The Case for Better Self-Service: Improving customer workflows and preventing fraud around the IVR

by Shawn Hall, VP, Pindrop

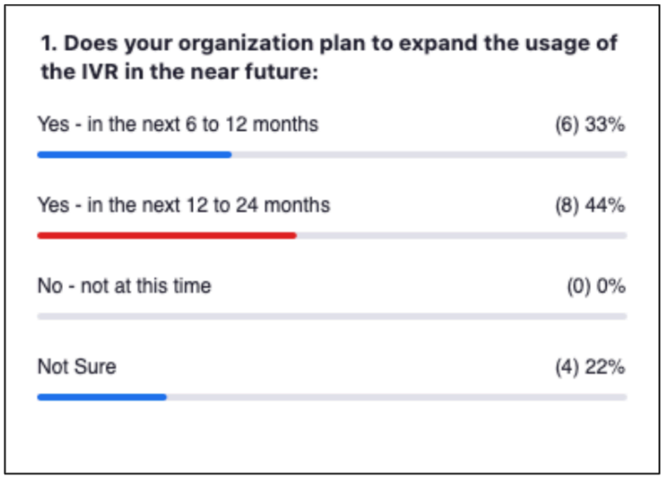
Creating the right strategy to handle fluctuating customer call volumes is an evolving process, and one that has likely been altered by the events from 2020.

Increased security concerns[1], variable call volumes and employee health all need to be considered as companies set new initiatives and make plans to achieve their goals, no matter the adversity. Companies that are looking to enhance tools, such as the interactive voice response (IVR), to handle call variability, overflows from other channel outages, and keep costs low will likely investigate sensible self-service options to achieve their goals. As companies are investing more to handle unpredictable demands, now is the time to make a case for better self-service. Self-service doesn't require a tradeoff that jeopardizes security for ease of use. If done properly, customer authentication can be both protected and seamless.

As organizations evaluate future strategic options, more and more are seeing self-service and a reduction in agent-assisted calls as a desirable outcome. While the desire to reduce staff needed to handle inbound calls isn't new, the 2020 pandemic may have accelerated plans to increase options for customer assistance. In a Pindrop survey of 23 senior financial services leaders, 77% said that they planned on making improvements to the interactive voice response (IVR) within the next 24 months; with nearly half (42%) of those improvements planned 6-12 months from now[2]. A report released by Avant stated that more than half (51 percent) of IT decision makers are planning to invest in new contact center systems because their current setups lack the functionality needed to support current demands over a longer term.

As practitioners look to improve efficiency and get maximum value for any IVR investment, its impact on work flows and future technology must be considered: What does the customer journey look like when they need to reach the company? Where is the best place for identity and authentication? What are the most effective ways to help customers self-service without having to speak to a call center agent?

Consumers are growing more comfortable and more willing to use self-service systems[3]. The challenge for contact centers is how to help customers serve themselves. This paper will examine considerations when investing in self-service tools for the contact center surrounding finance, security, and workforce automation and how enterprises can maximize their investment in self-service tools.



1. Does your organization plan to expand the usage of the IVR in the near future:

Yes - in the next 6 to 12 months	(6) 33%
Yes - in the next 12 to 24 months	(8) 44%
No - not at this time	(0) 0%
Not Sure	(4) 22%

Survey Results from Pindrop IVR Roundtable event on 4/29: 23 Senior Leaders from 16 FI's

[1] www.nytimes.com/2021/07/03/business/dealbook/hacking-wall-street.html?auth=link-dismiss-google1tap

[2] Pindrop Survey conducted during live event on 4/29 with 23 Senior Leaders from 16 FI's

[3] www.destinationcrm.com/Articles/Editorial/Magazine-Features/The-Top-Customer-Service-Trends-Digital-Channels-Overtake-Service-Options-147820.aspx

Why invest in the IVR and Self-Service?

