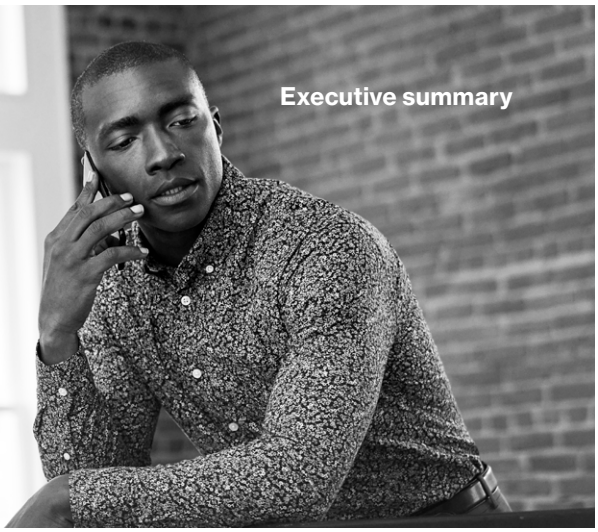
Voice Intelligence Report

A review of fraud, the future of voice and the impact to customer service channels



Executive summary

Imagine a world without passwords or secret questions that get you access to an account or device. Imagine a world that instead relies on an authentication method that's always been a part of you—your voice.

Now imagine a world where your voice—a part of you—gets used by fraudsters to access your accounts, steal your personal information and control your devices.

While it's exciting to think about where voice is headed, our technological advances quickly turn to nightmares if we cannot provide security to consumers. This is something we need to address. Now.

The following summary can help you increase your understanding of how voice security is falling behind, why that matters and what to do about it.

Welcome to the conversational economy.

During the next few years, voice will become the dominant interface across the Internet of Things (IoT) as a world full of smart speakers, smart offices and smart cars continues to propagate.

In 2016, Gartner predicted that a growing number of searches (30%) would be screenless by 2020. We are now stepping into that reality.[1]

But why voice? Competitive advantage. Forrester research shows a correlation between customer experience and stock performance, and a Walker study indicates that customer experience will become more important as a key brand differentiator than even price or product.

It's no surprise then that companies are aggressively deploying voice technology while consumer adoption continues to climb as people embrace digital assistants and voice activity through connected devices. The ultimate endgame? All those speakers, phones, apps, smart devices, cars and offices will identify you by your voice, regardless of platform or brand.

Even government is evolving its customer experience. The beta version of an Alexa skill developed for the city of Los Angeles offers information about public events, and the city plans to connect 311 services to the skill in the future. Mississippi and Utah are also developing skills for Alexa, and at the federal level, the GSA's Emerging Citizen Technology program is exploring solutions for making government services available via digital assistants.

There's just one problem: Where companies see economic opportunity, fraudsters see economic opportunity. A total of $14 billion is lost annually to fraud, and 41% of consumers blame brands for fraud.[2]

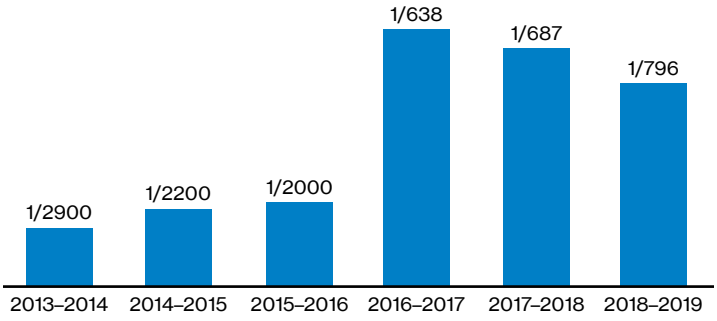
And voice is the least secure interface and one not yet trusted by the majority of consumers. Companies cannot and should not assume customers prize convenience over security.

According to Paysafe, "53% of consumers believe that voice-activated payments are quicker and more convenient than traditional online payment methods, but only 37% feel comfortable that their financial details remain secure when making a payment via a Smart Home device."

So while voice will undoubtedly continue to increase in popularity, companies need to strike a balance between improving internal security hygiene and delivering exceptional customer service.

