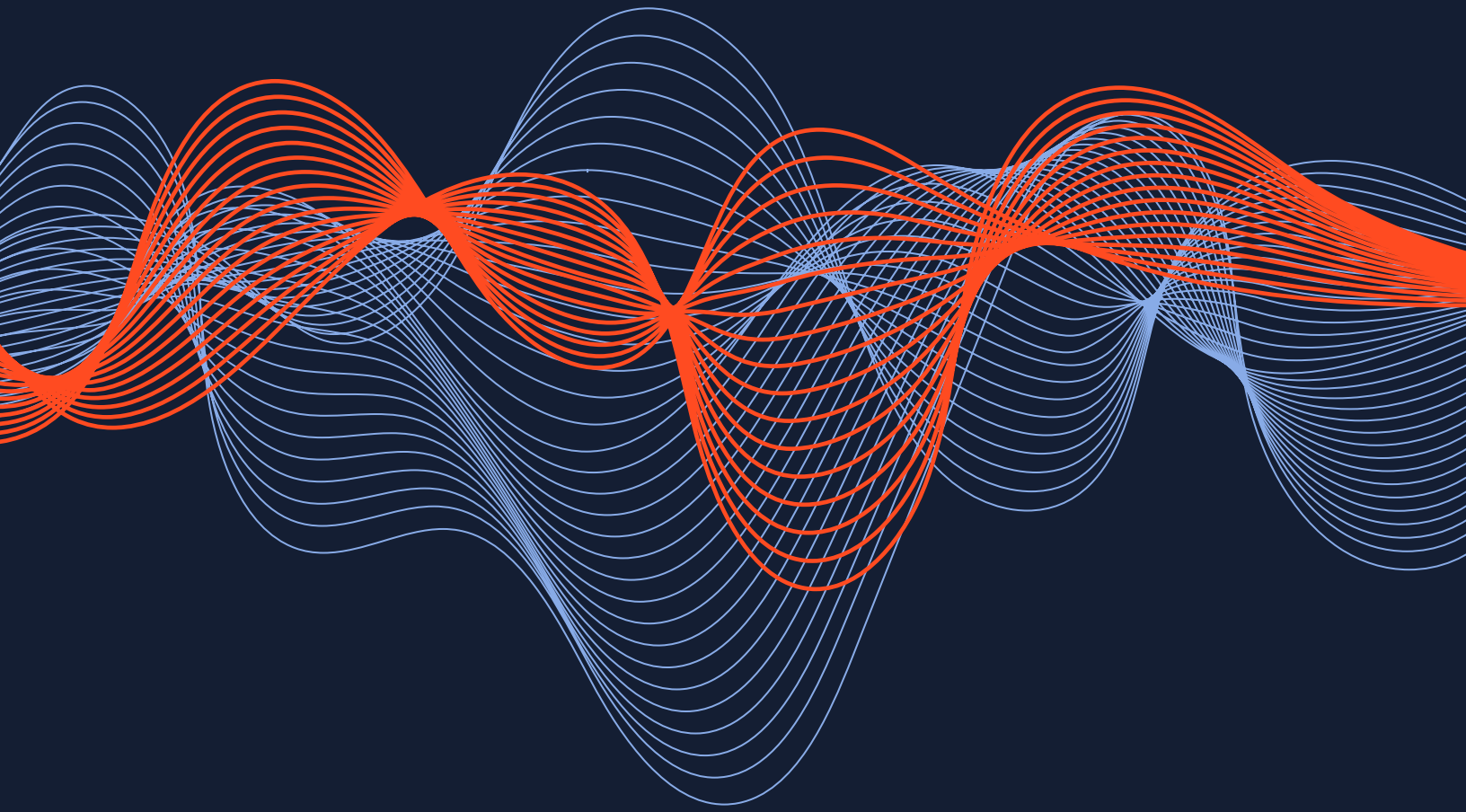
Pindrop®

2023

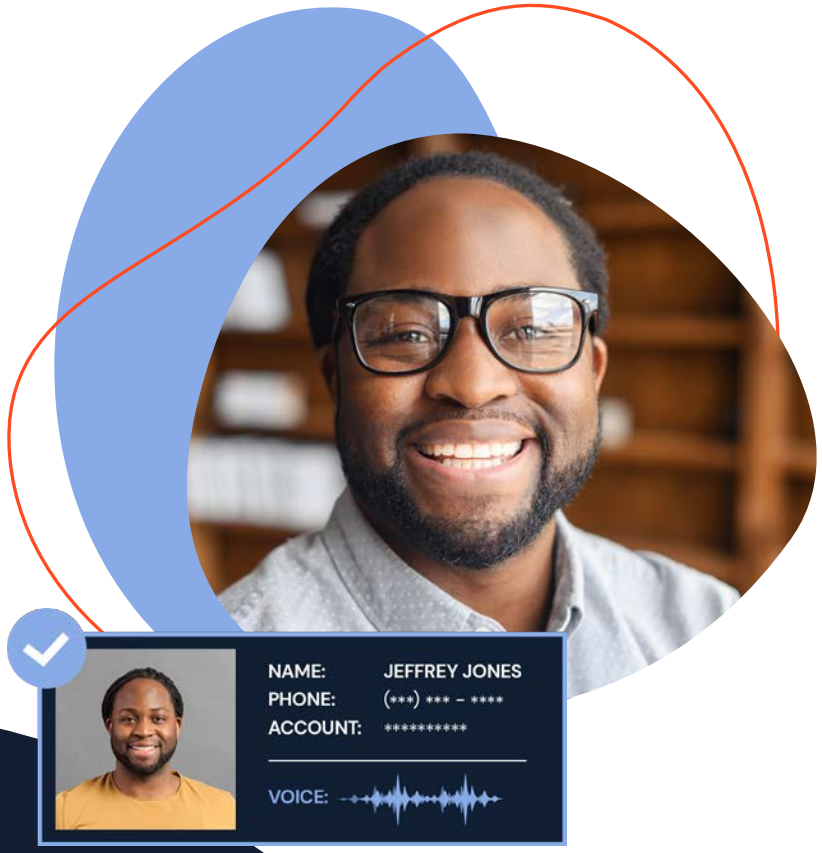
Voice Intelligence and Security Report

The Fraudsters Strike Back



REPORT

Identity and voice theft are growing concerns that can lead to financial loss and damaged trust between individuals and businesses. Fraudsters use stolen voice data to manipulate voice authentication systems, gain access to confidential information, and conduct fraudulent transactions. This report examines how advanced security frameworks, open communication with customers, and effective regulation can be leveraged to combat fraud. By working together, we can mitigate the risks of fraud and ensure a safer digital environment for everyone.



In this report

SECTION 1

Introduction: The Dynamic Nature of Fraud

A look into how our economic environment, technology, and social connections are impacting current fraud trends.

Following recent economic changes, fraudsters have shifted focus away from government payouts and back to their traditional targets—contact centers. However this time, today's fraudsters are now armed with new tactics, including the use of personal user data available on the dark web, advancements in artificial intelligence (AI) for creating synthetic audio, and an increased willingness to work in teams. This has led to a 40% increase in fraud rates on contact centers in 2022 compared to the previous year.

Three important questions you need to ask and this report will answer:

1. What tactics, technologies, and methods are fraudsters using to target not just contact centers but entire organizations?

2. What new tools and techniques are at your disposal to work as an effective fraud prevention framework?

3. What are the key elements shaping the landscape of fraud and fraud defense in 2023?

SECTION 2

Mitigating Fraud Risks in Times of Economic Uncertainty

2022 was a year marked by turbulence. The ongoing conflict in Ukraine reverberated across the globe, causing widespread economic uncertainty, soaring inflation, and prompting central banks worldwide to adopt high interest rates. Concerns about an economic downturn and a possible recession quickly emerged.

According to a recent Gartner® study "nearly half of financial services leaders surveyed believe a recession is coming".[1] While the extent of the economic disruption remains a topic of debate, what's abundantly clear is that the current climate of uncertainty provides a fertile breeding ground for fraudsters.

During an economic downturn, fraud is typically reported as a significant crime.[2] Historical data further suggests that both insurance claims and fraud will skyrocket in 2023.

During the 1980, 1990, and 2008 recessions, fraud offenses increased between 5% and

10%[3]

[1]N= 80 Senior Financial Services Executives. Gartner, Infographic: Financial Services Business Priority Tracker 3Q22, December 13, 2022
[2]Skopenow.com, Crime Trends During a Recession
[3]Professor Mark Button, Director of the Centre for Counter Fraud Studies at the University of Portsmouth, 2020

SECTION 3

Data Breaches as a Driver of Fraud

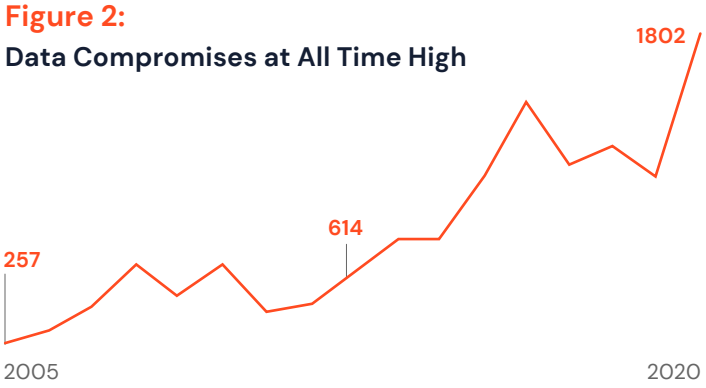
The digital economy has revolutionized the consumer experience, providing unparalleled convenience and access. Unfortunately, it has also led to an unprecedented number of data breaches. Fraudsters capitalize on the massive amounts of data that are dumped into the dark web every year. According to last year's report,[4] the dark web is now inextricably linked with fraud and increasing levels of sophisticated operations around buying, selling, and usage of illicit data.

In 2021 and 2022, the number of reported data breaches reached an all-time high, with over 1,800 incidents each year. These breaches compromise a wide range of sensitive information, including names (the most commonly compromised), full Social Security numbers, birth dates, addresses, email addresses, credit card details, phone numbers, medical records, and bank account details.

