disputes, and confusion over governmental program benefits; and wait times became extremely long. Now that the world is gradually returning to a new normal, it is important for contact centers to be able to provide timely, excellent customer service.

This Impact Report is based on mystery shopping calls made to various financial services firms' contact centers; the report documents the results of the calls. The learnings are plentiful and demonstrate the good, the bad, and the ugly with regard to results. Contact centers represent a delivery channel that is quite unique. Many customer needs can be met via self-service through IVR units, and contact center management's goal is often to contain as high a percentage of calls in the IVR as possible to reduce operating costs. However, many calls require interaction with an agent; the transition from IVR to agent can be seamless or horrendous. In many cases, callers have to start the authentication process all over again when they speak with an agent. Financial services firms have been focused on improving the customer experience in recent years, but some have apparently overlooked customer service in their contact centers. Contact center management, fraud executives, authentication managers, and customer experience directors should all find this report to be informative and useful.

METHODOLOGY

This report, sponsored by Pindrop, is based on the results of nine mystery shopping calls made to FI contact centers for two specific use cases. Calls were conducted and results documented by Aite Group analysts. In addition, telephone interviews were conducted with fraud executives at one FI that provided a great customer experience, and with an executive responsible for fraud solutions to support contact centers at a large core processor.

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

THE MARKET

Contact centers have been an integral delivery channel for years, but the COVID-19 pandemic in 2020 elevated the need for strong customer service in contact centers due to widespread branch closures and reduced branch operating hours for many months. Incoming contact center calls were elevated in many cases by 40% or more.[1] Customers who typically bank in person at their local branch were calling in droves. With FIs scrambling to set up agents with the ability to work from home and many offshore contact centers offline entirely for weeks, call waiting times lengthened dramatically. Many consumers adopted online or mobile banking for the first time, but contact centers continue to be the delivery channel of choice for others. Since contact centers are a critical delivery channel, better authentication methods must be devised to improve the customer experience and reduce the rise of identity crimes such as account takeover fraud (Table A).

Table A: The Market

Market trends	Market implications
Call waiting times increased dramatically during 2020 when branch closures caused many customers to turn to this channel.	While many branches have reopened (other than those permanently shuttered), some FIs are still struggling with answering incoming calls within a reasonable time period.
Fraudsters often use the contact center to enable cross-channel fraud.	Unreliable contact center authentication is defeated by fraudsters who may then have online credentials reset, order an additional card on an account, place a check order, or take other steps that lead to fraud.
Many authentication technologies that can help authenticate callers more reliably with less friction have been developed.	The largest FIs and some core processors are investing in new technologies that will improve customer service while reducing both fraud losses and operational expenses.
Some financial services firms are realizing advantages over their competition via contact centers if they invest in low-friction, reliable authentication measures.	Competitive advantages can be created by offering more self-service options in the IVR and more products and services through contact centers once reliable authentication measures are in place.

Source: Aite Group

1. See Aite Group's report *Workplace Distancing: Adapting Fraud and AML Operations to COVID-19*, April 2020.

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

IMPORTANCE OF RELIABLE AUTHENTICATION

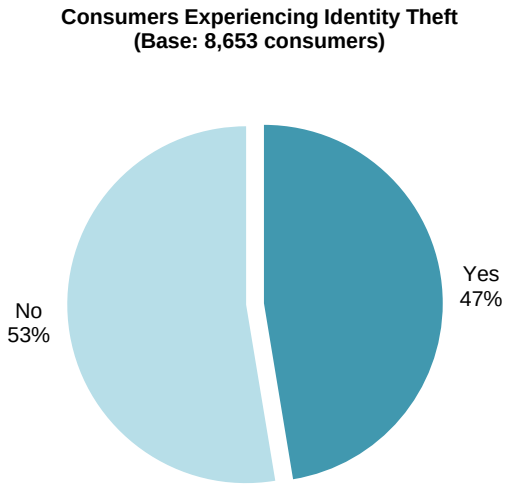
Contact centers represent a channel in which fraudsters have historically used information from data breaches, information from malware installed on devices, and social engineering tactics to take over existing customer accounts. Just a brief decade ago, the vast majority of contact centers used KBA questions as the primary tool to authenticate incoming callers. Many also used ANI validation to connect the incoming call to a customer or account record to streamline the call process and as a secondary authenticator. Fraudsters who had some knowledge about the customer and/or their accounts often called repeatedly until they were able to gain enough information to respond correctly to KBA questions, then spoofed the customer's phone number so the incoming call appeared to be legitimate. Account takeover rates rose dramatically as fraudsters focused on the contact center to steal funds. Indeed, in the past two years, 38% of U.S. adult consumers experienced some type of account takeover fraud,[2] some portion of which was enabled through contact center activity.