Fraud rates, tactics and trends

Call center fraud rates



Specific to each industry	Number of fraudulent calls
Insurance	1 in 7,500
Retail	1 in 325
Banking	1 in 755
Card issuers	1 in 740
Brokerages	1 in 1,742
Credit unions	1 in 1,339

Fraud rates in call centers have skyrocketed over the past few years. With an explosion of omnichannel payment options, fraudsters exploit retail call centers to take over accounts with information accessed from past data breaches and dark web research. Peer-to-peer apps, such as PayPal®, WhatsApp®, Zelle®, Apple Pay® and Venmo®, are also exploited as part of a call center attack.

Call center security simply isn't evolving fast enough to keep up. Following are six ways that contact centers are currently enabling fraud through poor voice security.

1. Password resets: As one of the most common scams, a fraudster, posing as a target victim, requests a new password and then uses the changed credentials to log in to accounts. If a fraudster has the right credentials, they can easily reset a password through the call center.

2. Reconnaissance and account mining: Call center interactive voice response (IVR) and customer service representatives (CSRs) offer a wealth of information to fraudsters. Without needing to commit a crime, fraudsters conduct reconnaissance to learn how best to execute a targeted attack.

3. Social engineering: Contact center representatives are especially vulnerable to social engineering. Fraudsters know how to psychologically manipulate people, exacerbated by CSRs feeling pressure to give the best customer experience. When the customer is always right, it's difficult for CSRs to lean on the side of vigilance.

4. Credential stuffing: With so many account credentials such as usernames, email addresses and passwords stolen and leaked after many major data breaches, fraudsters use automated programs to attempt online logins. Once they hack into an account, they can use the information found there to commit additional fraud over the phone.

5. Account takeover: As one of the most common fraudster practices, fraudsters take control of the account and change phone numbers, passwords and other information—allowing them to make unauthorized transactions in another person's name.

6. Synthetic identities: Synthetic identity fraud is the fastest growing financial crime in the United States. Artificial intelligence (AI) can now create convincing video from just one photo and synthetic audio from less than a minute of speech.

Over the last four years, phone channel fraud has increased 350%. Pindrop® Labs estimates that 90 voice channel attacks occur every minute in the U.S.

And fraudsters are constantly evolving their tactics to take advantage of call center weakness. Here are some of their favorite means of attack:

- Calling and acting extremely nice, getting the CSR on their side by commiserating with their struggles so that authentication controls are not used
- Spoofing a bank's automatic number identification (ANI), calling the customer and obtaining a PIN. Then, spoofing the customer's ANI, calling the bank and using the PIN to authenticate

- Spoofing a bank's ANI, calling the customer and obtaining personally identifiable information (PII). Then, spoofing the customer's ANI, calling the bank and using PII to authenticate
- Using call forwarding to receive outbound calls made from bank to verify outgoing wire transfers
- Enlisting elderly mules to open accounts in bank branches. These new accounts are then used for fraudulent Zelle transactions
- Pretending to be from a bank and asking for verification of funds on a checking account
- Spoofing a financial institution's and a victim's numbers to obtain a one-time password (OTP) code from the victim and successfully verify the OTP code with the financial institution on the other line. Activity followed by high-dollar gift card purchases at Walgreens and Publix
- Targeting personal loans for a business by getting fraudulent applications approved through the interception of an OTP by spoofing, ANI porting and SIM swapping
- Requesting new cards to be sent to the customer's home address. Fraudsters then use U.S. Postal Service's Informed Delivery® service to intercept the card in the mail

Trends in authentication

The rise of the conversational economy, the demand for better customer experience and the increase in fraud due to social engineering mean authentication has taken center stage as a key technology for companies. Voice authentication adoption lags behind fingerprint and facial recognition, and authentication methods may still include other biometrics (such as a person's face, fingerprint or gait). However, the interface will be the spoken word.

Voice authentication best practices must include:

- **A risk-based solution:** We need calculated decision-making that assesses the risk of each person who calls into your call center
- **Layered intelligence:** We need to think beyond even two-factor authentication, as any two factors are eventually overcome by sophisticated fraudsters
- **A continuous analysis:** We need to move authentication from an "event" (such as biometric enrollment) to a process
- **A passive process:** We need to add security without adding complexity, avoiding customer experience friction. The solution must work passively in the background to ease customer experience. Passive continuous voice authentication allows frictionless enrollment rates of more than 60% in 12 weeks and multifactor authentication rates of more than 60% in 26 weeks

Remember, customers expect a frictionless yet secure experience. Ideally, enterprises will eventually need to aim at an omnichannel authentication experience where customers authenticate once and gain access to their accounts across different devices.

