VOICE INTELLIGENCE REPORT

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

Why? During the next few years, voice will become the dominant interface across the Internet of Things as a world full of smart speakers, smart offices, and smart cars continue to propagate. In 2016, Gartner predicted that a growing number of searches (30 percent) would be screenless by 2020. We are now stepping into that reality. While only 28 percent of businesses in 2018 used voice technology to communicate with customers, 83 percent planned on using voice technology to communicate with customers in 2019.[1]

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.

Welcome to the conversational economy.

However, hurdles exist along this road. Many are related to technology. Computational resources. The right infrastructure needed to support these resources. The promise of 5G providing a breakthrough in edge computing. Privacy issues preventing the sharing of information needed to verify a person’s identity.

Many hurdles are also societal. Businesses now face a multi-generational customer base with broad-ranging levels of expectations and spending power. Increasingly, businesses are expected to provide an excellent customer service experience
whether their customers are members of the Silent Generation, Baby Boomers, Gen Xers, or Millennials. Each generation has specific tastes, needs, and capabilities when using technology—and the same will hold true with evolving voice technologies. To avoid abandoning a large segment of customers, businesses must face the challenges of delivering a customer’s preferred experience no matter their generation.

Despite these hurdles, organizations are increasingly implementing voice technology to gain a competitive advantage. Forrester research shows a correlation between customer experience and stock performance, and a Walker study indicated that customer experience will become more important as a key brand differentiator than even price or product. For example, a large bank that works with Pindrop has a high net worth client base because many of their clients have reached retirement. As a long-term growth strategy, this bank is actively improving their customer experience with voice technology in hopes of drawing in their clients’ children and grandchildren.

These efforts to streamline processes using voice technology may create a seamless customer experience but it also introduces security risks that can result in data breaches that negatively impact a company’s revenue and reputation. As with many technological advances, security is sadly often an afterthought. As more businesses join the conversational economy to remain at the forefront of their industries, it becomes more important to ensure that security is incorporated right from the beginning in the design and deployment of voice technology.

Because many organizations adopt “the customer is always right” mentality to provide the best experiences for customers, increasingly sophisticated criminals exploit customer service representatives with social engineering tactics and gain access to private accounts. As organizations augment digital security with the latest technologies, hackers understand that targeting company employees—especially through the call center—is the most effective and least expensive way to commit fraud. If they are to leverage voice to improve customer experience, companies will need to strike a balance between improving internal security hygiene and delivering exceptional customer service.
MACRO TRENDS IN VOICE

The growing conversational economy and increased demands for better customer experience are helping spur the evolution of voice interfaces. Concurrently, fraudsters are taking advantage of this rapid technological evolution by exploiting voice channel security gaps through both classic and cutting-edge social engineering tactics.

CONVERSATIONAL ECONOMY

As the conversational economy continues to grow, voice will become the dominant interface for its communication and transactions. What do we mean by the conversational economy? This is an economy driven by interaction. Currently, that means always-on internet connectivity, access to products and services anytime/anywhere through a plethora of devices, and platforms that allow people to engage directly with businesses and other consumers. Businesses already participate in the conversational economy when they immediately respond to customer complaints on social media, engage with prospects through chatbots, or provide seamless omnichannel buying experiences for customers across physical stores, the internet, and the phone.

Why has voice become so popular with consumers? Ease. Voice is the most natural form of communication and the first one we learn how to use, and it’s ironic that technology has only just now caught up to the rich intricacies of voices. Now that computing resources, internet bandwidth, and technological innovation can handle voice well, we predict that voice applications have become the current gold rush—just as we saw a gold rush with touch-enabled devices (starting with the iPhone)—and spawn an entirely new economy.

Voice already dominates customer interactions and grows exponentially each year. Currently, 78 percent of all customer interactions are by voice. For perspective, there are 10 times more call center agents than Uber, Lyft, and taxi drivers combined, and 10 times more voice assistants than call center agents.[2] Research indicates that voice-based ad revenue could reach $19 billion by 2022, thanks in large part to the growth of voice search apps on mobile devices.[3] And one estimate suggests that voice shopping will increase from a $2 billion industry in 2018 to a $40 billion industry in 2022.

Specifically, the adoption of voice assistants and voice activities is also starting to really accelerate. Over 25 percent of the US population has access to a smart device, and a large percentage of people anticipate more voice interactions going forward (such as on cell phones or using voice assistants for shopping).[4] Voice tasks encompassing a variety of situations will increase in adoption over the next 18 months and especially over the next five years—for inside the home, outside the home, and work tasks.[5]
CONVERSATIONAL ECONOMY
Consumers are seeing the benefits of voice as it simplifies their lives, gives them more free time, keeps them better informed, increases efficiency, removes barriers, and improves communication.