Figure 1:
Number of data Breaches (Millions)

Source: Identity Theft Resource Center, 2022 Data Breach Report

Figure 2:
Data Compromises at All Time High



Source: Federal Trade Commission, Consumer Sentinel Data Book 2023

Fraudsters sell this data to one another before using it in large-scale vishing/smishing efforts, victim social engineering, and (Interactive Voice Response) IVR reconnaissance. These tactics have caused permanent damage to brand reputations and forced consumer abandonment, resulting in the loss of billions of dollars.[5]

Since 2020, these data breaches have affected over 300 million victims,[6] highlighting how widespread and damaging online fraud can be.

[4]2022 Voice Intelligence and Security Report, How the Dark Web Broke Authentication Forever
[5]FTC, Consumer Sentinel Report Data Book, 2023
[6]Identity Theft Resource Center, 2022 Data Book, January 2023

Understanding the Abstract and Delayed Impact of Data Breaches on Fraud: the Challenge for Contact Centers

Data breaches have an abstract and delayed impact, due to a lag between the breach and the perpetration of fraud. Unfortunately, the frequency of these incidents, combined with limited collective action on digital security and data protection, has led to a phenomenon known as "data breach fatigue," in which people become indifferent to these events. The challenge then lies with the contact center, which must connect the dots between the breaches and their impact on the business while tracking the risks involved. The combination of unstable economic conditions and persistent data breaches is the perfect recipe for an increase in fraudulent activities.

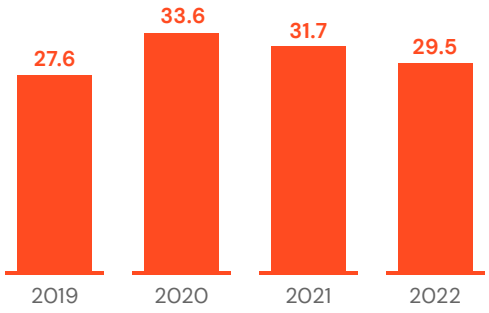
SECTION 4

Evolution of Fraud in Contact Centers

Balancing customer satisfaction with the need to protect against fraudulent activity is a daunting task for contact centers. Although call volumes have started to decrease to pre-pandemic levels, the challenges facing contact centers remain significant. To fully understand the impact of these challenges, it's important to take a look at how the industry has evolved in recent years.

During the peak of the pandemic, the number of calls handled by agents increased dramatically, rising by 22% in 2020 to reach a peak of 33.6 billion calls.[7]

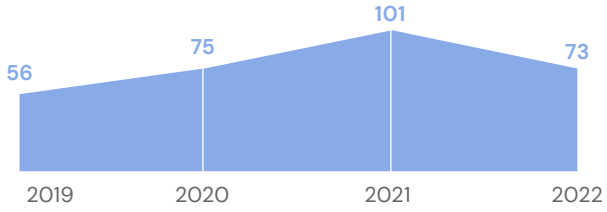
Figure 3:
US – Agent Handled Inbound Call Volume (Billions)



Source: Contact Babel, US Contact Center Decision Makers Guide, 2023

The surge in call volume led to longer wait times, with industry data revealing that the average time on a call before reaching an agent began to increase in 2020 and reached its highest point in 2021 at 101 seconds. However, by the end of 2022, this wait time had decreased to 73 seconds, representing a decline of 27%.

Figure 4:
Average Speed to Answer (Seconds)



Source: Contact Babel, US Contact Center Decision Makers Guide, 2023

While the reduction in call volume and wait times has improved the customer experience, it's also created unintended consequences. Since the traditional method of social engineering of agents became difficult, fraudsters adapted to longer hold times and reduced agent capacity during the pandemic by spending more time in the interactive voice response (IVR) system, mining the IVR's data and gathering intel.

[7]Contact Babel: US Contact Center Decision Makers Guides 2020, 2021, 2022, 2023

Today, fraudsters have returned to their traditional methods of manipulating contact center agents (sometimes referred to as the 'agent leg'), armed with better intelligence and more effective tactics.

In addition to the increasing fraud rate, contact centers are also facing the emergence of new types of fraudsters with different specialties. Specifically, there are fraudsters who specialize in mining IVR data, which is distinct from those who target call center representatives. These IVR fraudsters use the information they gather to bypass security measures and increase their chances of successfully manipulating agents with social engineering or accessing accounts through other channels.

In the past, fraudsters typically worked alone, but today they've started to collaborate and communicate with each other, which has made them a more formidable and effective threat.

Pindrop data reveals that the fraud rate at the agent leg, which had declined in 2020, started to rise back up again in 2022.[8] As a result, the fraud call rate is up by 40% in 2022 and the trend is expected to continue in 2023. Although fraud rates in the agent leg have declined, Pindrop's data shows that high-risk activity in the IVR has increased, with approximately 1% of all IVR calls being moderate or high-risk compared to only 0.15% in the agent leg.[9]

Now more than ever, it's imperative for contact centers to stay vigilant and proactively implement measures to protect themselves against emerging trends in fraud.

[8]Pindrop Labs, analysis of fraud rates at contact center agent leg
[9]Pindrop Labs, analysis of call risk and account risk in the IVR and at agent leg

SECTION 5

9 Emerging Fraud Profiles in 2023

Phishing Fraud

Phishing is a well-known tool used by fraudsters to obtain personal information through email attachments. They typically lure victims to open attachments or click on links and enter personal credentials, which are then sent to the attacker. Call center agents are also targeted, as they may be under pressure to provide customer satisfaction.

Recently, more sophisticated phishing attacks have emerged, leveraging phishing-as-a-service (PhaaS) toolkits that offer greater reach and a higher payoff for attackers. These toolkits enable the crafting of customized phishing kits, managing redirect pages, dynamically generating URLs that host the payloads, and tracking campaign success.[10]

IVR spear-phishing is another version of the attack, where fraudsters use interactive voice response (IVR) systems to validate customer information, such as recent transactions. This information can then be used to conduct fraud through other channels.

Check Fraud

Check fraud, a type of fraud where a fraudster gains access to legitimate checks by stealing them from mailboxes or ordering them from check supply companies, has made a comeback in 2022 after being on the decline for the past 10 years.[11] Attempted check fraud is up over 106% from 2021,[12] and check washing is on the rise in several states, including Illinois, California, New York, New Jersey, and Florida, and is spreading across the country.[13]

In check washing, key portions of the legitimate check are removed, and replaced with fraudulent information. The fraudster then rewrites the check with a higher amount or to a different payee and uses it to withdraw funds or make purchases.

Pindrop has observed that fraudsters are calling into the IVRs to gather balance information on accounts, enabling them to prioritize which checks to target—specifically those that are open and have money in a Demand Deposit Account or DDA.

[10]Hackernews.com, Researchers Warn of New Phishing-as-a-Service Being Used by Cyber Criminals 2022
[11]https://www.jackhenry.com/fintalk/why-is-check-fraud-so-rampant-again-in-the-u.s
[12]https://frankonfraud.com/fraud-trends/check-fraud-is-booming-again-in-a-post-pandemic-us/
[13]https://www.ncja.org/crimeandjusticenews/washing-checks-becoming-major-issue-in-some-states-in-u-s

Imposter Scams

An imposter scam is a straightforward tactic in which a fraudster impersonates someone else to trick their target into giving them money. The key to success is building trust and likeness with the victim. Recent advances in AI have made this type of fraud more prevalent and effective. Imposter scams were the most reported category of fraud in the US, with nearly 40,000 attacks.[14] AI voice-generating software can mimic the tone, pitch, and resonance of a target's voice with as little as 30 seconds of an audio sample. Voice samples are easily accessible from social media and online video sites.

Social Engineering

Fraudsters pose an ongoing threat to call center agents by using social engineering tactics to manipulate them into taking actions that they wouldn't normally take. These attackers use various methods to gain the agent's trust and deceive them into revealing sensitive information, providing access to accounts, or initiating fraudulent transactions. They can pretend to be trusted individuals or organizations to create a sense of urgency, or leverage emotional appeals to exploit vulnerabilities in the agent's judgment. In 2022, Pindrop observed an average of 30% of all call center fraud was committed using this tactic.[15]

Return or Concessions Abuse[16]

E-commerce fraud has been a persistent problem, with fraudsters devising new ways to scam retailers. One such method involves claiming that the purchased item was either never received or arrived empty and requesting a refund while keeping the original item. This type of fraud typically involves fraudsters posing as legitimate customers and contacting the retailer to report the issue.

According to the US National Retail Federation, a major return scam involved a Spanish buyer who stole items and returned boxes filled with dirt to match the weight of the original items, resulting in a loss of $370k for Amazon.[17]

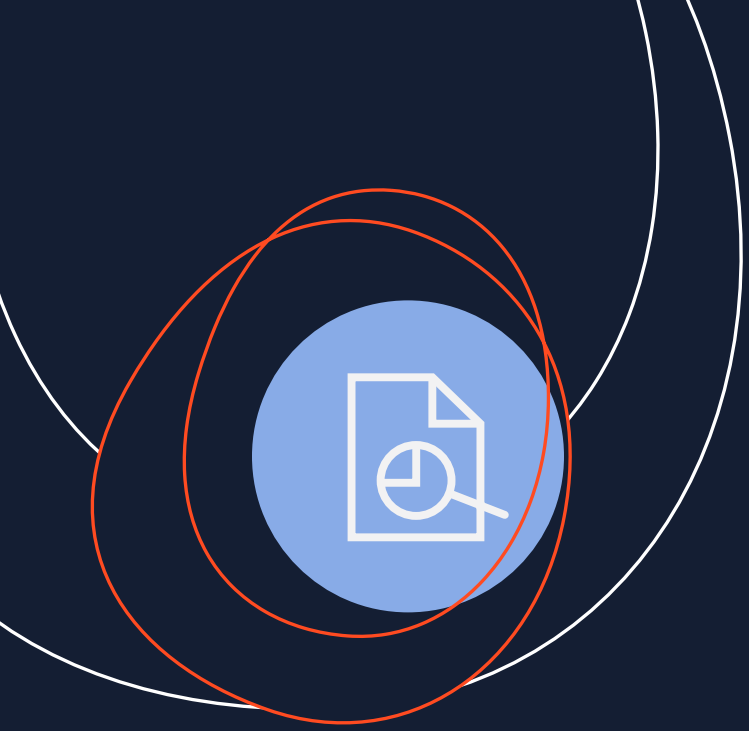
Card Not Present

Card-not-present fraud is when fraudsters use stolen credit card information to carry out unauthorized transactions online or over the phone, without having physical possession of the actual card.