The current state of voice solutions

Given the trends we've discussed with voice, fraud and authentication, we see multiple weaknesses with the current state of voice solutions—especially in call centers.

- **Poor security easily outpaced by fraudsters:** Where web and mobile security offers many layers of protection, call centers usually only have the telecommunications carrier, any IVR identity claims and knowledge-based authentication (KBA) questions offered by an agent. This is not enough as fraudsters easily outpace many of these basic security measures
- **Poor detection rates and false positives:** Many solutions simply miss a high volume of fraud calls while identifying legitimate callers as fraudsters
- **Ineffective enrollment processes:** While the intent to enroll customers is good, enrollment processes are long, cumbersome, do not capture most callers and do not provide a return on investment
- **Poor implementation:** Enterprises sometimes make missteps when rolling out a voice solution, training staff or enforcing processes and policies. These weaknesses result in friction for customers, high average handle time (AHT), low IVR containment rates, higher contact center operational costs, increased fraud exposure and loss, and risks to a company's brand and reputation. For example, the increased time it takes to enroll a customer during active enrollment situations could likely eat up the time savings they are meant to provide

Additionally, customers might not authenticate as expected if they don't remember the phrase or exact wording of the phrase they created, which would impact a short utterance citation.

So, given all that we've highlighted and analyzed in this report, what is needed for companies to succeed in the conversational economy, provide excellent customer experience and deter fraudsters? The ideal includes the following:

- **Rapidly adopted and zero-effort enrollment experience:** Enterprises need to quickly enroll customers and create credentials using short utterances that are phrase and language agnostic. Enterprises should be able to enroll a majority of customers in less than a year
- **Secure authentication transparent to the customer:** The customer needs confidence in the security and reliability of any authentication process related to voice calls and transactions. Once authenticated, this status is known by the CSR in seconds. This process also needs to prevent imposters from enrolling as customers
- **Risk-based fraud assessment for unenrolled and noncustomer calls:** While analysis occurs in seconds in the background, a CSR gets a notification of a caller's authentication status during the few seconds of a call and can custom-route any high-risk callers
- **Comprehensive analysis across technology factors, accounts, the business and industries:** To identify fraudsters and authenticate with high accuracy, a solution needs to analyze callers with data provided from a variety of factors (including voice, device and behavior) during the entire call duration. This data builds call history by establishing credentials and tracking both call and account risks across the organization—comparing your data with enrolled customers and known fraudster blacklists. This shared intelligence can also span your industry and even other industries
- **Intuitive tools to set the right authentication policies and that possible frauds are investigated quickly and efficiently:** This kind of analysis grows more complex over time, and so any tools used by CSRs, call center managers and IT directors need to be intuitive and align with internal policies and processes—meaning that potential fraud is detected and investigated quickly and efficiently
- **Adaptive technology that supports you today and grows with you:** Because voice technology is evolving so quickly, a solution must adapt over time—as anything today will be obsolete in a short time. Enterprises that fail to find voice solutions that adapt over time and account for the trends, weaknesses and expectations related to the conversational economy and customer experience will fall behind, risk permanent negative brand perception and remain an open target for fraudsters

Conclusion

It's exciting where we're headed with voice. Many lingering security issues that have plagued businesses for years—including KBA questions, passwords and push notifications to a device—may soon go the way of other obsolete technologies as voice becomes the dominant interface of the conversational economy.

But this new era of smart homes and offices brings new, scary risks if security is ignored. Cybercriminals and fraudsters keep up with technology and sometimes even outpace it, and we are always playing a game to keep ahead of them. The conversational economy cannot succeed without voice security, as customers will need to trust without hesitation that their voices indeed work as a reliable, secure and easy-to-use key or password.

Companies that embrace security alongside rapid developments in voice technology will find much uncharted market terrain ahead, including unprecedented opportunities to revolutionize the customer experience through voice.

verizon

1 "Pindrop Voice Near Future Consumer Report," Loudhouse Agency, Oct 2018.

2 Unless otherwise noted, all data and findings come from Pindrop Labs annual "Call Center Fraud Reports," 2013–2017.