INSIDE THE HOME: 18 MONTHS TIME

- Currently using my voice
- Will do in next 18 months

<table>
<thead>
<tr>
<th>Activity</th>
<th>18 Months</th>
</tr>
</thead>
<tbody>
<tr>
<td>Conduct internet search</td>
<td>56%</td>
</tr>
<tr>
<td>Check the weather or news</td>
<td>53%</td>
</tr>
<tr>
<td>Play/control music or radio on my smart device</td>
<td>50%</td>
</tr>
<tr>
<td>Dial numbers on my smart phone</td>
<td>49%</td>
</tr>
<tr>
<td>Check transport timetables or situation and help navigate</td>
<td>44%</td>
</tr>
<tr>
<td>Conduct life admin</td>
<td>43%</td>
</tr>
<tr>
<td>Help with cooking</td>
<td>43%</td>
</tr>
<tr>
<td>Operate technology</td>
<td>43%</td>
</tr>
<tr>
<td>Use as child entertainment</td>
<td>30%</td>
</tr>
<tr>
<td>Manage my home</td>
<td>33%</td>
</tr>
<tr>
<td>Book travel</td>
<td>30%</td>
</tr>
<tr>
<td>Make purchases below £/$/€30</td>
<td>29%</td>
</tr>
<tr>
<td>Bank online</td>
<td>26%</td>
</tr>
<tr>
<td>Order groceries</td>
<td>30%</td>
</tr>
<tr>
<td>Operate my car</td>
<td>21%</td>
</tr>
<tr>
<td>Make purchases over £/$/€30</td>
<td>21%</td>
</tr>
<tr>
<td>Conduct life admin</td>
<td>26%</td>
</tr>
<tr>
<td>Help with cooking</td>
<td>25%</td>
</tr>
<tr>
<td>Operate technology</td>
<td>25%</td>
</tr>
<tr>
<td>Use as child entertainment</td>
<td>24%</td>
</tr>
<tr>
<td>Manage my home</td>
<td>23%</td>
</tr>
<tr>
<td>Book travel</td>
<td>23%</td>
</tr>
<tr>
<td>Make purchases below £/$/€30</td>
<td>22%</td>
</tr>
<tr>
<td>Bank online</td>
<td>21%</td>
</tr>
<tr>
<td>Order groceries</td>
<td>21%</td>
</tr>
<tr>
<td>Operate my car</td>
<td>21%</td>
</tr>
<tr>
<td>Make purchases over £/$/€30</td>
<td>21%</td>
</tr>
<tr>
<td>Conduct internet search</td>
<td>20%</td>
</tr>
<tr>
<td>Check the weather or news</td>
<td>18%</td>
</tr>
<tr>
<td>Play/control music or radio on my smart device</td>
<td>18%</td>
</tr>
<tr>
<td>Dial numbers on my smart phone</td>
<td>18%</td>
</tr>
<tr>
<td>Check transport timetables or situation and help navigate</td>
<td>18%</td>
</tr>
<tr>
<td>Conduct life admin</td>
<td>18%</td>
</tr>
<tr>
<td>Help with cooking</td>
<td>18%</td>
</tr>
<tr>
<td>Operate technology</td>
<td>17%</td>
</tr>
<tr>
<td>Use as child entertainment</td>
<td>17%</td>
</tr>
<tr>
<td>Manage my home</td>
<td>17%</td>
</tr>
<tr>
<td>Book travel</td>
<td>16%</td>
</tr>
<tr>
<td>Make purchases below £/$/€30</td>
<td>16%</td>
</tr>
<tr>
<td>Bank online</td>
<td>16%</td>
</tr>
<tr>
<td>Order groceries</td>
<td>16%</td>
</tr>
<tr>
<td>Operate my car</td>
<td>16%</td>
</tr>
<tr>
<td>Make purchases over £/$/€30</td>
<td>16%</td>
</tr>
</tbody>
</table>

BASE TOTAL: 4057

Q6 Think about some of the devices you could potentially control and interact with using your voice in your home; which actions do you do today and/or plan to be doing in the next 18 months and in 5 years’ time?
However, consumers still have a high distrust of voice-activated technology—using it for low-value versus high-value purchases. Today, consumers mostly use voice in the home for low risk interactions and simple tasks, but we are seeing a gradual evolution of more complex use cases and higher-value purchasing behaviors. Ultimately, people want to use voice to manage their lives, become more efficient, and remove barriers to productivity. That includes the workplace where voice adoption has so far been low. However, while voice has gained the least traction in the workplace, the pace of change is expected to pick up.

As voice interfaces become ingrained into our lives at nearly every point in our homes, cars, and even offices, businesses and IT leaders predict that the use of voice technology will grow three times in the next 12 months. They anticipate this technology will enable cost savings, increase customer satisfaction, and become a competitive advantage. However, voice is also the least secure interface—and companies cannot assume customers prize convenience over security. Most customers are concerned about businesses keeping voice-acquired data safe, misusing data, or failing to combat fraud.