In the past two years, 47% of U.S. adults have been victims of some form of identity theft through application fraud or account takeover (Figure 1), and this fraud trend has really gained the attention of regulators. Contacts centers represent an undetermined subset of that fraud activity. FIs offer different products and services through their contact centers dependent on their desire to make the delivery channel similar to other delivery channels and the level of risk they are willing to assume. Some FIs open new accounts through contact centers; it is equally important to prove the identity of applicants calling in as to authenticate returning customers due to the growth of application fraud using stolen and synthetic identities. Not only does the FI run the risk of fraud losses due to application fraud, but it can also open itself to regulatory and reputation risk by not complying with requirements of the Know Your Customer (KYC) aspect of the Bank Secrecy Act. As a delivery channel, contact centers must have the ability to properly identify who is calling.

2. See Aite Group's report *U.S. Identity Theft: The Stark Reality*, March 2021.

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

Figure 1: Identity Theft Victims in the U.S. in the Past Two Years



Source: Aite Group's online survey of 8,653 U.S. consumers, December 2020

If FIs don't take action to better authenticate both applicants and returning customers in their interactions, regulators may start imposing more fines and sanctions for noncompliance with KYC requirements. If they are not satisfied with the progress made, they can seek additional legislation, further increasing the regulatory burden on the industry. The industry must police itself or accept the inevitable increase in regulatory requirements.

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

MYSTERY SHOPPING FI CONTACT CENTERS

Mystery shopping is a tool often used by companies to ensure customers are being treated fairly and well. Mystery shoppers attempt to conduct various types of transactions, then observe and report on the results of the interaction.

To understand current authentication processes in financial services firms' contact centers, mystery shopping calls were conducted for two specific use cases. Mystery shoppers documented the results of each call, including how they felt at the conclusion of the call based on the experience, whether they were able to accomplish the purpose of the call, and the treatment they received.

MYSTERY SHOPPING RESULTS—MONEY MOVEMENT

The first use case tested by mystery shoppers was deliberately a relatively high-risk scenario to determine the types of authentication performed. The mystery shopper was trying to move US$500 from their account at one FI to their account at another FI. This is a use case that was offered in the past by many FIs, so it seemed to be a good use case for this purpose. The results of the mystery shopping calls are shown in Table B.

Table B: Money Movement Use Case

Mystery call to:	FI size	Authentication measures used	Length of call	Purpose of call accomplished	Result of call
FI A	Top 10 bank	Demand deposit account number, ATM PIN	13 minutes (included voice enrollment)	No	Surprised customer, very dissatisfied
FI B	Top 10 bank	Last 4 digits of Social Security number (SSN) or of debit card number	10 minutes	No	The high level of personalized service made this call very positive despite not being able to move funds as desired
FI C	Top 10 bank	Full SSN, ATM PIN, and date of birth	19 minutes	No	Very dissatisfied customer, due to excessive hold time and duplicative processes

Source: Aite Group

ADDITIONAL DETAILS OF CALLS

These mystery shopping calls made it clear that the inability to perform a simple task—transferring money from a customer's account at their FI to their account at another

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

FI—has apparently been discontinued by many firms due to the inability to control fraud (i.e., the inability to consistently and reliably authenticate a caller). When a fraudster successfully impersonates a customer and moves funds out of the account, a fraud loss often results unless authentication is reliably performed. FIs cannot afford to offer products and services via the contact center without consistently reliable authentication processes in place.

- FI A has a circular IVR problem. The caller was repeatedly shuffled through the same IVR module over and over, trying her best to get out of IVR hell. The mystery shopper was sorely tempted to hang up; in all, she spent 11 minutes in the IVR (although in fairness, part of that time was waiting on an available agent). Before the caller realized what was happening, she was informed she was eligible to be registered for Voice Verified, was transferred, and was told to repeat a specific phrase (two sentences) three times. She was told her voice would be used to verify her identity on future calls. After this process, the caller cannot recall being offered the opportunity to opt out and thinks she would have had to hang up and call again if she refused to register her voice. After enrollment, she was transferred to an agent who explained that she could not assist with moving funds out of the bank to another FI. She was instructed to go to online banking, register the account at the other bank, and go through a trial deposits process. After completing that process, she would be able to move the funds. The mystery caller asked whether, subsequent to successfully completing the trial deposits process, she would be able to call and move funds. She was told absolutely not; she would have to use online banking to do so. Since this is a service that her bank used to offer, the caller was not happy she could not accomplish her goal of moving the funds. In this scenario, if she wanted to move funds between the accounts anytime soon, she would have to write a check, drive to the ATM, and deposit the check to her account at the other FI. Doing so, funds would be available the following day—but what an inconvenience! Lastly, the agent clearly didn't want to assist the mystery shopper, showed absolutely no friendliness or empathy, and provided no apology for the long wait time. It felt as though she couldn't wait to shuttle the caller off to online banking permanently.