For contact centers, servicing the highest possible number of customers with the least amount of manpower and cost is an overarching principle as leaders set strategic initiatives. Avoiding expensive agent phone times is often a primary reason for investments in IVRs, intelligent virtual agents (IVAs), and other self-service tools. Driving efficiency in getting calls to the correct department helps reach a resolution faster, shorten handle times and ultimately leads to cost savings. So seeking to reduce any handle time is highly desirable.

Providing good service doesn't require agent assistance. A personalized and automated way to do basic tasks like balance inquiry, appointment confirmations, or being able to connect to an open customer service case, can all quickly and effectively shave precious seconds off some tasks.

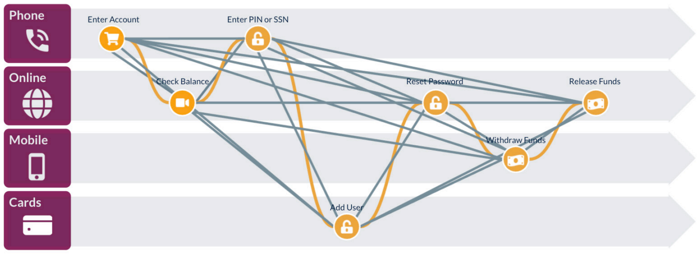
What obstacles are stopping customers from reaching those goals?

Limiting high value transactions to more secure channels can be standard protocol in some contact centers. Without a strong identification process and the ability to authenticate callers to accounts in the IVR, conducting a secure transaction can be severely compromised. Without the ability to authenticate customers or have any insight on their identity, trusting callers would impact the organization's security.

In an average contact center, the suspected fraudster reaches agents about 1 in 1000 times but an average IVR showed that 1 in 162 accounts accessed is high risk. Why is this? In a word, Reconnaissance. Bad actors use the IVR to verify or mine account information, use it to perform account reconnaissance trying to learn everything possible about their intended target.

Common fraud types seen in the IVR are phishing and reconnaissance in an effort to obtain account status, balances mining of account info and password resets. This information is then used by the fraudster throughout the omni-channel such as debit and credit card hijackings and digital account takeovers.

Most enterprises today are restricted to a siloed view of fraud by channel. 60%[4] of fraudulent transactions start with or include a call into an IVR. Additionally, fraudsters looking to take over accounts make an average of five calls[5] into an organization before attempting a transaction. Fraudsters committing online fraud, mobile fraud, card fraud, and account takeovers (ATOs) are going to use any tool they can to make a withdrawal successful, and if possible, repeat the process.



[4] Pindrop Voice Intelligence and Security Report Archives
[5] Pindrop Voice Intelligence and Security Report Archives

Example IVR Fraud activity

Using the IVR in combination with other channels helps the fraudsters maneuver around security controls. It's in the cross channel blind spots where these fraudsters exploit to maximize their effectiveness in systematic account takeover attacks. Below are results from two separate IVR investigations: 2 top 10 Banks in the US.

Investigation #1:

- An average of 615 accounts a day with an account status = high risk
- 84% of accounts with "high risk" status associated with a confirmed fraud event post the IVR call
- Post IVR reconnaissance, some attempts to monetize an account occurred in less than 2 hours, most attempts 1-2 days after the IVR reconnaissance
- One event - 49 calls to 46 accounts (no agent leg) with ~$500K in fraud exposure
- 80% bailout rate on high risk calls, meaning the fraud caller disconnects the call when transferred out to an agent to assist and calls back into the IVR

Investigation #2:

- 5 days offline correlation pilot with confirmed agent fraud calls (Protect) to ANI Validation (Express)
- More than 1% of the total calls in the IVR scoring as high risk - 93.35% were valid/ low risk
- 343 agent fraud calls from 97 different ANIs - which allowed thorough investigation to uncover 432 additional calls contained in the IVR
- 56% of the fraud calls were contained in the IVR

These are just two examples of how bad actors and organized crime rings systematically attack contact centers. Despite not being able to perform transactions in the IVR, criminals are using the IVR as part of their attack. The up to date account information, the low security checks to access the information make the IVR an vital tool in committing account takeover and identity theft. On average bad actors make 2-3 calls before even attempting to speak to an agent for a withdrawal[6]. Those calls, we estimate, are reconnaissance calls to check balances, fraud holds, account activity, or even to mine for additional information. If that is not enough, a fraudster can even attempt to make calls to genuine customers pretending to be working for their bank or trusted organization. to collect more proprietary information. In certain cases, through all of that recon activity, a fraudster can even put together a complete data set ready to commit fraud with and sell to other fraudsters.