According to PaySafe, “53 percent 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.” Succeeding in the conversational economy also means overcoming challenges with voice such as securing it, allaying privacy concerns, copying and relaying voice accurately, and recognizing slang, mumbling, or regional accents. If enterprises want to leverage cost savings, customer satisfaction benefits, and competitive advantages from voice, they must address voice application security to help encourage adoption.

ZELLE: PEER 2 PEER PAYMENTS APP

“As consumers become increasingly accustomed to splitting dinner checks, paying for their coffee and hailing an Uber without touching paper money, banks are rushing to stake their claim on the wallet of the future.”

OWNED BY BANKS, INCREASING IN POPULARITY, BUT HIGH IN FRAUD

“…Items bought from an on-line bidding or sales site, we recommend you do not use Zelle for these types of transactions. These transactions are potentially high risk. Neither Zelle nor the participating financial institutions offer a protection program for any purchase or sale conducted using Zelle.”

“The con was elaborate. First, a phishing email that appeared to be from Wells Fargo tricked her into entering her bank ID and password into a fraudulent website. The next day, Ms. Butler got a call that appeared to be from Wells Fargo’s fraud department. The number she saw displayed on her phone screen matched the phone number on the back of her bank card—but it wasn’t her bank on the other end of the line. The call had been spoofed. The caller tricked her into handing over one-time passcodes that provided access to Zelle, which was then used to make six transfers from her account, ranging from one penny to $999.98. Wells Fargo refunded Ms. Butler for her loss.” -New York Times, April 2018
As companies move to compete on customer experience as a strategic imperative, it has become a top priority for a large percentage of enterprises. We see customer experience as the next revenue battleground. By the year 2020, customer experience will overtake price and product as the key brand differentiator. And by 2022, digital businesses with great customer experience will earn 20 percent more revenue than comparable businesses with poor customer experience. Among competitors with similar products that solve the same problems, consumers will ultimately choose the company that provides the most thoughtful experience.

However, more demand for better customer experience causes more customer churn. Over 90 percent of consumers answered a survey saying that three or fewer bad experiences would lead them to seek out another business—with 25 percent saying they would do so with just one bad experience. Consumers are now willing to pay more for a better experience and prioritize personalization over speed—moving ahead of price and product as key factors in their buying decisions and brand loyalty.

Societally, customer experience also represents a significant challenge as we now live in an age where at least four generations—the Silent Generation, Baby Boomers, Gen Xers and Millennials—are all potentially a target for some enterprises. Each generation demonstrates patterns of tastes, needs, and capabilities when using technology. For example, will the Silent Generation know how to use a voice assistant to confirm their healthcare benefits? Would that tool work better than a web portal? What happens when a retiree doesn’t have a smartphone to receive an SMS text, or doesn’t know how SMS texting works?

The challenge for enterprises is not to ignore one segment in favor of another but to market to all of them without isolating a specific generation. If Baby Boomers expect someone to answer their call 24/7 while Millennials want to serve themselves without talking to anyone, how will companies serve both of their needs? If Generation Z prefers biometric authentication, are companies ready to meet their expectations? Despite predictions about the demise of phone-based customer service, it remains the number one choice of nearly half the population.

---

**Percentage of Each Generation That Prefers Phone-Based Customer Service over All Other Forms of Customer Service**

<table>
<thead>
<tr>
<th>Generation</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>RETIREES (70+)</td>
<td>80%</td>
</tr>
<tr>
<td>BABY BOOMERS (55-69)</td>
<td>45%</td>
</tr>
<tr>
<td>GENERATION X (35-54)</td>
<td>50%</td>
</tr>
<tr>
<td>MILLENNIALS (25-34)</td>
<td>40%</td>
</tr>
<tr>
<td>GENERATION Z (18-24)</td>
<td>36%</td>
</tr>
</tbody>
</table>

---

“The other day I called my computer helpline, because I needed to be made to feel ignorant by someone much younger than me, and the boyish-sounding person who answered told me he required the serial number on my computer before he could deal with me. …We haven’t been talking four seconds and already I can feel a riptide of ignorance and shame pulling me out into the icy depths of Humiliation Bay.”

– Bill Bryson Silent Generation / Retiree
A changing customer base across multiple generations means changing customer experience preferences. Ignoring the newest preferred platform, growing market segments, or the need to factor security into decisions about customer experience will become detrimental to companies. Many companies still prioritize speed to market and may ignore how accommodating market preferences implicitly involves security. Customers assume security on the part of the provider. Part of a customer’s brand experience is trusting that their account, information, and activities are protected from data breaches and bad actors who could use that data unethically.

The evolution of customer experience related to voice transactions will go through three important stages from now into the future:

**Today - Contact Centers and Voice Assistants**

Today, voice as a part of customer service primarily exists through contact centers for most businesses. Customers call into contact centers to make purchases and resolve customer service issues with the help of IVRs and customer service representatives (CSRs). Companies also leverage AI (such as through chatbots and voice assistants) to provide personalized and real-time attention for customers.