- FI B seemingly has a highly integrated contact center wherein the incoming call is identified and transferred to wealth management for those customers who also have that relationship with the firm. The mystery caller called the normal bank customer service number, entered the last four digits of her SSN, then was transferred and asked to hold for the next representative. After holding for less than a minute, the caller was greeted by name by a wealth management officer. The caller had a pleasant conversation with the officer, and even though the transfer could not be done, she was given options on how to move the funds between banks. The options provided were via online banking or via a wire transfer. The lack of hold time and personalized service made a tremendous difference in the caller's satisfaction level after the call concluded.

- FI C has a high call volume or too few agents since wait times are long. The mystery caller explained that he wanted to move funds from his account to an account at a different FI. After having waited 10 minutes to speak with an agent, he was told he could do that through the online contact center and was transferred. After

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

navigating through one IVR, he was transferred to another IVR, where he had to input all the same information he keyed in the first IVR. In the online contact center IVR, he had to hold for seven more minutes until speaking with an agent. The end result was being told they could not do the transfer at all. This mystery caller went through two IVRs, keyed all the authentication data required in both, talked to two agents, and was on the phone a total of 19 minutes, only to be told his transfer could not be made. He was upset due to the long hold times and the duplication, and he wondered why the first agent he spoke with gave him the incorrect information that his transfer would be completed in the other contact center. Would any customer want to receive treatment such as this?

There are many reasons a consumer may have multiple banking accounts and need to transfer funds from one account to another. This simple use case has been discontinued by many FIs, even though it is a service many consumers need. Having the ability to consistently authenticate callers and identify a potential fraudster can enable FIs to offer more products and services either through the IVR or through contact center agents.

MYSTERY SHOPPING RESULTS—TRAVEL ALERTS

The second use case that was tested by mystery shoppers was to place a travel alert on a debit or credit card. Travel alerts make a card issuer aware that the customer is in a different geography than normal so that (hopefully) transactions will not be declined in error when the customer is travelling.

The results of mystery shopping calls to place travel alerts are shown in Table C.

Table C: Travel Alert Use Case

Mystery call to:	FI size	Authentication measures used	Total length of call	Purpose of call accomplished	Result of call
FI A	Top 10 issuer	Last 4 digits of card, date of birth	3 minutes	Yes	Happy customer
FI B	Top 10 issuer	Last 4 digits of SSN, telephone number	7 minutes	Yes	Very annoyed customer—card to back of wallet
FI C	Top 10 issuer	Voice verified (repeat 2 specific sentences)	4 minutes	Yes	IVR was irritating, but agent quickly placed travel alert
FI D	Top 10 issuer	Enter last 4 digits of SSN or enter account number	2 minutes	No—told in IVR that travel alerts are no longer required	Skeptical/ concerned that transactions may be turned down

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

Mystery call to:	FI size	Authentication measures used	Total length of call	Purpose of call accomplished	Result of call
FI E	Top 75 credit union	Asked 5 KBAs—questions were based on transactional activity client had with FI	13.5 minutes	Yes	Long hold time was frustrating—process with agent was pleasant and efficient
FI F	Top 20 issuer	Account number, last 4 digits of SSN, ZIP code, and date of birth	23 minutes	Yes, but agent stressed transactions may still be declined	Length of call was very frustrating—customer was uncertain if transactions will be approved

Source: Aite Group

ADDITIONAL DETAILS OF CALLS

Additional important details of each call are as follows:

- FI A enabled the caller to quickly and easily identify herself. While all the authentication measures operating in the background are unknown, keying two short items into the telephone enabled the IVR to begin asking what the mystery shopper needed. Very importantly, the shopper was easily able to leave the IVR and speak to an agent, as desired. Knowing the customer had been authenticated in the IVR, the agent processed the travel alert request, and the call was ended quickly. On this call, the mystery shopper was able to accomplish what was desired quickly and easily, which is every caller's goal.
- FI B made it very difficult to exit the IVR, although it did not offer the ability to place a travel alert in the IVR. Almost four minutes elapsed while the mystery shopper attempted to find the correct sequence in the IVR to place an alert or speak to an agent. Two obvious authentication measures used were the last four digits of the SSN and the phone number (i.e., Is the number you are calling from associated with your account?). This card actually went to back of wallet due to the difficulty of adding a travel alert, and the mystery shopper made a mental note not to use it when travelling in the future. Once the call was transferred to an agent, the travel alert was placed fairly quickly, but the call lasted a total of seven minutes.
- FI C had the mystery shopper repeat two sentences to authenticate; no additional means of authentication were requested. (This is FI A from Table C.) This FI's IVR is difficult to exit and reach an agent, but the agent quickly placed the alert once the mystery shopper was able to make the request.
- FI D provided the briefest call time at only two minutes. The IVR was used, and the mystery shopper was told that travel alerts are no longer required. This concerned the shopper because she was afraid her transactions might be declined, but no

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

transactions were declined throughout the travel period even though the card was used often. Overall, this was a great contact center experience, but concerns remain that the card may be declined during future travel.

- FI E was the only mystery shopping call in which KBA was used as part of the authentication process. A total of five questions were asked, but the mystery shopper commented that the questions were quite good compared to some she has been asked in the past since they were based on the FI's transactional experience with the client, rather than credit bureau or demographic data. The primary complaint regarding this mystery shopping call was the long hold time (13.5 minutes) before being able to speak with an agent.
- FI F holds the record for the worst mystery shopping caller experience; the call lasted a total of 23 minutes, 19 of which were spent navigating the IVR and waiting to speak with an agent. While such long hold times were very rare prior to the COVID-19 pandemic, they became the norm when many FIs closed branches and call volume skyrocketed. (Actually, during the pandemic, some FIs had much longer average hold times than this call.) Some FIs still have not recovered to pre-pandemic wait times. Perhaps the worst thing about this experience is that the mystery shopper was told a note would be placed on the file regarding his upcoming travel, but suspicious transactions would still be denied during the travel period. This left the mystery shopper uncertain whether he had accomplished anything by placing the travel alert and enduring the long wait time.

MYSTERY SHOPPING RESULTS SUMMARY

Several key learnings can be gleaned from the combined results of these mystery shopping calls:

- There is little consistency from one FI to another concerning how they authenticate callers to contact centers.
- Only one FI used KBA questions—the trend to decrease or eliminate the use of KBA is very strong across large financial services firms. It is possible some of these firms still use KBAs for other use cases.
- No FI used one-time passwords (OTPs), which is surprising. OTPs are used more commonly in digital channels, but there have been recent fraud rings with schemes that defeated OTPs. Either contact centers reserve the use of OTPs for high-risk activity or FIs are moving away from using OTPs for authentication.
- Long wait times tend to make callers dissatisfied with the contact center experience, even if they are able to accomplish the purpose of their call. IVRs that are difficult to navigate and exit to talk with an agent also irritate callers. If a product or service is not offered in the IVR, it should be easy to transfer to an agent for assistance.
- The courtesy and sincere desire of a representative to assist a caller can override other negative aspects of a contact center call (such as an irritating IVR).

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

- Some FIs require a great deal of data to be entered to authenticate callers. With many callers using small mobile devices, it can be difficult to enter lengthy account numbers or other data without making an error. While not documented above, several mystery calls had to be abandoned and started over due to making keying errors when entering up to 16-digit-long account numbers on a tiny smartphone keyboard. This type of keying error, hanging up, and calling back, can increase an FI's incoming call volume, even though no one is benefitting, and can also be very frustrating for callers.
- Sharing the results of authentication in the IVR with the agent improves the customer experience; a continuous authentication process in which the authentication results (and risk score, if available) from the IVR is passed to the agent prevents the customer from having to duplicate authentication steps already performed and enables the agent to more quickly meet the caller's need or perform additional authentication steps, as necessary.

AUTHENTICATION BEHIND BEST MYSTERY CALL EXPERIENCE

Two fraud executives who partner with contact center management to combat fraud and ensure sound authentication is in place were interviewed to determine what types of solutions are used in their contact centers that provided the best customer experience for mystery shoppers. A number of solutions are in place from three vendors. The authentication strategy is currently being reviewed and upgraded; the rollout of enrolling customers for voice recognition is part of the strategy. In addition, the FI is evaluating implementing additional aspects of the solution used from another provider that will enable them to capture more details of suspicious incoming calls to share with the fraud department.