Reconnaissance attempts in the IVR have shown evidence of such fraud attempts. Fraudsters can obtain credit card data by breaching the security mechanisms of credit monitoring agencies, financial institutions, and mobile service providers. They then use this information to test in the IVR and combine it with other acquired information of the user to carry out the final attack. Card-not-present fraud losses reached $8.75B in 2022 and are projected to surpass $10B in 2024, according to Insider Intelligence.[18]

Pindrop's data reveals that 60-65% of fraud post-reconnaissance is carried out using cards (both debit and credit),[19] which may happen outside of the contact center.

[14]https://www.washingtonpost.com/technology/2023/03/05/ai-voice-scam/
[15]Pindrop Labs, fraud data types at the contact center agent leg
[16]https://www.justice.gov/usao-cdca/pr/hacienda-heights-man-admits-bilking-amazon-13-million-refund-scam-and-will-plead-guilty
[17]https://seon.io/resources/how-to-fight-return-fraud/
[18]https://www.insiderintelligence.com/content/card-not-present-fraud-payment
[19]Pindrop Labs



In 2022:

Over 45,000 instances of wire transfer fraud were reported in the US with over $300M in reported fraud losses.[21]

Senior Fraud

Senior fraud is a type of fraud that specifically targets older adults or senior citizens through various financial scams such as investment scams, identity theft, and fake charities, as well as fraudulent telemarketing and mail scams. Fraudsters often use fear, urgency, and pressure tactics to deceive older adults into providing personal information, making purchases, or sending money. In the US, people aged 60 and over account for 34% of all reported fraud losses, with the highest median dollar loss per fraud report being for the age category 80 & over ($1,674), followed by 70-79 ($1,000).[20] These losses are substantially higher than any other category, highlighting the need to protect this vulnerable demographic from ongoing fraud.

Property & Casualty Insurance

Property and casualty insurance fraud involves making false or exaggerated claims for property or casualty insurance benefits. This can occur through arson, staged accidents, fake thefts, or inflating property damage. Fraudsters may also submit false or forged documents, such as medical bills or repair estimates. To avoid detection, they may call businesses directly to make their claims rather than using online submission processes.

ACH (Automatic Clearing House) Fraud

ACH fraud refers to fraudulent activities that include fraudulent payroll or vendor payments or unauthorized electronic transfers, initiated by cybercriminals who have gained access to bank accounts. The perpetrators of ACH fraud often use social engineering or malware to gain unauthorized access to bank accounts and initiate fraudulent transactions. In 2022, there were over 45,000 reported cases of wire transfer fraud in the US, resulting in over $300 million in reported losses.

[20]FTC Consumer Sentinel Databook, 2023
[21]FTC Consumer Sentinel Databook, 2023

SECTION 6

Identifying and Analyzing the Top 3 Types of Fraud[22]

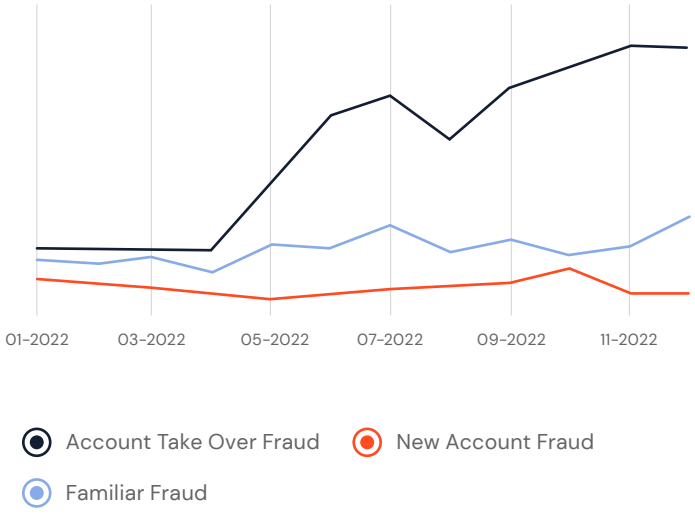
Now that we've identified the fraudulent tactics that pose a risk, we can explore in more detail how and where they take place. To do that we've utilized Pindrop's vantage point as a fraud detection solution provider to identify specific types of fraud reported within our diverse customer base.

Pindrop has classified the different types of frauds detected in our customer base into three distinct groupings that constitute over two-thirds of all the fraud detected by our system.

- Account Takeover Fraud (ATO)
- New Account Fraud
- Familiar Fraud

In 2022, all three types of fraud were observed closely, with ATO being the most prevalent method. However, we observed a significant increase in ATO attempts since May of that year, while the rate of new account fraud and familiar fraud attempts remained stable. The trend of rising ATO attempts persisted throughout the year.

Figure 5:
Fraud Types: Number of Cases for Sample Customer Base



[22]Unless otherwise noted, all data from this section sourced from Pindrop Labs' analysis of all customers using fraud detection solution

Account Takeover Fraud (ATO)

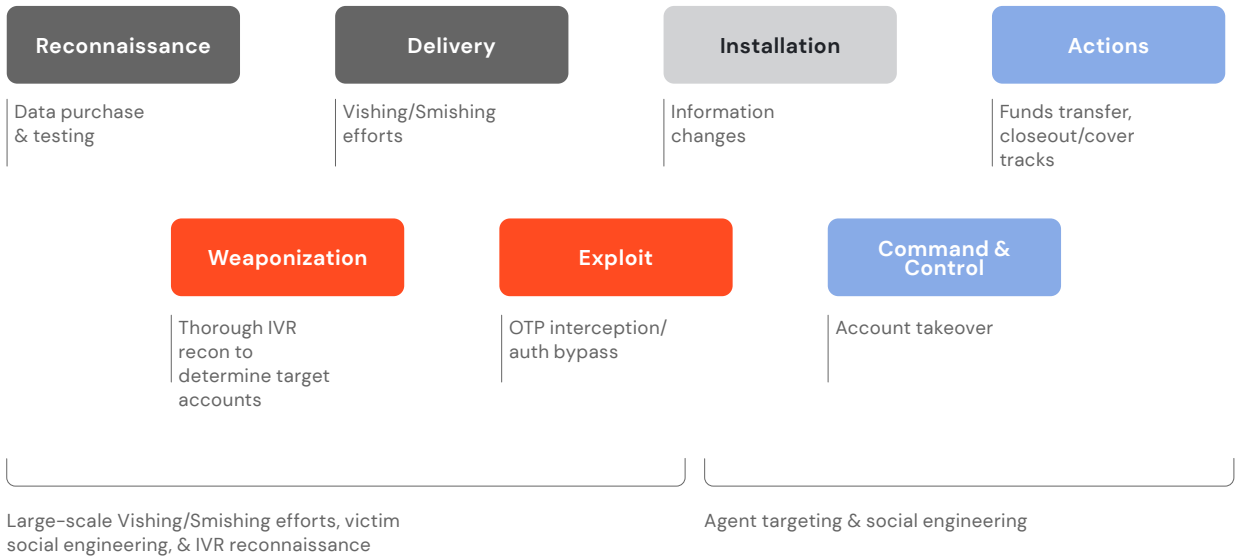
The sharp increase in ATO can be attributed, in part, to the large-scale data breaches and identity thefts that have occurred in the last decade.

ATO is a long-term process that begins when fraudsters gain access to personal information of targeted victims from the dark web. Fraudsters can also extract data from IVR using touch tones or AI to determine PINs, SSN, DOB, address, and more, or through account reconnaissance by checking account balances, transaction history, and transfer status. Additionally, fraudsters use phishing attempts[23] to gather data, bypass OTP and authentication attempts, or even change phone numbers or personal details associated with accounts.

This process can take anywhere from 10 to 120 days before the fraudster gains full control of the victims' accounts, enabling them to initiate transfers of funds and close out the accounts undetected by the contact center or the victim.

While social engineering of contact center agents remains the prevalent method for ATO attempts, phishing attacks are becoming more common. These include fake emails, websites, or SMS messages designed to trick customers into disclosing their personal and banking information.

Figure 6:
The Fraud Process: Security Kill Chain



[23]Splunk, Phishing Scams & Attacks: What To Expect in 2023

New Account Fraud

New account fraud involves opening new or expanded lines of credit using stolen credentials. Amongst our customers, two prevailing types of new account fraud are Application Fraud and Synthetic Fraud.

Application Fraud is when the fraudster uses false or stolen personal information to open a new account with a financial institution such as a bank or credit card company, with the intention of defrauding the institution or its customers.

Whereas, in **Synthetic Fraud**, the perpetrator combines real SSN and fabricated personal information (such as a fake name, address, and DOB) to create a new identity and open a new line of credit with the intention of defrauding a financial institution or its customers.

Familiar Fraud

Familiar fraud poses a unique challenge as the perpetrator is typically known to the victim or is the direct account operator. Types of familiar fraud include:

First Party Fraud is committed by the account holder who provides false information or forges documents to obtain goods or services.

Family Fraud occurs when someone with whom the account holder has a relationship misuses their financial information.

Spousal Fraud involves one spouse committing fraud against the other or against a financial institution where both spouses have accounts.

Authorized User Abuse occurs when authorized users make unauthorized purchases on the victim's credit card without their knowledge.