**Near Term - Point Solutions**

Just starting to emerge, these solutions include areas such as keyless home security (requiring voice unlocking and identity matching) and smart speakers (requiring invoking voice applications, identifying voice, and verifying devices through voice). Keyless home security that relies on your own voice instead of traditional keys is already in development. Smart speakers will likely experience growing pains, but we already see numerous digital assistants from Amazon (the market leader), Apple, Samsung, and Bank of America dominating the market while the list of products continues to grow.

During this time, voice commerce (vCommerce) will also grow as consumers use voice more as they shop with digital assistants. Voice authentication (such as a second factor of authentication at an ATM) will emerge alongside biometric authentication such as facial recognition. Consumer devices that already use voice include pet feeding devices, nursery sleep monitors, umbrellas, refrigerators, microwaves, and ovens. These types of point solutions will continue to proliferate until a standard or popular platform for identity is established.

**Future - Ubiquitous Authentication**

Eventually, we are headed toward the smart home, connected car, and the smart office - integrated solutions spanning devices that are all powered by voice. For example, cars currently respond to voices but soon will become the key to your car. All voice scenarios will start to connect. The same authentication and security enjoyed today in call centers will be inside digital assistants and authorize the use of a vehicle.

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.
VOICE FRAUD AS AN ARMS RACE
Where companies see economic opportunity with the conversational economy and improved customer experience, fraudsters see economic opportunity. $14 billion is lost annually to fraud, and 41 percent of consumers blame brands for fraud.[9] On the horizon, we see the threat of deepfakes and AI-generated voice helping fraudsters become even more sophisticated at exploiting the voice channel to effectively steal identities and access accounts.

To say we’re not ready for these advancements is an understatement. With more than 70 security categories, digital channel cybersecurity receives an average spend of $11.7 million from companies while overall spend will increase to $1 trillion by 2021.[10] Meanwhile, protecting voice transactions in the contact center essentially falls to the call center CSRs—resources skilled in customer service but may not be great fraud detectives. After all, he makes $15 per hour and fights fraudsters with a list of questions.

FRAUD RATES, TACTICS, AND TRENDS
Reducing fraud and increasing security affects the success of the conversational economy and customer experience. Because voice fraud skirts the “superhuman” cybersecurity applied to the digital channel, fraudsters prefer to use social engineering tactics that easily get past a contact center representative.

Let’s look at current fraud rates, explore the “why”s behind the data, and look at some concerning fraud trends.

FRAUD RATES
Fraud rates in call centers have skyrocketed over the past few years, and we reached another peak in 2018. The 2018 fraud rate is 1 in 685, remaining at the top of a five-year peak. We will likely see this peaking trend continue for years to come as fraudsters make fewer attempts but exploit companies for bigger losses as fraud becomes more effective over time.

Just like any industry that uses continual improvement processes like consumer electronics and automobiles, each generation gets improved over time.
Over the last four years, phone channel fraud has increased 350 percent. Pindrop® Labs estimates that 90 voice channel attacks occur every minute in the U.S.

Fraud is increasing and staying at these peaks across all industries for many serious reasons.

**Repercussions from data breaches:** The amount of information available on the dark web from data breaches effectively renders knowledge-based authentication (KBA) obsolete. The US remains a favorite target of fraudsters because Social Security numbers (SSNs), often used to verify identity over the phone, are now very easily accessible. We are unable to change SSNs, so as long as institutions rely on them, fraudsters will succeed.

**Consumers not following security best practices:** Consumers share passwords between friends and coworkers at an alarming rate. In addition, consumers often choose weak passwords and KBA questions while not paying attention to cyber hygiene. For example, previously used one-time passwords (OTPs) over mobile are easily acquired through social engineering as a fraudster pretends to be the bank. They talk to the victim while another fraudster initiates the OTP, pretending to be the customer on the phone with the bank. Or, they may change the phone number on the account and then receive the OTP on their own phone.

**Fraudsters getting smarter and working less for more payoff:** As fraudsters grow more sophisticated, they use more targeted social engineering attacks for bigger payoffs. They plan more, rely on information acquired on the dark web, and go after large amounts of money. The “why” boils down to success. If fraudsters can succeed, they will continue. And weaknesses in the call center encourage fraudsters to continue committing voice fraud.

**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.**
LEARNING TO THINK LIKE A FRAUDSTER
THE FRAUD BIBLE

Have you ever wondered where - and how - fraudsters learn how to do what they do best? A new publication, The Fraud Bible, is here to answer all your questions - and unfortunately share the means of becoming a criminal. From a consumer mindset, this bible will offer insight into the ways fraudsters take advantage - but from a fraudster mindset, it is only a starting point.

Regardless of how it appears, this guide is more sinister than a first glance may allow. Though gaining immense traction this past week, over six months have passed since the Fraud Bible was originally released. Inside, there’s information on everything from counterfeiting to creating fake IDs, bitcoin and giftcarding. These shared fraud tactics and methods are criminal offenses, yet in a format of a guide found on the internet, it looks more and more like non criminal activity.