Current tests that incoming calls are subjected to include the following:

- Device recognition—verifying that the device the call originated from is the same device that has been previously associated with the customer
- Spoofing detection—determining that the call is not actually coming from the number it appears to be coming from; fraudsters routinely spoof customer numbers to give contact centers agents a false belief that they are talking to their customer
- Analyzing various aspects of information about each incoming call to determine a risk score for each one
- Transferring the results of risk scoring to the agent who will either know the caller has been authenticated or knows stepped-up authentication processes must be used (multifactor authentication)
- Multifactor authentication is required for all risky interactions—meeting at least two of the three requirements, which are something you know (e.g., PIN, password), something you have (e.g., device, token), and something you are (e.g., biometric)

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

- Enrolling fully authenticated customers to use voice recognition on future calls (other viable alternatives include using phone recordings to create voiceprints and creating a hot file of known fraudster voiceprints to screen incoming calls)
- Testing that the customer's phone number is actually in an active session with the contact center telephone number
- Mobile network operator (MNO) data—determining whether the mobile number has been ported or forwarded and whether the SIM card has been switched out recently

New functionality that is being evaluated and may be added includes analytics focusing on IVR activity, risk scoring in the IVR, and using a case manager that can enable the fraud department to view details of each suspicious call. In 2021, the FI will implement machine learning models that will improve account takeover detection over time based on feedback.

These executives also shared that prior to the implementation of voice recognition, contact center agents used more KBA questions and OTPs; they have dramatically scaled back the use of both of these authentication techniques but have not totally eliminated either of them.

Another executive from this FI stated that he doesn't foresee the firm ever using fewer than three technology solution providers in the contact center for fraud because what each of them provides is totally different. While large financial services firms can afford to use multiple technologies, smaller FIs often cannot. The good news is that core processors, which handle contact center solutions for many small and midsize FIs, are also evaluating the authentication solutions their client FIs have access to, and plan to broaden the range of solutions offered.

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

CONTACT CENTER AUTHENTICATION TOOLS

There are many tools and technologies available to help detect and defeat fraud attempted in contact centers. As all fraud executives know, there are no silver bullets, and using layers of protection is always important. Each FI should determine which tools will be most beneficial in its environment, based on the level of risk the institution is willing to accept and the customer experience it wants to provide. Some technology providers offer multiple solutions, enabling an FI to minimize the number of vendors that must be managed; this is a big consideration since vendor management can be time consuming. Achieving the desired balance between security and customer experience can be challenging but will provide optimal results when accomplished.

Regardless of which authentication measures an FI chooses to use, it is important to implement risk-based authentication to further improve the customer experience. Of course, this is particularly important if the FI uses solutions that impose friction during the customer interaction. Callers who have a simple question (e.g., the amount of a particular fee) need little authentication, but those requesting high-risk activities (e.g., changing contact information for an account) require authentication commensurate to the level of risk involved. The risk of each authentication can be tailored to match the level of risk of the caller's request as opposed to treating every customer interaction as high risk, and subjecting all callers to friction that may serve no purpose.