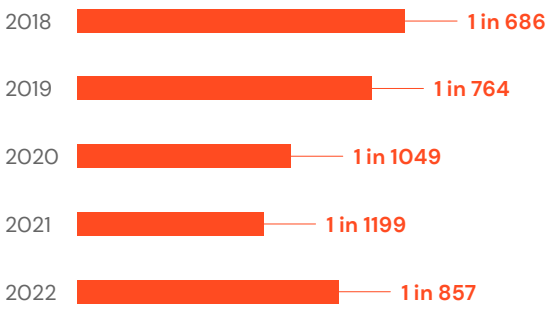
SECTION 7

Analyzing the Rise of Fraud Rates and Trends Across Different Industries

Fraudsters have been actively purchasing personal data of targeted individuals from the dark web to conduct large-scale account reconnaissance activities in the IVR. Through these activities, they can identify high value accounts with maximum payoffs. Vishing and smishing attacks are also employed by fraudsters to take control of accounts or change the account information, providing them with the necessary tools to socially engineer contact center agents into initiating fraudulent transfers. According to PWC's Global Economic Crime and Fraud Survey 2022, fraud rates have increased, with 52% of companies with global annual revenue over $10B reporting fraudulent activities within the last 24 months, and nearly one in five experiencing financial losses of over $50m.[24]

We anticipate that the fraud rate will continue to rise in 2023, reaching pre-pandemic levels of approximately 1 in 700 calls. As of Q4 2022, the fraud rate had already increased to 1 in every 784 calls, indicating the continued impact of economic uncertainty and data breaches on fraudster activities.

Figure 7:
Fraud Rate Trend



Fraud Rates by Verticals[25]

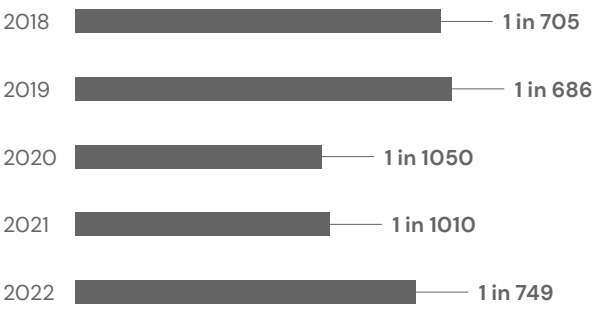
Pindrop's research found that fraud rates in banking and financial institutions follow a similar pattern. Fraud peaked in 2019 at 1 in 686 calls, dropped to 1 in 1050 calls in 2020, and is now returning to 2019 levels as fraudsters return to the contact center. Prepaid businesses have even higher fraud rates, with Pindrop observing rates of 1 in 75 calls for a leading US financial institution, significantly higher than the retail banking arm.

[24]https://www.pwc.com/gx/en/services/forensics/economic-crime-survey.html
[25]Unless otherwise noted, all data from this section is sourced from Pindrop Labs' analysis of all customers using fraud detection solutions

Financial institutions are still optimistic about investing in automation to improve customer experience, despite concerns about a possible recession. The challenge for them is twofold:

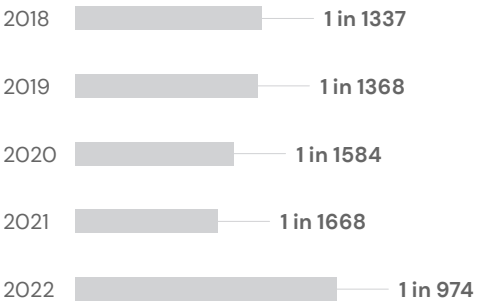
1. Finding the best way to implement better controls to prevent fraudsters from accessing the contact center
2. Ensuring that these controls do not create hurdles for legitimate customers to overcome

Figure 8:
Fraud Rate: Banking



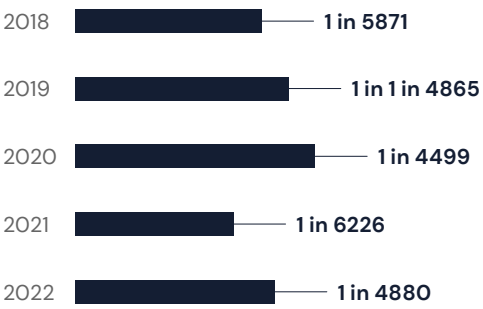
Among Pindrop's credit union clients, call volumes surged in 2020 due to pandemic-related changes, while fraud rates only slightly declined from 1 in 1,368 to 1 in 1,668 calls. However, in 2022, fraud rates jumped over 70% to 1 in 974 calls, the highest level seen in credit unions. This highlights the need for prevention of unauthorized access and account takeovers while balancing member service.

Figure 9:
Fraud Rate: Credit Unions



Fraud is less frequent in insurance but potentially involves larger payouts, especially in life insurance. Fraud rates continued to rise in 2020, reaching about 1 in 4,450 calls, as property/casualty companies saw fake credentials being used during automated claim processes. Fraud rates dropped in 2021 but resumed pre-pandemic levels of 1 in 4,880 calls in 2022.

Figure 10:
Fraud Rate: Insurance



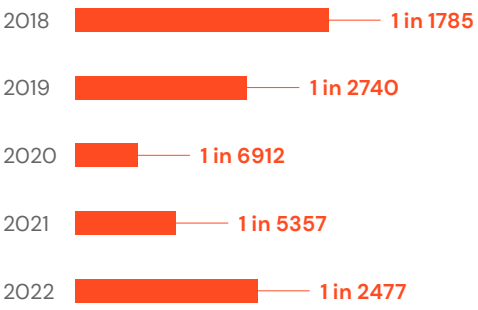
According to a recent Gartner® report,[26] leveraging artificial intelligence (AI) is one of the topmost priorities with insurance companies. Ninety-two percent of executives have deployed or expect to deploy AI at their organizations and fraud detection is the fourth most widely deployed use case after claims processing, customer service, and actuarial pricing. By 2027, fraud detection is expected to be the top area employed across insurers.

[26]Gartner, What to Do With All That Data: The Top Areas Where AI Is Applied in Insurance, December 13, 2022

Brokerage and asset management services are provided by companies such as stock brokers, investment firms, retirement, and wealth management firms that manage billion dollar portfolios. They cater mainly to high-net-worth individuals with significant asset balances. Although fraud attempts on these institutions are infrequent, they are targeted and can involve significantly higher payouts. Fraud rates in brokerage have shown a similar pattern, dropping in 2020 (from 1 in 1,785 to 1 in 6,912) before rising back to pre-pandemic levels of 1 in 2,477 calls.

Figure 11:

Fraud Rate: Brokerage & Asset Management

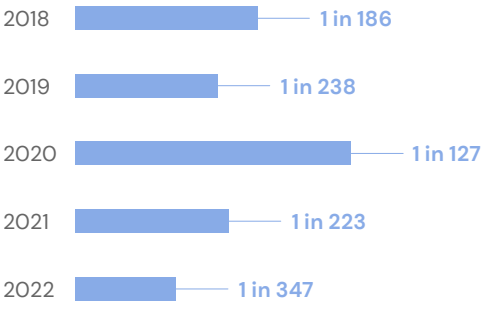


Fraud rates in the retail industry have been especially volatile in the last two years, particularly in contact centers. However, there's been a significant increase in online and e-commerce fraud activity, with fraudsters stealing 3.6% of all e-commerce revenue in 2022, and payment fraud rising by 40% from 2021 to 2022.[27]

Despite the fluctuating trend in fraud rates, retail and telecom stands out as the most fraud-dense verticals we've examined. With a fraud rate of 1 in 347 calls, it's twice as high as the next highest industry (banking) at 1 in 749 calls. Retail is vulnerable to various fraud risks, including return fraud, e-commerce fraud, and debit/credit card fraud.

Figure 12:

Fraud Rate: Retail & Telecom



[27]Sumsub, Annual Identity Fraud Report, Identity fraud doubled in crypto and banking in 2022

SECTION 8

The Complexities of Fraud in Contact Centers

Vishing (Voice Phishing)

Vishing uses phone calls to deceive customers into giving sensitive info. Cases have increased 550% from Q1 2021 to Q1 2022,[28] with the financial sector as the main target.

One example of vishing is when fraudsters pretend to be bank security departments and call customers using a spoofed phone number to trick them into giving away sensitive account details, like PINs. After convincing the customer that the call is legitimate, the fraudsters socially engineer them into providing the information needed to access and defraud their accounts.

Smishing

Smishing uses SMS messages to deceive customers into providing sensitive information. In September 2021, 1.227 million spam texts were sent, compared to 10.89 billion in August 2022.[29]

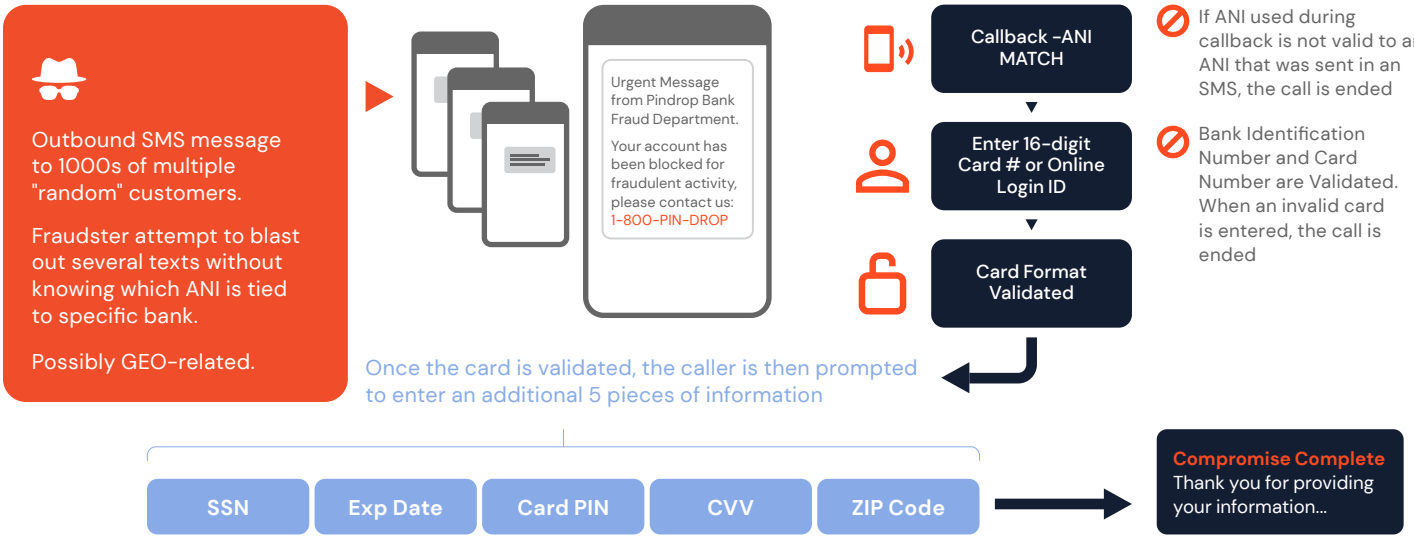
Fraudsters maximize their chances by blasting thousands of texts, hoping for the right target to respond. Once a victim calls back, the fraudster checks if the targeted number is valid. Armed with valid numbers, the fraudster proceeds to gather card numbers and login IDs, then key pieces of info like SSN and zip code to take over the account.