The IVR is not only a source of information bad actors use on contact center agents, but can be used as part of fraud that ends up in other channels. For example, if a bad actor had enough information to authenticate into a customer account in an IVR or while on the phone with an agent, and easily reset a password for online banking. Fraudsters are omnichannel operators just like customers. A bad actor might only authenticate into an account for password reset because they can access the victims email, and reset the password to access the account online and empty the funds before a customer would know.

With these multiple threats looming, how can institutions trust any callers or allow self-service? The truth is that no system is perfect, but taking a classic defense, in-depth strategy, and leveraging advanced machine learning technology, can provide a more comprehensive view of channel activity. This increased visibility provides greater knowledge of fraudster behavior which can significantly reduce risk to the organization, and provide better tools to fraud teams, security teams, and contact center agents themselves.

Making Customer Authentication a Seamless Experience

A call center generally deals with thousands of callers on any given day, so adding a personalized touch in every call might seem like a daunting task at first. But, it is crucial to avoid the discouraging sound of indifference in an automated menu or in an agent's voice.

Active Authentication is the process of authenticating callers by requiring callers and/or agents to actively participate in authentication. The most common permeation of this is the use of knowledge-based authentication questions. Here, agents are expected to ask questions to ascertain whether or not the person is who they say they are.

Passive Authentication is the process of authenticating callers without any interaction with the caller or required actions on behalf of the agent or the caller themselves. Passive authentication results in calls that are authenticated before being connected to the agent which creates a smoother, more personalized customer experience and reduces average handle time by eliminating required actions on behalf of the agent and the caller. This strengthens the front lines of your contact center against attack. Passive authentication methods also help increase self-service options in the IVR.

[6] Pindrop Voice Intelligence and Security Report Archives

Combining ANI Validation with ANI Match

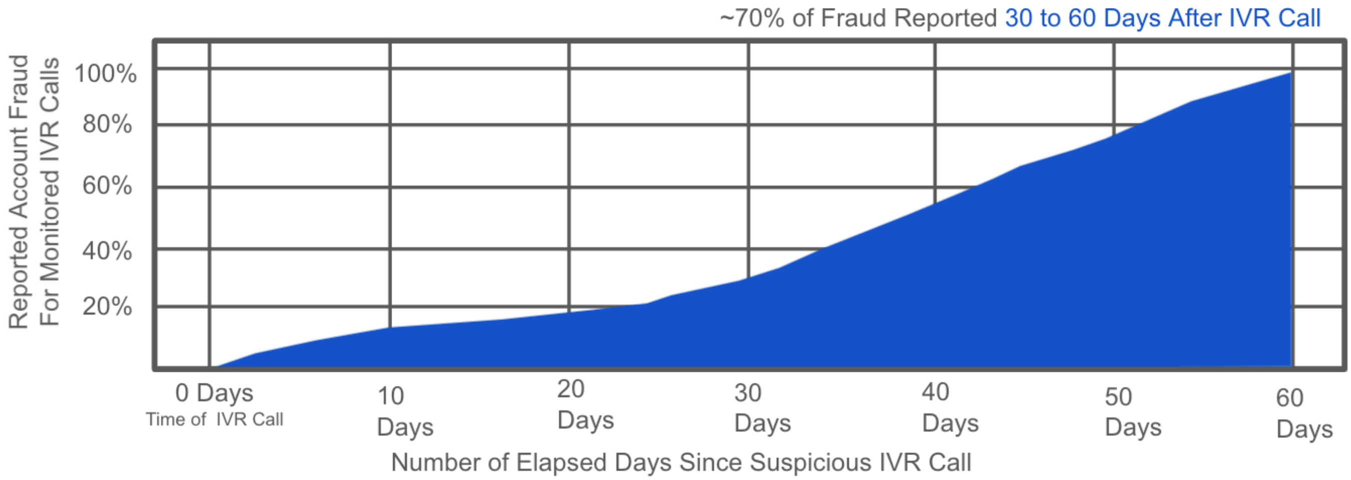
ANI (Automatic Number Identification) Match is a telephony service that allows a business to search their own database for a match with an existing customer account. This process makes it fast and easy for the business to identify the person calling and potentially personalize the interaction. However, ANI Match can only be used safely if the business can trust the number displayed on the Caller ID. For that, a business will need to validate the ANI. ANI Validation confirms that a call is coming from the device that owns the number, meaning that the call has not been spoofed or manipulated, and the number on the caller ID can be trusted. Once the number calling has been validated, the ANI Matching process can begin. ANI Validation combined with ANI Match can be a powerful tool to improve the customer experience while also saving time and money for the contact center.