KBA

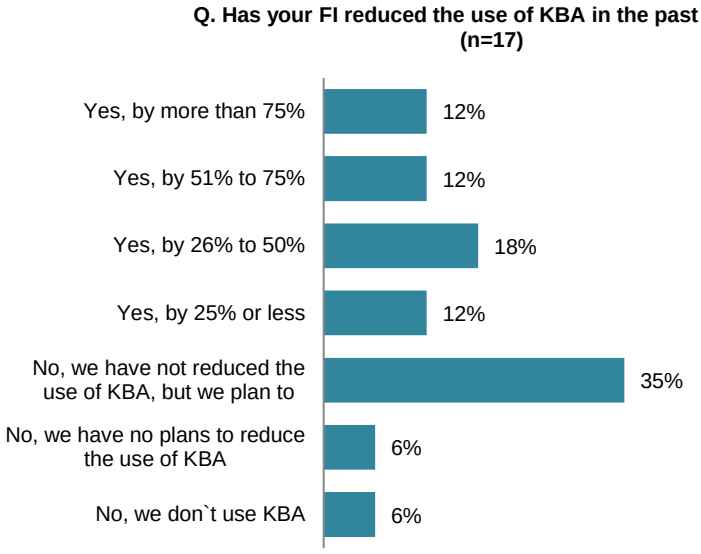
KBA questions are used to ask a caller about things other people typically wouldn't know; the questions asked typically fall into two categories. Credit-based questions are often asked based on data from credit bureaus. For example, how much is an auto loan payment, or which FI (out of a list of four) does the caller have an account with? Demographic-based questions may ask the caller on which street out of a list of four they previously lived or other information about their past or present life. Some FIs ask a mixture of credit and demographic-based questions or rely on internal data to ask about recent activity on the customer's account(s). Fraudsters will often obtain a copy of the credit bureau reports for customers they plan to try to impersonate; they also may look for information about the customers on social media websites, use information accumulated from data breaches, buy data off the dark web, etc., in order to be able to answer KBAs. The use of KBA is decreasing in recent years in many financial services firms[3] because the questions are so easily defeated by dedicated fraudsters; 54% of FIs have decreased usage to varying degrees (Figure 2). In addition, the National Institute of Standards and Technology (NIST) has stated that KBAs can no longer be used as a means of authentication for governmental agencies;[4] many FI executives follow NIST guidelines closely and view them as global best practices.

3. See Aite Group's report *Revisiting Your Authentication Control Framework*, December 2020.

4. "NIST Special Publication 800-63: Digital Identity Guidelines Frequently Asked Questions," NIST, July 5, 2020, accessed May 5, 2021, https://pages.nist.gov/800-63-FAQ/#q-3.

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

Figure 2: FI Use of KBA Is Diminishing



Source: Aite Group interviews with 20 fraud executives from 18 large North American FIs, July to October 2019

ANI VALIDATION

Many contact centers use systems that can capture the incoming telephone number and match it to a customer's existing account; using this type of technology can help shorten the length of a call by associating the caller with their account(s) more quickly. Like KBAs, ANI matching has been used for decades in contact centers, and the technology can be a very useful tool. One of the challenges of using ANI matching as an authentication factor is that fraudsters may be able to pass call center authentication by spoofing the telephone number when spoof detection technology is not in place.

ANI validation systems, on the other hand, assess the carrier metadata associated with the incoming telephone number to evaluate whether the call is coming from the physical device that owns the number. Combining ANI validation with ANI matching can be a very useful tool to authenticate callers for more self-service in the IVR and to reduce reliance on KBAs, without compromising operational security. Fraudsters' more sophisticated attacks can be avoided by combining ANI validation with other authentication tools, such as biometrics and behavior, for further validation.

SPOOFING DETECTION

If a contact center relies on ANI matching at all for authentication, spoofing detection is essential. While there are some legitimate uses for spoofed telephone numbers, spoofing can be an indicator of fraud. Fraudsters often spoof the telephone number of the legitimate customer, giving the contact center agent a false sense of security. Knowing that the real caller is located in eastern Europe, Russia, or another geography where high rates of fraud originate can help avoid allowing a fraudster to pass for a legitimate customer.

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

DEVICE RECOGNITION

Device recognition is often used to verify a particular device that a customer has used previously; while this doesn't guarantee that the legitimate customer is using his or her device to call the contact center, it can help eliminate many types of fraud (other than family or friendly fraud). Knowing that a device has been used previously by a customer can answer the requirement of "something the person has" in multifactor authentication.

VOICE BIOMETRICS

Voice solutions may use random language or a set phrase to create a voiceprint used to identify a consumer's voice. While actively enrolling a customer by having him repeat the same phrase three times may enable slightly faster recognition of a caller's voice going forward, it introduces a lot more friction into the process. Passive enrollment using telephone recordings of customer voices doesn't inconvenience the customer at all, but a customer should be notified if a biometric will be used. (Some FIs amend their contact center recordings to notify callers that recorded calls may be used for future fraud prevention to achieve this goal.)

Some technology solutions also enable the creation of a hot file of known fraudster voiceprints. Since fraudsters often call repetitively, and may impersonate a number of existing customers or complete applications for a number of identities, a hot file can add a great deal of value in identifying high-risk incoming calls. Sharing known fraudster voices via a consortium of FIs can create additional value.

Before implementing, it is important to understand the compliance aspect of any type of physical biometrics, as well as to monitor future governmental regulations[5] with which an FI must comply.