My next question is how do you find this criminal guide? A quick Google search will get you there - some with promises of a free download, others costing you hundreds of dollars. And with it, there are over 14,000 files making up 35 gigabytes. These files are in highly specific named folders, which gives us an insight to how detailed fraudsters are in their methods of committing fraud - and how they target their victims.

We have seen fraud rise 350% over the past five years. Is the Fraud Bible responsible? Not solely - but it has definitely contributed. As fraudsters begin to become more intertwined with one another, and as there is more communication between who fraudsters are targeting and the ways they are accomplishing this, the fraud rate will continue to rise.
CALL CENTER WEAKNESSES

Fraudsters are always playing a cat and mouse game by asking for different information when they call into contact centers. Originally, fraudsters used available credentials to take over accounts and focused first on banks. As banks eventually shored up their security (such as with Chip and PIN), fraudsters started to look at other industries and developed techniques specific to those industries. Any industries currently overlooked by fraudsters will become targets as fraudsters exploit industry-unique contact center security vulnerabilities.

Today, fraudsters can now overcome formerly effective security measures such as the one-time password (OTP), knowledge-based authentication (KBA) questions, and Automatic Number Identification (ANI).

Six ways that contact centers currently enable fraud through poor voice security include:

1. **Password Resets**: As one of the most common scams, fraudsters request a new password, posing as a target victim, and then use the changed credentials to log into 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 IVRs and 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 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. AI now exists that creates convincing video from one photo and synthetic audio from less than a minute of speech.

Despite knowing the deficiencies of KBA questions, enterprises still use them and they remain a big role in authentication. When authentication methods fail, enterprises use KBA questions as a fallback—and bad actors are well prepared to answer. And even with security involving “something you have” (such as a smartphone), there are ways for a fraudster to get around this multifactor authentication obstacle. OTPs, push notifications, and other forms of multifactor authentication are vulnerable to SIM swapping, cloning, and telecommunications account takeovers.

It’s true that voice ("something you are") is a great method of authentication because fraudsters
have much more difficulty compromising it. But even voice is not foolproof. Research has also shown that voice recognition technology can skew toward white males—with results more accurate with them than women or non-white males.

These problems aren’t just impacting your call center—they also impact the security of your digital channel. Fraudsters use call centers as a jumping off point to get further into target accounts by resetting passwords, changing shipping addresses, performing reconnaissance on target accounts, and testing which agents they can manipulate. Weaknesses in the call center compromise other channels.

**FRAUD TACTICS AND TRENDS**

Fraudsters evolve their tactics to take advantage of call center weaknesses. These are some of the top fraud tactics we are seeing.

**RETIREMENT AND ELDER FRAUD ABUSE**

Retirement funds are now a huge target for fraudsters. After banks and payment providers started shoring up their phone channels, fraudsters sought out adjacent targets such as pension providers and retirement firms. Retirees and elder individuals come from a more trusting generation and are a ripe target for fraudsters.

Required Minimum Distribution plans are a special target for hackers. Typically, these accounts have large balances—often in the six or seven figures. To withdraw those funds, a particular fraud ring could obtain the appropriate download forms from a company’s website and use the call center to complete the fraudulent transaction(s).

Fraudsters are also using the elderly as mules to open new accounts, which then are used in peer to peer payments. Again, the elderly can be trusting and in need of employment in their retirement years if they don’t have enough savings. They can be deceived into thinking they are working

**HOW FRAUDSTERS ARE ATTACKING**

Here are some of the many ways that fraudsters can attack your call centers.

- Calls and acts extremely nice, getting the CSR on their side by commiserating with their struggles so that authentication controls are not used.
- Spoofs bank’s ANI, calls customer, and obtains PIN. Then, spoofs customer’s ANI, calls the bank, and uses PIN to authenticate.
- Spoofs bank’s ANI, calls customer, and obtains PII. Then, spoofs customer’s ANI, calls the bank, and uses PII to authenticate.
- Uses call forwarding to receive outbound call made from bank to verify outgoing wire transfer.
- Enlisting elderly mules to open accounts in bank branches. New accounts are used for fraudulent Zelle transactions.
- Pretends to be from a bank and asks for verification of funds on a checking account.
- Spoofs financial institution and victim’s numbers to obtain OTP code from the victim and successfully verify the OTP code with the financial institution on the other line. Activity proceeded by high dollar gift card purchases at Walgreens and Publix.
- Targets personal loans for a business by getting fraudulent applications approved through the interception of an OTP by spoofing, ANI porting, and SIM swapping.
- Calls into call center requesting new cards to be sent to the customer’s home address. Fraudsters then use USPS’s Informed Delivery service to intercept the card in the mail.
FRAUDSTER PROFILE  
MARK TWAIN

This fraudster calls as a son and beneficiary of the policy owner to obtain a death claim worth over $200,000. The true policy owner lives in another country and another beneficiary (the wife) receives a letter from the insurer notifying the wife of her husband’s untimely demise and is provided the claim packet. The wife and owner call to state that the policy owner is in fact still alive.