Armed with a collection of valid ANIs (Automatic number identification), the fraudster proceeds to gather the correct card number and login ID. At this stage, the fraudster is equipped to obtain key pieces of information such as the SSN, CVV, and zip code, which would help them get through to the call center agent and take over the account. Ironically, the victims themselves have provided the fraudster with all the data they need.

[28]Helpnetsecurity.com, Vishing cases reach all time high 2022
[29]Slicktext.com: 17 Spam Text Statistics & Spam Text Examples for 2023

Figure 13:

Fraudster in Action: Data Harvesting



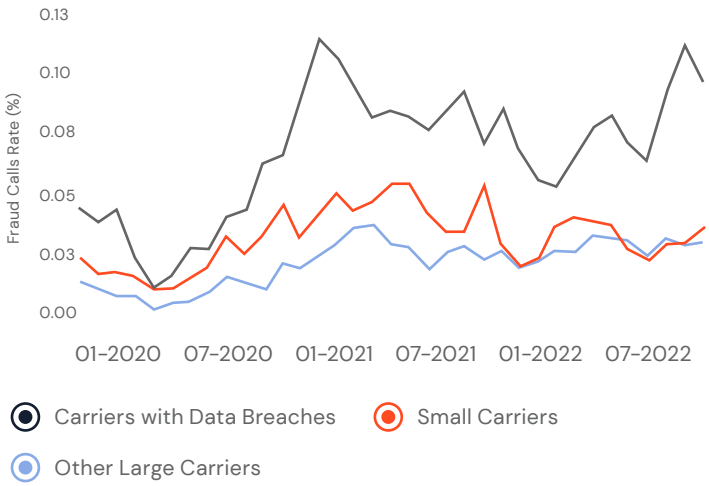
Targeting Carriers[30]

Pindrop not only tracks fraud rates by customer and industry verticals but also by the carrier to identify fraudster behaviors. Since 2018, telecom carriers have suffered large-scale data breaches, resulting in the release of personal information of millions of subscribers on the dark web. Organized crime rings have established storefronts on the dark web and become illicit data vendors, packaging and reselling the data between fraudsters with varying levels of sophistication and depth of detail.

Fraudsters also target the carriers that have suffered data breaches. Although the overall fraud rate has increased for both small and large carriers since mid-2020, we've observed a widening gap between these affected carriers and others in terms of fraud rate, starting in early 2021. The gap continued to widen through 2022, with the average fraud rate for affected carriers being 274% higher than other large carriers and 244% higher than smaller carriers.

Figure 14:

Fraud Rates by Carrier



[30]Pindrop Labs analysis of fraud rates by carriers at the agent leg

IVR Reconnaissance

The average percentage of calls that are handled by the IVR (Interactive Voice Response) system is 33%, covering both large and small contact centers in the US.[31]

In most cases, Pindrop's customers have about 60-80% of their call traffic contained in their IVR system, without ever reaching a live agent. This suggests that at least one third of the contact center traffic, and probably more, never reaches a live agent. Traditionally, businesses have not considered the IVR as a vulnerable point and have therefore not put appropriate measures in place. However, a survey by Forrester Consulting, commissioned by Pindrop, revealed that 76% of fraudsters are using the IVR for account mining or reconnaissance.[32] Shockingly, the same study found that 64% of executives are unaware of how vulnerable the IVR is, posing a daunting security question.

Fraudsters use the IVR to confirm account balances, verify transactions, confirm changes to the account, or even initiate changes. An analysis of 13 organizations across multiple industries conducted by Pindrop showed that there's 10 times more risky activity in the IVR than in the agent leg. Moreover, some type of loss occurred in 1 out of 4 targeted accounts. Looking beyond the numbers, it shows that a large North American bank was the target of fraud on 2,848 accounts with unique IDs. 1,178 accounts or 41% of these accounts were hit for a second time. The repeat fraud rate was highest (1 in 3) within the first 30 days of the initial attack. This is concerning for two reasons:

1. An account targeted once by a fraudster is likely to be hit multiple times within a very short time window.

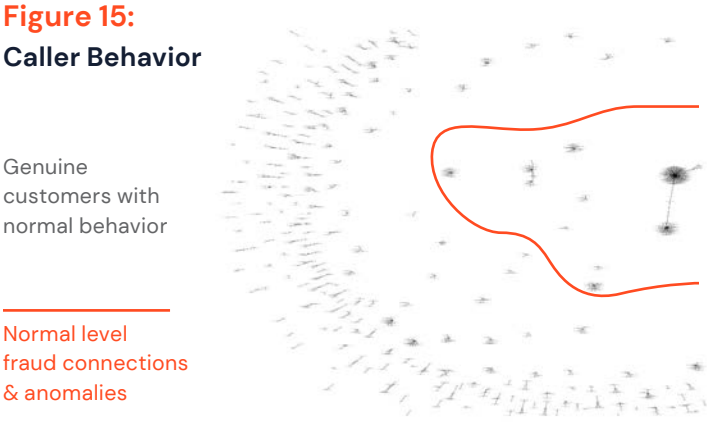
2. The repeat nature indicates the likely presence of multiple fraudsters who share the account information with other attackers who attack the account again.

There are many highly suspicious activities going on in the IVR systems, which tend to fly under the radar until the point where the fraud is actually perpetrated much later in the agent leg. To effectively catch this fraud, we need to be able to go back in the process and weed out the problem at the point of origin.

Data Breaches + Unprotected IVR = Massive Business Risk

When there are no large-scale data breaches, there is usually a clear pattern of fraud activity in the IVR system. The graph below illustrates the behavior of both genuine customers and malicious actors. The majority of the calls show normal behavior, while the fraudulent activity is concentrated in a smaller volume. The fraudsters can be identified through common caller ID and behavioral parameters, making it easier to isolate and address the issue. Unfortunately, with the rise of data breaches, the pattern of fraud activity may not be as clear-cut.

Figure 15:
Caller Behavior



This graph shows a representation of caller behavior, both genuine customers and malicious actors. On one side of the graph, you can see a high number of legitimate calls displaying normal patterns of behavior. On the other side, there is a significant concentration of fraudulent activity that can be linked to one another through shared caller ID/account ID and behavioral characteristics. The anomalies are localized and contained within a relatively smaller activity volume which makes it relatively easier to isolate.

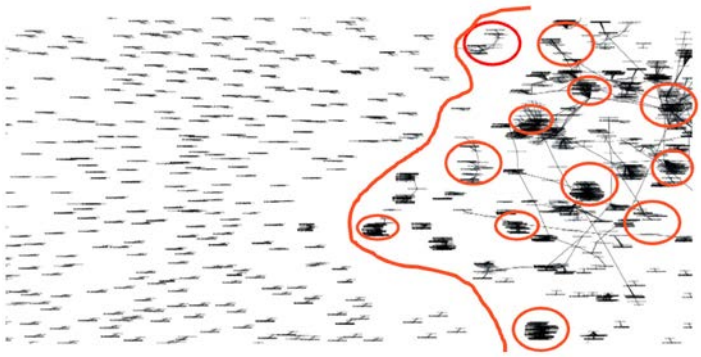
[31]Contact Babel, US Contact Center Decision Makers Guide 2023
[32]Forrester, Reducing IVR Fraud Through Advanced Account Risk Capabilities, 2021

Post Data Breach: A Feeding Frenzy

Figure 16 illustrates the contrast in fraudster activity after a data breach. You'll see the difference from Figure 15, where after the breach there's a much higher level of fraudulent activity on the right side. The behavior of genuine customers remains relatively constant, but the fraudulent activity is significantly increased.

Figure 16:

Fraudster Activity Post Data-breach



Genuine customers with normal behavior

Above normal level fraud connections & anomalies

Fraudulent activity in contact centers has become more complex and widespread, with several bots and fraudsters testing different combinations of caller IDs, accounts, and SSNs to match breached data with active and valuable account targets in the IVR system. This has led to an increase in fraud attempts at the agent leg and higher fraud exposure after a data breach. Traditional fraud detection techniques, which rely on security questions, personal information, and OTPs, are insufficient to handle this level of complexity and scale.

To address this issue, it's necessary to distinguish normal behavior from anomalous behavior. Both fraudulent and genuine activities may show clusters of account-related activity, particularly near the "red line" of risk. A combination of account intelligence and sophisticated behavior analysis, supported by risk engine intelligence, is required to differentiate between fraudulent/bot activities and genuine customers.

Omni-channel Fraud

The phone is just one mode of interaction in a call center, with other channels including email, chat, and web. Fraudulent activity is no longer limited to just the phone channel but can occur across multiple channels in a cross-channel ecosystem.