BEHAVIORAL BIOMETRICS

Some solutions use behavioral biometrics to identify returning customers (or fraudsters or even bots that are harvesting data in the IVR.) One aspect of behavioral biometrics is the way a caller handles the mobile device itself (e.g., the pressure exerted in pushing keys, whether a caller is right- or left-handed, and many other unique data points related to behavior). Combining many diverse factors can help identify consumers' reliably over time. Using this technique at the beginning of a call can be helpful, but continuous monitoring throughout the session can ensure that someone else hasn't taken over the call.

5. See Aite Group's report *Improved Customer Experience, Reduced Fraud and Cost: Contact Center Solutions*, December 2020.

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

BEHAVIORAL ANALYTICS

Some solutions analyze consumer transaction and activity patterns—for example, many customers tend to call contact centers on the same day of the week or date of the month, at similar times of day, and conduct similar activities on each call. That is one component of behavioral biometrics, but there are many others. Identifying anomalous transactional patterns (compared to the customer's historical activity) can be helpful in identifying fraud attempts.

MNO DATA

MNO data can include several tests to detect whether fraud may be in process. These tests may include detecting SIM swaps, detecting forwarded or ported telephone numbers, and determining that an actual telephone number is connected to the contact center on a live call.

MNO data can help detect instances when the customer may have lost control of his or her device. While the tests above are not always indicative of fraud, they are important data points to use in conjunction with other information as part of the authentication process. In fighting fraud, time is vital, and unfortunately, some carriers don't update this information as quickly as would be desirable.

ONE-TIME PASSWORD

Many FIs use OTPs as part of their authentication process, so it was surprising that no OTPs were used in any of the FIs contacted by mystery shoppers. In 2020, there were organized fraud rings running schemes designed to defeat OTPs; while some of the schemes were labor intensive, many FIs were impacted. One such scheme targeted customers with large balances, so some large fraud losses were experienced. This particular scheme entailed a fraudster calling a customer, claiming to work for their FI. Unknown to the customer, the fraudster had already taken over the customer's account and entered a transaction to move funds. The fraudster who purported to work for the FI told the customer that there was a problem with which he needed the customer's assistance to make sure everything was straightened out and working properly. He stated the bank would send an OTP, and he needed the customer to provide it to him when it was received. The FI sent the OTP (which was intended to verify that the customer initiated the suspicious transaction), and as instructed, the customer gave the OTP to the caller/fraudster. The fraudster provided the OTP back to the FI, and the fraudulent transaction was executed based on the FI's belief that their customer had authorized it. To make a long story short, fraudsters are very creative and will do whatever it takes for their schemes to succeed. This is just one example of OTP's vulnerability. The use of OTPs in FIs' contact centers is currently not as widespread as in the online and mobile delivery channels,[6] but that could change.

6. See Aite Group's report *Market Trends in Digital Fraud Mitigation*, December 2019.

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

INCOMING TELEPHONE NUMBER TESTS

An FI can perform some relatively simple tests related to the incoming telephone number that can be helpful in combating fraud in contact centers. After capturing the real telephone number the call is originating from (not the spoofed number, which can change from call to call), the FI can perform tests such as velocity tests to detect when the same number is calling repetitively and detecting instances when the same number is calling about multiple accounts that belong to different customers.

Tests such as these are red flags that indicate potential fraud; these situations should be evaluated carefully before providing data or taking actions the caller requests.

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

RECOMMENDATIONS

Every FI must balance risk and customer service; achieving that balance in contact centers is the goal, but it is not always easy to do. Here are recommendations to consider:

- A caller's first impression of your firm may be your IVR. Ensure the IVR is simple to use, and if the service the caller needs is not offered in the IVR, make it easy for the caller to reach an agent. While IVR containment reduces operational expense, that should not happen at the expense of the customer experience.
- Callers would like simple and quick authentication to occur so they can get to the purpose of their call. Introducing too much friction can cause a bad customer experience and lengthen the call, thereby providing poor customer service, as well as increasing operational expense (through lengthy call times).
- Find the right balance between the level of risk the firm is willing to take and the customer experience you want to offer callers.
- Use friction-free authenticators as much as possible to reduce friction for callers while still minimizing fraud risk. For example, no caller will know you are using spoofing detection, but it can be a powerful tool in detecting fraudulent calls.
- There are no silver bullets in fighting fraud; no one factor will provide full protection against all types of fraud. Using multifactor authentication is imperative.
- Analyze the authentication measures currently in place to determine whether they are working well. Analyze how fraudsters are defeating current authentication methods and what can be done to fill coverage gaps.
- Don't hesitate to replace or reduce the use of outdated authentication methods (e.g., KBA) that fraudsters routinely defeat. There are many options for upgrading authentication.
- If you don't have reliable authentication measures currently in place, consider solution providers that offer a variety of tools instead of point solutions that only do one thing; this can reduce vendor management expense and enable later implementation of additional authentication measures from one provider.
- If you decide to use voice biometrics, be sure to monitor and comply with governmental regulations to avoid regulatory fines and penalties.
- While many small and midsize FIs cannot afford multiple authentication solutions in the contact center, they can influence the solutions provided by their core processor. If enough customers request a new authentication solution, core processors will be incented to develop the capability or partner with another firm to provide it.