While the IVR helps to decrease hold times and improve customer experience in some ways, designing the ideal self-service menu also has its challenges. The result of a bad IVR experience may leave customers rapidly pressing the "0" key or screaming "agent" into the phone to give up on their preference for automation. Fortunately, passive authentication can be used to optimize the IVR experience to steer away from the things that frustrate callers. Optimizing the IVR can be the key to delivering on customer expectations and bottom-line contact center savings.

Leveraging Multiple "Factors"

Voice, device, and behavior are 3 common points used to authenticate callers, though multi-factor authentication generally refers to the use of two or more ways of verifying an identity. multi-factor authentication, and more so passive multi-factor authentication, is a more effective and beneficial form of caller authentication. The passive approach offers many benefits concerning security, operations, and customer experience. Call center leadership looking to increase capacity, improve customer experience, reduce agent stress, and address fraud costs should seriously consider passive multi-factor authentication as a solution.

Advanced fraud tools, like Pindrop® Protect, can provide truly proactive fraud monitoring, alerting to risky behavior that is a highly probable "precursor" to fraud. For example, Pindrop performing analysis in the IVR can help identify risky behavior before they are able to collect information to perform an attack, up to 60 days in advance. Systematic fraud attacks tend to take a while for the fraud teams to identify all of the accounts they are targeting, and collect enough information to social engineer a call center agent. That upfront work takes time. We see a large percentage of fraud occur one to two months after the initial contact is made.



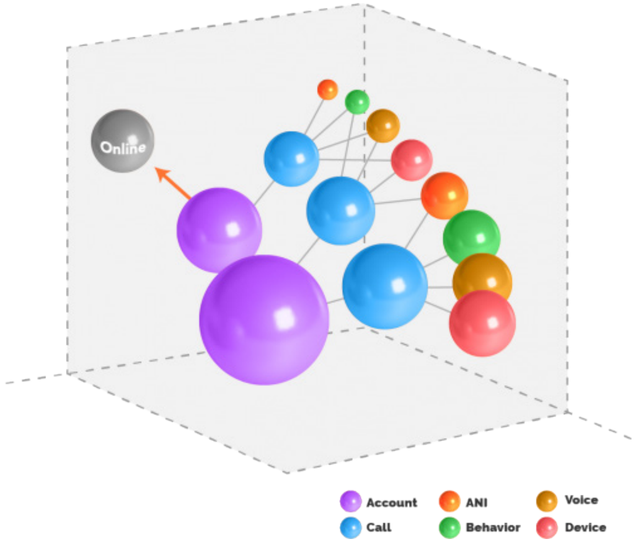
Account Risk Providing Another Dimension

Pindrop measures both call risk and account risk based on actions performed in the IVR or at the agent for suspicious activity. Single actions viewed in isolation may seem innocent, such as an address change, but when coupled with intelligence about how many risky callers have been accessing the account, an account change might signal something suspicious. With the help of machine learning, actions in the IVR and at the agent can provide ratings against how likely an account is to be under attack by a fraudster using both the call risk information and history of account activities. We use that analysis to formulate account risk. Signals from other channels can be added to strengthen account risk ratings, and provide advanced intelligence on which accounts might be under attack.