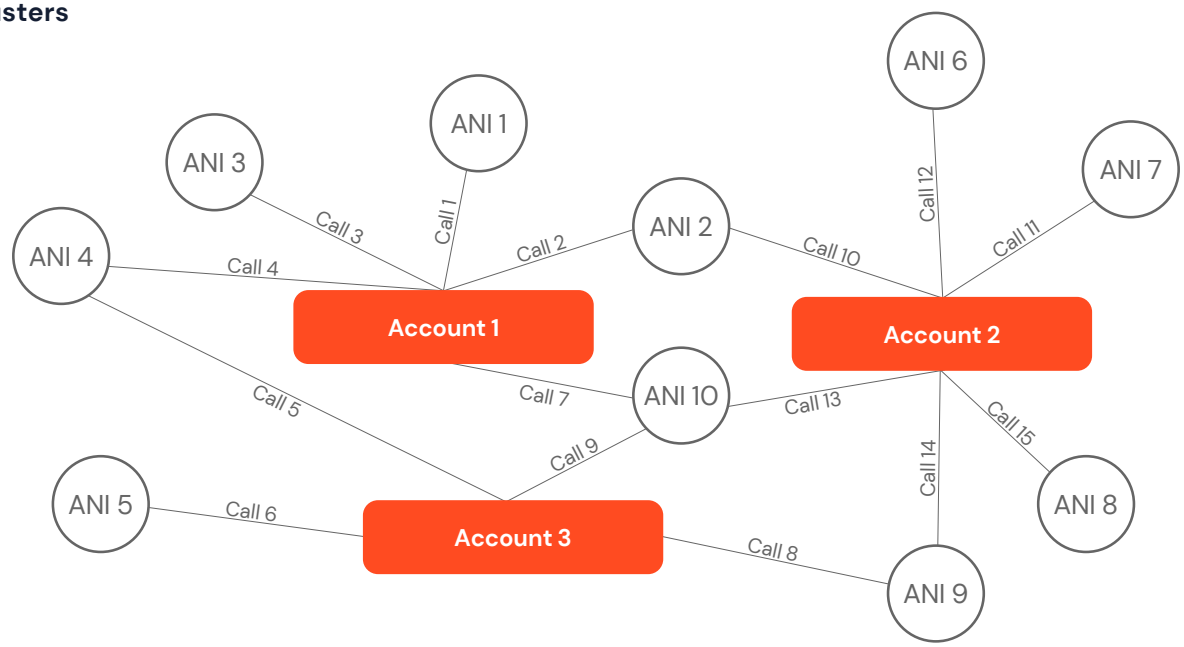
If the IVR system is where the fraud begins, the fraud may be completed in a different setting such as branches or kiosks outside of the contact center. It can be challenging to identify and flag suspicious activity in real-time unless companies track the chain of activities back to the origin of the fraud in the IVR.

Fraud Clusters

In a case study involving a regional bank in North America, Pindrop® used Account Risk Intelligence to identify an active fraud ring in the bank's IVR system.

The fraud cluster consisted of 18 unique phone numbers (ANIs) that made a total of 157 calls to the IVR over a 10-day period. The calls targeted 16 unique account IDs, with 82 of the calls successfully matching to an account and 75 failing to do so. Of the 16 accounts that the fraudsters matched, 40 calls were able to pass authentication in the IVR, allowing the fraudsters to gain access to the accounts they were targeting. Ultimately, seven of these accounts were confirmed to have been subjected to fraud attempts, which were monetized in the credit card channel.

Figure 17:
Fraud Clusters



Thanks to Account Risk Intelligence, the bank was able to detect the fraudulent IVR activity early and monitor the targeted accounts across all channels, ultimately stopping the attack before it could be completed.

The IVR is often the starting point for fraud, which can then spread to other channels. Taking a traditional siloed approach to the enterprise, particularly in the contact center, can be counterproductive. Instead, it's important to implement a continuous and seamless method for tracking risk from its origin to its endpoint. This can be achieved by focusing on protecting the largest or most valuable accounts or attributes through targeted monitoring and risk assessment.

Synthetic Identity

Synthetic identity fraud is a significant and growing problem. According to the Aite Group, synthetic identity fraud for unsecured U.S. credit products is expected to reach $2.42 billion by 2023. The COVID-19 pandemic has also had an impact on synthetic fraud, with research from Socure indicating a sharp rise in synthetic fraud attempts from March to September 2020, which continued to steadily climb through 2022. Many of the synthetic accounts created during this time were used by fraudsters to establish money mule accounts for the movement of funds.[33]

There are two elements of synthetic identity from a contact center fraud perspective:

1 Synthetic Data: Use of a mix of fabricated and real credentials including valid data assembled from multiple identities such as SSNs.

2 Synthetic Voice: AI-generated synthetic voice as well as deepfakes. The recent advancements in AI technology, such as the large language GPT, have enabled fraudsters to create synthetic voices or deepfakes, which is a growing concern in the context of contact center fraud.

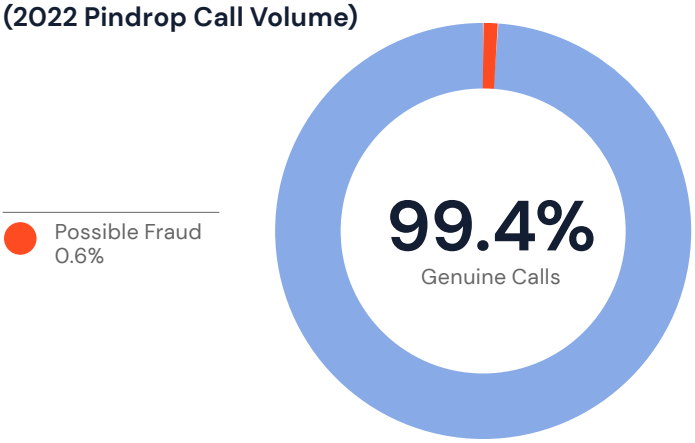
[33]Socure, The State of Synthetic Fraud: Evolution, Trends and How We Will Eradicate it by 2026

SECTION 9

Shifting Consumer Authentication Preferences: Moving Beyond Traditional Methods

Fraud is becoming more prevalent and contact centers are facing increasingly sophisticated attacks. Companies need to determine how to prevent these attacks from succeeding. While there are effective strategies to combat fraud, it's important to acknowledge that fighting it can also negatively impact the consumer experience and carry business risks.

Figure 18:
Proportion of Fraud to Genuine Calls (2022 Pindrop Call Volume)



Source: Pindrop Labs analysis of customer call data

Pindrop's call volume from last year indicates that the majority of fraud was concentrated in just 0.64% of the calls, while 99.4% of calls were from regular consumers or low-risk activity. While it's essential for companies to strengthen their fraud defenses against that small slice of call volume, doing so may negatively impact the overwhelming majority of genuine callers by creating unnecessary friction, delayed service, and call abandonment, ultimately leading to consumer attrition and revenue losses.

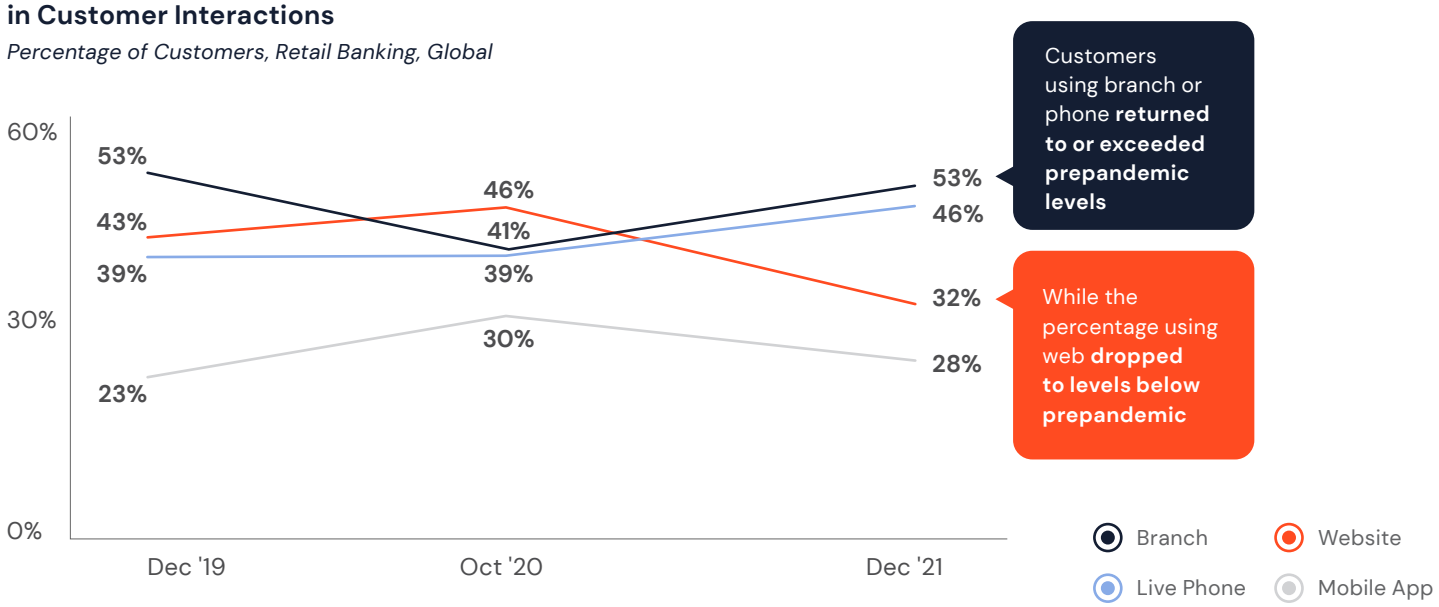
Any effective strategy for preventing fraud must consider both authentication and consumer experience. It's crucial for enterprises to analyze authentication trends and implement solutions that prevent fraud while providing an exceptional authentication experience for their customers. By doing so, companies can safeguard against fraud while maintaining customer satisfaction and loyalty.