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

RELATED AITE GROUP RESEARCH

U.S. Identity Theft: The Stark Reality, March 2021.

Revisiting Your Authentication Control Framework, December 2020.

Improved Customer Experience, Reduced Fraud and Cost: Contact Center Solutions, December 2020.

Beating the Bad Guys: Safe and Secure Voice Interactions in the IVR, November 2020.

Workplace Distancing: Adapting Fraud and AML Operations to COVID-19, April 2020.

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

ABOUT PINDROP

Pindrop solutions are leading the way to the future of voice by establishing the standard for security, identity, and trust for every voice interaction. Pindrop solutions protect some of the biggest banks, insurers, and retailers in the world using patented technology that extracts intelligence from every call encountered. Pindrop solutions help detect fraudsters and authenticate callers, reducing fraud and operational costs, while improving customer experience and protecting brand reputation. Pindrop Security, Inc., a privately held company, headquartered in Atlanta, GA, was founded in 2011 by Dr. Vijay Balasubramaniyan, Dr. Paul Judge and Dr. Mustaque Ahamad. Pindrop is venture-backed by Andreessen Horowitz, Citi Ventures, Felicis Ventures, CapitalG, GV, IVP and Vitruvian Partners. For more information, please visit pindrop.com.

PINDROP PASSPORT

Pindrop's Passport solution is a multifactor authentication solution that reduces friction for genuine callers by providing passive authentication prior to connection with call center agents, thus significantly reducing average handle times, decreasing costs, enhancing self-service, and hardening vulnerable call centers by eliminating absolute dependence on knowledge-based authentication.

PINDROP PROTECT

Pindrop's Protect solution is a multifactor anti-fraud detection solution that helps fraud teams to stop fraud in real-time, predict future fraudulent activity, reduce fraud-related costs, improve efficiency and review rates, and defend the contact center from attack. Unlike other solutions, the Protect solution works from IVR to agent, identifying which calls are risky and which accounts are likely to be attacked as well as which adjacent channels are vulnerable to fraud.

ABOUT NEXT CALLER

Next Caller, a Pindrop® Company, provides enterprise-grade ANI validation, call verification, and spoof detection technology for contact centers. Next Caller's primary service, VeriCall®, uses machine learning to analyze the metadata of an incoming call, then deliver a risk score to the IVR in under 300 milliseconds. The technology enables businesses to personalize the customer experience, encourage self-service, and reduce reliance on frustrating and time-consuming authentication methods like knowledge-based questions and one-time passcodes for over 75% of all calls. VeriCall® technology also detects call spoofing and other forms of call manipulation to protect against phone fraud. Over 2 billion calls have been analyzed for clients across industries, including financial services, insurance, healthcare, and telecommunications.

CONTACT

For more information, please contact Pindrop: pindrop.com | pindrop.com | info@pindrop.com

Twitter | Facebook | LinkedIn

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

ABOUT AITE GROUP

Aite Group is a global research and advisory firm delivering comprehensive, actionable advice on business, technology, and regulatory issues and their impact on the financial services industry. With expertise in banking, payments, insurance, wealth management, and the capital markets, we guide financial institutions, technology providers, and consulting firms worldwide. We partner with our clients, revealing their blind spots and delivering insights to make their businesses smarter and stronger. Visit us on the web and connect with us on Twitter and LinkedIn.

AUTHOR INFORMATION

Shirley Inscoe
+1.617.398.5050
sinscoe@aitegroup.com

CONTACT

For more information on research and consulting services, please contact:

Aite Group Sales
+1.617.338.6050
sales@aitegroup.com

For all press and conference inquiries, please contact:

Aite Group PR
+1.617.398.5048
pr@aitegroup.com

For all other inquiries, please contact:

info@aitegroup.com

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com