As the population ages, the number of consumers reaching retirement age is growing—presenting more victims to fraudsters. Elder abuse has been cited by Pindrop customers as a growing problem. Family members or caretakers can call on behalf of the elderly, or even pose as the elder customer, to make changes to an account, submit a claim, or cash out policies. According to the ICX 2019 Trend Report, “Senior citizens are more likely to have savings and own property, making them an attractive target to criminals. And due to generational differences, many elderly people are more trusting than younger generations, making them more susceptible to scams. According to the Consumer Financial Protection Bureau, financial institutions reported more than 180,000 suspicious activities targeting the elderly, involving more than $6 billion.”

INSURANCE VOICE FRAUD INCREASING

With insurance, the sums of money and stakes of success go up. Fraudsters use fewer but more effective tactics to steal this money. We have seen a 248 percent fraud increase in insurance contact centers. The current fraud rate for insurers (1 in 7500) is still much lower than the overall call center fraud rate of 1 in 685, but the fraud exposure for insurance is much higher. Life insurance policies are typically a higher value target than a bank account, and fraudsters attacking this space often
go after policies that exceed $500,000. During the past year, one Pindrop insurance customer saw attempted fraud loss average go from $5,000 to $500,000.

In the insurance industry, IVRs are highly at risk for data mining and reconnaissance, and ineffective KBA questions do not work to deter fraudsters. For example, the “Policy Marm” fraudster phishes through the phone channel to get information about insurance policies and 401k plans, gains intimate knowledge about the rules and processes involving large withdrawals, and pretends to be an elderly female to gain the trust of call center agents.

The insurance industry’s shift to digital business channels, both for customer onboarding and claims submissions, has further exacerbated these problems by making it easier for criminals to create fake identities and perpetrate fraud. According to the FBI’s website, the total cost of insurance fraud (excluding health insurance) is estimated to be more than $40 billion per year. That means insurance fraud costs the average U.S. family between $400 and $700 per year in the form of increased premiums.

Common types of insurance fraud gaining popularity with fraudsters include:

- **Policy fraud**: Policy fraud is the cashing out of life insurance policies or taking loans against them. Consumers check in with a life insurance company infrequently, and fraudsters will use that fact to their advantage. Sophisticated
fraudsters have a well-developed knowledge of how to cash in a policy or loan without arousing suspicion. They know the paperwork process of the company they target and can pose as an enterprise policy administrator as well as a policy holder. The more process knowledge they acquire, the more they are able to socially engineer the CSRs they encounter.

• **Claims fraud**: Claims fraud involves the use of counterfeit documentation and in-depth knowledge about the paperwork process to change the policy owner or beneficiaries. Some fraudsters even go so far as to claim the death of the policy owner to collect benefits or redirect benefits of claims in process. This is a less frequent occurrence than policy fraud but still a high value target for bad actors.

• **Account Takeover (ATO)**: The most popular and most frequent type of insurance fraud is the account takeover. Fraudsters are looking to gain credentials to claim themselves as the owner of an existing account. From here, the fraudster can make claims, change mailing addresses, change beneficiaries, and even take out loans against life insurance policies.

Other types of fraud include true name fraud (taking a person’s stolen credentials to open a new account), enrollment fraud (fraudsters calling a person to steal information while pretending they are enrolling them as a customer), and fraud reconnaissance (calling CSRs and navigating IVRs to collect information later used in fraud).
FRAUDSTERS CRACKING VOICE BIOMETRICS
While we already highlighted voice biometrics as vulnerable if used in isolation, trends show that voice biometrics will only increase in adoption. The boon of voice biometrics for omnichannel customer experience, spurred by improved voice biometrics technology, will only increase adoption. Enterprises benefit from authentication that only takes two to six seconds while reducing Average Call Handling (ACH) time and customer experience friction.

Voice biometrics alone isn’t perfect. Fraudsters are finding ways to crack voice biometrics and Pindrop diligently monitors any possible threats to voice as a valid form of authentication and fraud prevention.

Some tactics fraudsters use to bypass voice biometric solutions include:

- **Imitation**: Fraudsters either impersonate the genuine speaker or escape positive identification through a disguise.

- **Replay Attack**: Well-recorded audio is perceptually indistinguishable from legitimate speech, making replay attacks—recording someone’s voice and playing it over the phone—simple and effective. Recording devices (usually on a smartphone) are ubiquitous and easy to use, requiring no social engineering or imitation skills. Quality, of course, is highly dependent on the recording and acquisition conditions.