Call Center and Voice Remain Crucial to Business Strategy

Figure 19:

Changes in Channels Used in Customer Interactions

Percentage of Customers, Retail Banking, Global



n = 5,437 (Dec 2019); n = 5,502 (Oct 2020); n = 5,807 (Dec 2021) – retail

Source: 2020 Gartner Customer Experience Survey, 2020 COVID-19 Gartner Customer Experience Survey, 2021 Gartner Customer Experience Survey

Gartner® Financial Services Operations report (December 2022) reveals that the proportion of customers using a branch or live phone channels has returned to or exceeded pre-pandemic levels. Prior to the pandemic, most banks were focused on a digital migration and received support from consumers who were hesitant to use phone channels due to long wait times. However, as pandemic restrictions eased, customers seemed to value human support once again. The same Gartner® report[34] also demonstrates that 46% of people prefer to speak to someone on the phone in the service center vs 14% who would rather interact through email.[35] These data points highlight the significance of contact centers and particularly the phone channel in meeting consumer preferences, making consumer experience and authentication in the contact center more important than ever.

Consumer Authentication Preferences are Shifting

The process of authentication is currently at a significant inflection point. Until recently, it's been treated as an afterthought, a necessary but non-strategic step to get customers to the point of service. Contact center agents are often incentivized to prioritize customer satisfaction scores rather than identity verification, leaving them vulnerable to social engineering tactics employed by fraudsters seeking access to customer accounts.

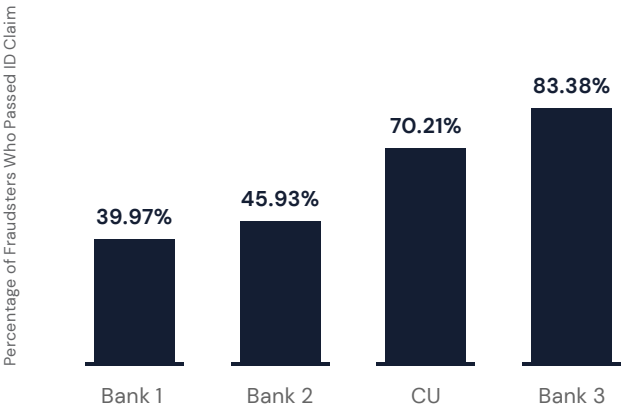
However, both businesses and consumers are now recognizing the value of authentication not only as an important security measure but also as a critical component of the calling experience that must be streamlined and improved.

[34]Gartner, Leadership Vision for 2023: Financial Services Operations, December 6, 2022
[35]n = 5,807 (December 2021) — retail. Q1. Which of the following options did you use to complete your action? Select all that apply. Source: 2022 Gartner Customer Experience Survey

A survey of 3,797 US adults commissioned by Pindrop and conducted by PYMNTS.com found that 57% of respondents who have used advanced ID verification technologies, such as voice recognition, behavior analysis, liveness detection, and other biometric modalities, want to use them again.[36] Among these enthusiastic respondents, 39% said that the use of such technologies for authentication would positively impact their trust in the organization, and 70% said that it would improve their satisfaction level. These results are significant because they challenge the belief that consumers are apathetic about identity verification. Instead, consumers are proactive in seeking a better experience that involves less friction, enhanced security, and greater convenience. They want companies to invest in better technology and are willing to reward them with more trust and better satisfaction ratings.

It's time for companies to take note of what their consumers really want, which is not more passwords, knowledge-based questions, or one time passwords (OTPs).

Figure 20:
Fraudsters Passing KBAs at Worringly High Rates



Source: Pindrop Labs analysis of KBA response rates for a sample of US financial institutions

Reexamining the role of Knowledge-Based Authentication (KBAs)

Knowledge Based Authentication questions, or KBAs, are not effective in preventing fraud. In fact, they can be a helpful tool for fraudsters. The numerous data breaches in recent years have provided fraudsters with enough critical information to impersonate genuine customers. An analysis of four financial institutions revealed that fraudsters are skilled at answering KBAs. Across all institutions evaluated, fraudsters had a high success rate of passing identity verification processes. This indicates that fraudsters have a good understanding of the typical identity verification processes used by financial institutions and are equipped with the answers to the security questions that institutions commonly ask.

Both Knowledge Based Authentication questions (KBAs) and One Time Passwords (OTP) are vulnerable to fraudsters. Gartner® reports that the increase in phishing and similar attacks against phone-as-a-token authentication methods, including mobile push, as well as legacy OTP tokens, is one of the drivers for Fast Identity Online (FIDO) and the imperative to use phishing-resistant multi-factor authentication (MFA)[37]. In fact, a study commissioned by Pindrop and conducted by Aite - Novarica found an example of a fraudster who cleverly manipulated both the customer and the financial institution into intercepting the OTP, which was then used to gain access to the account.

The traditional security model based on KBA questions and OTPs is being challenged by the ease with which fraudsters can manipulate these systems. However, the downside of this model is also its impact on genuine customers. Remembering answers to KBA questions and passwords can be difficult for legitimate users, while fraudsters can easily obtain this information. Moreover, customers may face long wait times and multiple questions during authentication processes, leading to frustration and a reliance on OTPs or second-factor authentication.

[36]Consumer Authentication Experiences: How to Achieve Friction-Free Customer Care
[37]Gartner, Hype CycleTM for Digital Identity, 2022, July 25, 2022

Pindrop's analysis of call data of a leading North American financial institution reveals that 81% of the callers have a prior history with the bank. This means that the majority of callers are "repeat callers" who may or may not have previously enrolled profiles with the company. However, repeatedly using time-consuming KBAs and OTPs to authenticate these callers creates a lot of friction, which negatively impacts the caller experience. Additionally, using KBAs incurs a cost burden for companies that is neither productive nor secure, as fraudsters can exploit them.

A study of 26 Pindrop customers who switched from KBAs to multifactor authentication in their identity verification process saved a combined value of $4.3M per month and reduced average handle time by 3% to 27%. This underscores the significant benefits that companies can gain by adopting authentication methods that are more secure and user-friendly. It improves the customer experience, reduces costs, and enhances security by minimizing the opportunities for fraudsters to exploit vulnerabilities in the authentication process.

Figure 21:
Business and Financial Value of KBA Removal[38]

KBAs Removed	Average Handle Time Reduction	Cost per Call Savings
1–2	13–25 seconds	$0.25 - 0.50 per call
3	34–44 seconds	$0.68 - 0.75
4 or more	50–75 seconds	$1.00 - 1.50

[38]Pindrop Labs analysis of customer call data, KBA reduction and cost savings

SECTION 10

Fraud Prevention Strategies: Enhancing Security and Customer Experience

Strategy 1: Bet on the Cloud

The transition to cloud technology has been in progress for several years, with both Contact Center as a Service (CCaaS) and Communications Platform as a Service (CPaaS) experiencing significant growth across multiple industries, particularly in financial services. Contact centers have shifted from on-premises infrastructure to private and then public cloud. In 2022, companies showed remarkable commitment to their cloud transition, despite economic challenges. On-premises based delivery units shipped for telephony equipment in North America declined by 22% compared to 8% decline in 2021, while cloud-based delivery units continued to grow albeit at a slower pace seen in past years.[39] According to a Gartner®add Press Release, worldwide end-user spending on public cloud services is forecast to grow 20.7% to total $591.8 billion in 2023, up from $490.3 billion in 2022.[40]

The cloud offers not only economic and operational advantages, but also benefits in terms of fraud detection, particularly for contact centers. With the cloud, there's more effective use of a Consortium, a centralized database of confirmed fraudster data acquired from all customers, and carrier signaling. Cloud technology also allows for better audio and voice extraction. Unlike on-prem solutions, cloud capabilities are not localized and can be shared across geographies and environments. Cloud models provide a faster and more consistent path towards upgrades, as well as the ability to quickly deploy new fraud detection models across multiple regions, lines of business, and channels. This points to a more efficient fraud detection framework, not just for catching more fraud but also for improving the effectiveness of fraud investigation processes.

[39]Gartner, Forecast Analysis, Unified Communications Forecast 4Q2022, October 10, 2022
[40]Gartner Press release, Gartner Forecasts Worldwide Public Cloud End-User Spending to Reach Nearly $600 Billion in 2023, October 31, 2022

Strategy 2: The Importance of Leveraging Multiple Authentication Factors and Risk Signals

While the cloud has simplified some of the infrastructural and workflow complexity, the consumer experience remains complex. Demographics, locations, service expectations, and personal preferences all play a role in determining what service outcomes consumers expect from contact centers. While some may prefer self-service options like IVR, others may be more comfortable speaking to agents. Additionally, some consumers may not want to use their voice for authentication, while others may prefer it as their preferred mode of identification. The same applies to fraudsters, whose methods range from caller ID spoofing and IVR mining to sophisticated voice synthesis attacks.

Contact centers need to be prepared to address all of these scenarios, not just from a consumer experience perspective, but also to create an effective defense against fraud. Relying on a single tool, such as security questions or voice authentication, can shut out a large section of consumers from getting the experience they deserve and create gaps in the security of the contact center and the enterprise as a whole.

The answer lies in leveraging multiple factors, not just for authentication but also for fraud detection. Implementing multiple factors involves a specific strategy that ensures organizations utilize various tools at their disposal at the right time and with the appropriate context to optimize the consumer experience while reducing the risk of fraud with less operational burden on the organization. By continuously implementing multi-factor fraud detection and authentication measures, contact centers can maintain security while delivering a positive consumer experience.

Top 5 Techniques for Multi-Factor Fraud Detection and Authentication

Enable voice where available: Contact centers should capture voice samples securely and detect anomalous voices where possible. This helps authenticate callers and reduce KBA burden.

Use carrier metadata for lower risk calls: Analyzing carrier signals can identify risk and weed out known fraudsters. This reduces the burden on live agents and improves accuracy.

Analyze behavior signals: IVR and agent leg can provide valuable behavioral patterns to distinguish between legitimate and high-risk callers. Combining this with voice and carrier signaling improves accuracy and speed.

Consider device profile: Phone data such as keypress patterns and background noise can create a unique profile for authentication. Combine this with voice and carrier metadata.

Ensure continuous coverage: Use machine learning to switch between multiple authentication factors in real-time. Create a robust risk database for continuous call coverage and optimization.

Strategy 3: Empowering Your Fraud Detection Process with Custom Attributes

Detecting fraud is a challenging task for fraud investigation teams who handle call center fraud cases. With an average US contact center receiving around 1 million calls per year,[41] even if a small fraction (5%) is flagged as high risk, it results in 38,000 fraud cases that need to be investigated and disposed of by a small team of analysts. The task becomes even more challenging for smaller contact centers without dedicated fraud investigators.