Standardizing on a risk measure across the organization can help identify cross channel fraud. Suspicious activity and alerts from the online channel can use risk signals from interactions in the IVR and agent. This helps complete missing security protection for the contact center for many companies.

Now that we are using technology to assess call risk and account risk, Pindrop uses that intelligence to help us automate the routing of high risk calls to a dedicated team. Isolating these calls also helps reduce agents' interaction with bad actors to avoid social engineering possibilities.

Better fraud prevention means using any form of connection to track down organized crime syndicates. Because of their systematic nature in which they operate, they likely are after multiple customer accounts at any given institution. If you are able to detect one, there is a strong likelihood that the same bad actors also have other accounts they are working on. Investigating any possible connection through email, device prints, caller id, and even voices will help pull the threads of complex fraud ring networks of account takeover activity. Leveraging technology, as always, can help scale the process. Pindrop Protect, using advanced graph analytics, connects confirmed fraud accounts to any possible connected account to increase the account risk scores accordingly, and help produce more fruitful investigations.



Risk Analysis as another Layer

Risk analysis helps to know exactly when to use step up methods to authenticate customers. Step up authentication strategies use additional security measures when you are unable to confirm identity alternatively. Using risk analysis and ANI validation techniques can provide clues when to use extra security or add steps to an agent's process for an increased security posture. Using the IVR to assess when to use additional screening techniques based on technology can save time and provide a smoother experience for customers not requiring extra security.

Organizations should examine the path of the caller, assess whether to validate their identity, and evaluate if there is an opportunity to authenticate the customer earlier to avoid the channel hoping to bypass security controls. By securely authenticating customers during the initial moments of the call, downstream identity verification can either be shortened or eliminated altogether saving time on each call.

Voice verification should be optimized for very short utterances. Being able to authenticate using less than a second of voice can boost handle times by reducing and eliminating the need for other verification techniques. Pindrop Passport can authenticate known customers in the IVR or at the agent for less than one second of speech. This means when a customer says "representative" that phrase might be enough to positively authenticate using voice, and provide faster and more personalized service.

Enabling authentication in the IVR helps to reduce (most) KBA questions unless further step up is needed. Security questions take time, and often are based on information that may no longer be private. Technology can be used to make identity verification decisions and remove a tool that fraudsters rely on to commit fraud. Even if your IVR isn't voice enabled, adding authentication to the IVR can still help improve security posture and high levels of identity assurance without the need to involve an agent. Self-service can also include authentication without an agent's assistance.

Whether it's through ANI Match and ANI Validation, in the IVR or at the agent, it's crucial for your business to use the right solutions at your contact center to authenticate legitimate callers quickly and accurately. Doing so you can reduce call handle times, enable personalization, and improve customer experience. Proper fraud protocols, and case management best practices can help reduce frauds in your contact center and throughout your organization if the right information can be shared and operationalized. Increasing security doesn't have to mean increasing friction. In fact, proper security can actually help improve customer workflows and reduce handle times as well as fraud losses.

ABOUT PINDROP

Pindrop® solutions are leading the way to the future of voice by establishing the standard for identity, security, 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 an unrivaled amount of intelligence from every call and voice encountered. Pindrop solutions help detect fraudsters and authenticate genuine customers, reducing fraud and operational costs, while improving customer experience and protecting brand reputation. Pindrop, a privately held company, headquartered in Atlanta, GA, was founded in 2011 by Dr. Vijay Balasubramaniyan, Dr. Paul Judge and Dr. Mustaque Ahamad and is venture-backed by Andreessen Horowitz, Citi Ventures, Felicis.

FOLLOW US

in Pindrop @Pindrop

@PindropSec @Pindrophq

pindrop.com