- **Voice modification**: Much more sophisticated than the previous two methods, fraudsters use software that converts their voice to the target’s voice. The software’s electronic voice distortion capabilities allow the fraudster to perfect nuances such as the pitch of the voice.

- **Voice synthesis**: Synthesized voices have improved in quality in recent years through the evolution of deep learning. Services such as Google WaveNet can take text and make it sound like a natural human voice. While Google WaveNet produces the sound of generic human voices, software such as Adobe VoCo or Lyrebird can take a few minutes of genuine speech to sound like the target’s voice.

FRAUDSTER PROFILE

**MR. NICE GUY**
This fraudster calls and acts extremely nice, getting the CSR on their side by commiserating with their struggles so that the authentication controls are not used.

**GHOST VENDOR**
After setting up a fake account for access, the fraudster sends an invoice he found in the organization email and sends it to the target business. The business, that happened to owe money, now wires the money to the fraudster control account.
DEEPFAKES AND SYNTHETIC VOICES

Originating in academia in the late 1990s, deepfakes grew out of computer vision research and evolved into programs such as Face2Face (2016) and “Synthesizing Obama” (2017). Deepfakes gained major popularity after Jordan Peele voiced a video of President Obama about deepfakes that was made by Peele’s production company using a combination of old and new technology: Adobe After Effects and the AI face-swapping tool FakeApp. More advanced research was presented at a 2018 Siggraph conference called Deep Video Portraits that offered a photo-realistic re-animation of videos debuted by researchers at Cornell University.

Concurrently, amateurs in online communities began sharing deepfakes while improving software made it easy to experiment. In 2018, deepfakes used for pornographic purposes gained attention but the topic started to become mainstream in 2019 because the technology had improved so much that people were having trouble telling apart real from fake videos.

The audio portion of deepfakes is part of a wider trend of synthetic voices growing more accurate and indistinguishable from a target’s voice. Currently, benign positive uses are being developed such as Google Duplex that can help people make mundane, routine calls on their behalf (such as making an appointment or reservation). Deepfakes and synthetic voices can also serve as entertainment or a fun app, but malicious uses immediately emerge from such a technology. The impact ranges from involuntary pornography to political slander. Many security experts call deepfakes worrying.

Currently, we are seeing the dawn of the testing of synthetic voices in the banking sector. Fraudsters are calling into contact centers using synthetic voices that start talking gibberish. These fraudsters are likely testing reactions to detected synthetic voices or seeing if they have the technology in place to detect them. If their ANI isn’t blacklisted, they may try to further push these attacks.

Deepfakes will only become more concerning as deep learning improves. Deep learning depends on Generative Adversarial Networks—deep neural net architectures comprised of two neural nets, pitting one against the other. Under certain conditions, the training process reaches a point where the discriminator cannot classify generated examples from real ones. GANs were introduced in a paper by Ian Goodfellow and other researchers at the University of Montreal.

The potential of GANs is huge because they can learn to mimic any distribution of data—replacing images with video, or video with sound. These technologies use machine learning to generate audio from scratch, analyzing waveforms from a huge database of human speech and re-creating them at a rate of 24,000 samples per second. The end result includes voices with subtleties such as lip smacks and accents.
TRENDS IN AUTHENTICATION

The rise of the conversational economy, the demand for better customer experience, and the increase in fraud due to social engineering means 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.

Consider the following statistics:

• Live agent authentication is conducted for 88 percent of calls
• 68 percent of calls require security and identity checks
• The average length of time for a security check is 35 seconds
• The cost of agent authenticated calls is $0.67 per call
• The total cost of authentication in contact centers is $10.2 billion per year
• The contact center fraud rate increase over the last 5 years is 350 percent\(^{[11]}\)

We see various myths about authentication propagated by companies that, if not debunked, will affect them from succeeding in the conversational economy and providing the best customer experience in a world dominated by voice interfaces. Let’s debunk a few of these myths.
MYTH 1: VOICE BIOMETRICS CREATE AN IMPENETRABLE OBSTACLE FOR BAD ACTORS. IT IS (ALMOST) COMPLETELY BULLETPROOF.

Actually, any single authentication factor is vulnerable to exploitation. What happens when a false positive biometric gets into an account? How would you prove that someone else was verified as you? What happens when someone else can authenticate into your account? If someone else has your password, are they you?

It’s critical that companies use multiple authentication factors and methods to reduce the odds of false positives and assure skeptical consumers that these methods are secure. Yet, companies must still provide as frictionless an experience as possible with multi factor authentication. The technology must be able to identify a person’s voice accurately, and the authentication must serve the omnichannel demands of the conversational economy—traversing both the real world (call centers) and digital world (texting, chatting) with voice-activated assistants and products.

MYTH 2: AUTHENTICATION SOLUTIONS KEEP FRAUD OUT OF MY CALL CENTER.

Not necessarily. Authentication solutions work by blacklisting fraudsters. But voice blacklisting means a fraud must first occur in order to then blacklist a fraudster and later catch them during the authentication process. But how do you stop a fraudster the first time? How are you preventing fraudsters from enrolling as customers during an initial rollout? Even when they call for the first time, you need to catch them in the act by positively identifying a fraud call and adding their voice to your blacklist.

But what if that same fraudster uses a voice modulator? What if they use a call center to reset a password and then commit the fraud online? What if the fraudster gets a friend to get past the first part of the call or the point in time where the company collects the voiceprint? So many weaknesses surround current authentication solutions that fraudsters can easily get around.

MYTH 3: KNOWLEDGE-BASED AUTHENTICATION WORKS FOR US.

Although we dealt with this topic earlier, it’s worth mentioning KBA in the context of authentication because so many companies still cling to this method.

Consider a few statistics:

- In 2018, 446 million records (including answers to KBA questions) were exposed from more than 1200 data breaches
- 47 percent of people can’t remember their favorite food answer after 1 year (Google)
- 30 percent of callers are unable to authenticate because of KBA question issues (Gartner)

It’s clear that KBA questions are not an effective form of authentication anymore. After major data breaches, nearly everyone’s personal data—including answers to most KBA questions—has been leaked several times over in breaches by consumer credit companies, retailers, social media companies, and other entities. Additionally, fraudsters are actually better than customers at answering KBA questions. They know what types of questions institutions typically ask and are prepared to answer.
So should the questions become harder? No, because then legitimate customers also have a hard time answering them, rendering the authentication process ineffective. Relying on KBA questions is a losing proposition.

**MYTH 4: ONCE YOU HAVE ENROLLED A CUSTOMER INTO A VOICE BIOMETRIC PLATFORM, THEIR VOICEPRINT WILL WORK FOREVER.**

Voice ages just like our bodies. Over time, vocal cords lose elasticity and flexibility. The larynx, across which the vocal cords stretch, is a muscle that can atrophy and become thinner or weaker over time. As these muscles change, the pitch and speed of a voice can change—rendering a “permanent” voiceprint impossible. A Pindrop® Labs study confirms that the error rate of voice biometrics doubles as voices age just two years. Even health issues, emotions, and stress can alter a person’s voice enough to fail a voice biometric match.

**MYTH 5: REACHING CRITICAL MASS FOR ENROLLMENT IS EASY OR CAN BE DONE QUICKLY.**

Many enterprises are overly optimistic about enrollment despite evidence to the contrary. Active enrollment is costly and can produce less than desired results—making it a huge challenge for enterprises.

In an eight-month Pindrop® Labs study, 48 percent of callers only called once and less than 10 percent called three times or more. Enrollment also involves time retraining staff on new call procedures. Then, even when implemented, let’s say each call takes two minutes to enroll but only saves 30 seconds of call time later. That means an enrolled customer needs to call back four times before a return on investment can happen—forcing you to enroll a large portion of your customer base to justify the purchase price of an authentication solution.

Further, active enrollment typically nets only about 30-40% at best over the lifetime of the solution. Unless you have an identity claim (such as a phone number on file) that is accurate for your entire customer base, enrollment and authentication rates will mathematically be imperfect. Of your total customers, how many have an identity claim on file? Then, how many call in often enough to enroll? Then, are they authenticating when they do call? If you can only get 50 percent of callers into your voice biometric authentication, then what about the other 50 percent of your customers?

What about facial recognition as an alternative to voice recognition? Some issues crop up if enterprises want to go this route. First, facial recognition requires an HD camera (which everyone doesn’t own) and lighting as a variable. These factors detract from accurate identification. By contrast, audio noise can actually help the credentialing of a voiceprint. Voice is more universal because we can assume that everyone has access to a telephone (even if it’s a landline) as opposed to a smartphone. Any mobile phone verification still leaves the device as the choke point and becomes something you have versus something you are—your voice.

**Voice Authentication best practices must include:**

- **A risk-based solution:** Calculated decision making needs to take place 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 through adding obstacles. The solution must work passively in the background to ease customer experience. Passive continuous voice authentication allows frictionless enrollment rates of more than 60 percent in 12 weeks and multi-factor authentication rates of more than 60 percent 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 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

---

**FRAUDSTER PROFILE**

**GOLDEN GIRL**

This fraudster can pass all verification questions, create an online account, and fax in annuity withdrawal paperwork. Funds are wired to a business account where the imposter is listed as a signer after socially engineering the CSR to add her on the account.
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 non-customer 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 to 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 the criminals. 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. Solutions and best practices exist to stay ahead of the fraudsters. This report serves as a way to outline the nature of the threat and why taking action early is so imperative as we glimpse the beginnings of a new economic battleground, gold rush, and technological disruption.
“You are actually identifying all the things it takes to start mimicking a million years of human evolution in voice. Our synthesis systems do a good job at synthesizing a voice but not yet things like cadence, emotion and flair, which are all active areas of research.”

Vijay Balasubramaniyan
Pindrop’s CEO