Prioritizing high fraud exposure events targeting high-value accounts and large insurance policies is crucial to optimize the limited time and resources of fraud investigation teams.

To solve this problem, investigators need a framework of custom data attributes, allowing for enhanced analysis and relevant context. This framework comprises two types of attributes:

- Attributes related to a fraud case
- Attributes related to an account

By defining custom data attributes, institutions can prioritize fraud attacks and focus on the ones that pose the greatest risk to their enterprise or consumers. Predefined attributes, such as the caller's account state, ANI verification, and fraud attack details, along with the ability to create custom attributes, enable investigators to optimize fraud investigation operations and achieve a high ROI.

Strategy 4: Leverage the Collaboration of Authentication and Detection Processes

Both a robust, multi-factor authentication solution and an effective fraud detection solution are mutually beneficial. The authentication solution provides actionable insights to detect more fraud, while the fraud detection solution stops fraudsters from infiltrating the enrollment process.

To achieve optimal results, it's crucial to ensure that these systems communicate and collaborate effectively.

Example 1: One Plus One > Two

Pindrop® Protect and Pindrop® Passport are integral parts of the Pindrop® Platform, with the former serving as a fraud detection solution and the latter as a multi-factor authentication solution. While Pindrop® Protect is capable of detecting a significant amount of fraud on its own, combining it with Pindrop® Passport and utilizing the authentication feedback and risk signals from both systems results in a more effective fraud detection platform. For instance, at a prominent US financial institution, the combined use of voice mismatch detection and authentication policies with the fraud detection system resulted in the identification of 9% more fraud cases compared to using the standalone fraud detection system. Similarly, combining voice authentication with the fraud detection system led to a 35% reduction in fraud case alerts, leading to a more cost-effective case investigation process.[42]

Example 2: Improved Authentication Security

Pindrop recognizes the importance of risk in the authentication process. Simply getting a positive match is not enough; it's equally important to obtain a low probability of risk to ensure a safe and effective authentication process. When risk feedback is integrated into a multi-factor authentication engine, the resulting authentication assessment provides a higher level of confidence in the authentication score.

With a highly secure authentication score, call centers can authenticate more calls or allow more transactions for authenticated users with less concern about risk implications. This is particularly effective in the IVR, where there's a balance between risky activity and genuine users seeking a fast, low-friction response.

[41]Contact Babel, US Contact Centers 2021-25 State of the Industry
[42]Pindrop Labs case study of a leading US life insurer

By using a combination of multiple factors (such as carrier metadata, behavior, or voice) for authenticating callers in the IVR and utilizing risk feedback in the form of call spoof or account reconnaissance risk, the call center gains more flexibility and assurance to trust incoming calls. With this higher level of trust, the contact center can develop flexible policies for authenticating callers at different levels of authorization, allowing them to perform more functions in the IVR without reaching agents.

For a leading US Life and Health Insurer, Pindrop was able to increase the IVR authentication by 15% and improve the IVR containment by 10%, resulting in tangible cost savings and consumer experience benefits without compromising on security posture.

Example 3: Voice Mismatch Detection—A Failed Voice Match Tells You a Lot More Than You Think

Voice mismatch occurs when a caller's voice has a low match against an enrolled profile. While treating it as an indication of risk is traditional and valid, using it as a standalone factor and viewing it in isolation can lead to missing the bigger picture and generating a large volume of false alerts.

The recommended approach is to use voice mismatch information in conjunction with authentication policies and voice clusters. Contact centers can leverage "do not authenticate" policies for real-time authentication treatment if a different voice is not expected against a given identity. Alternatively, they could combine the failed match with other risk factors to create alerts for post-call analysis. In cases where multiple voices are expected against an identity, such as joint account holders, voice clustering information should be used to ensure all account holders experience expedited frictionless authentication.

As the use of synthetic voices, presentation attacks, and deepfakes increases, accurately capturing voice signals and leveraging contextual analysis becomes ever more important. Doing so could have significant implications not only for keeping fraudsters out but also for ensuring genuine customers aren't subject to delays or a poor consumer experience.

SECTION 11

Emerging Fraud Trends to Watch Out for in 2023

Fraudsters Will Continue to Exploit the IVR

Pindrop has received direct feedback from our clients, indicating that fraudsters are increasingly targeting "self service" channels provided to consumers. As a result, many of our clients are introducing more self service options in order to automate processes and reduce costs, despite the challenge of staffing. However, the ease of self service also provides a new opportunity for fraudsters to exploit it.

To investigate this trend, we analyzed and graphed the activity of fraudsters in the Interactive Voice Response (IVR) system. The results revealed a significant increase in fraudulent activity, which illustrated how fraud starts and spreads across the enterprise. Once fraudsters acquire a list of data from the dark web, their first step is to attempt to validate that data in the IVR. These lists are often sold to multiple fraudsters who simultaneously act upon them, creating a pattern of interconnectedness.

In the future, we anticipate seeing more concerted attacks that are fueled by data breaches and networks of interconnected fraud activities. Fraudsters may work together in teams to build out the reconnaissance process and create execution networks across different parts of the organization.

The Kidney Beans

This graph shows two groups of fraudsters and bots conducting reconnaissance on a set of accounts in the center. The density at the center represents fraudulent profiles that Pindrop's models have identified. As the attack progresses, the account data is passed from one fraudster to another, resulting in an increase in fraudulent activity. The graph highlights the need for organizations to implement effective fraud prevention measures.

Figure 22:
Kidney Beans: Fraudsters Performing Simultaneous Reconnaissance

The Tricycle

Figure 23:
Fraudsters Race to Perform Reconnaissance

In this graph, a new group of fraudsters is visible at the top, and more fraudulent profiles are emerging. These fraudsters are in a race to perform reconnaissance, get authenticated in the IVR, and move to the execution phase. They've identified key accounts and characteristics, and are working to break into them.

At this stage, Pindrop's multi-factor fraud detection engines and account monitoring systems have already begun to identify suspicious activity and build a fraudster profile that can be tracked across the enterprise. This enables the organization to take action and prevent further fraudulent activity.

The Spiderweb

Fraudsters have now spent more time on reconnaissance and have identified not only which accounts to focus on but also how to target them. They are now in the execution phase, working to build their "execution networks" and determine the best strategy to exfiltrate money from the targeted accounts.

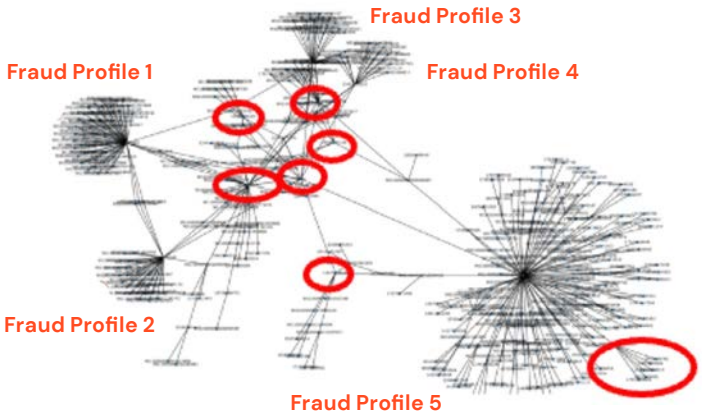
Figure 24:
Fraudsters Building Their Networks

Red circles indicate confirmed fraud detected

The Dandelion Field

The attack has entered the monetization phase, with the fraudsters understanding the account value and how to monetize the attack. They may sell account data to another perpetrator specializing in Account Takeover (ATO) or move the attack to a different channel with a card-not-present tactic. As a result, there are fewer fraud densities but more branches as specialist fraudsters handle different accounts. The reds highlight clear fraudster profiles simultaneously active in multiple account clusters.

Figure 25:
Fraudsters Monetizing Their Attack



It's important to note that a single fraudster is not an expert at all three stages of the process - reconnaissance, execution, and monetization. Multiple fraudsters with different expertise work together in mutual interconnectedness to perpetrate these attacks. Only a comprehensive account monitoring strategy, along with reconnaissance monitoring, behavioral risk analysis, and pattern recognition engines, can help detect and prevent these attacks.

Graph algorithms reveal a fascinating and detailed picture of how fraud starts, evolves and expands over time in the IVR and then across the company. A key trend for this year is the evolution of fraud tactics from linear call-based attacks to complex, concerted, and specialized campaigns across multiple channels, utilizing sophisticated bots, tools, and data-driven tactics.

Generative AI will Fuel Deepfakes & Synthetic Voice

Generative Artificial Intelligence (AI) that can not only analyze but also create new content is a major technological breakthrough. ChatGPT, introduced by OpenAI, is one of the most famous examples of this trend. However, the underlying idea of leveraging fast-learning AI models to create synthetic audio and content is already having far-reaching consequences in the world of fraud.

While synthetic voices and deepfake audio have existed and been used for fraudulent attacks in the past, they've become more potent due to the ability to pair them with smart scripts and conversational speech. A well-known recent example of this tactic was the demonstration by Do-Not-Pay, a legal services chatbot, which used a combination of the GPT-J causal language model with Resemble.ai's synthetic voice and their own script model to create a very realistic chatbot that successfully negotiated a refund from Wells Fargo bank. Another example is Vice.com, which used a synthetically generated voice with tools from ElevenLabs to utter a fixed passphrase "My Voice is My Password" to get past the voice authentication system at Lloyds Bank.

Although synthetic audio is not yet pervasively used by fraudsters, it could become part of their arsenal, especially in combination with breached data and the ability to perform IVR reconnaissance. Companies need to be able to detect voice liveness in sync with automatic speech recognition (ASR) and audio analytics to determine the speaker's environment and contextual audio in order to prevent synthetic voices, pitch manipulation, and replay attacks.

To prevent synthetic voices, as well as pitch manipulation and replay attacks, companies must be capable of detecting voice liveness through automatic speech recognition (ASR) and audio analytics that determine the speaker's environment and contextual audio.

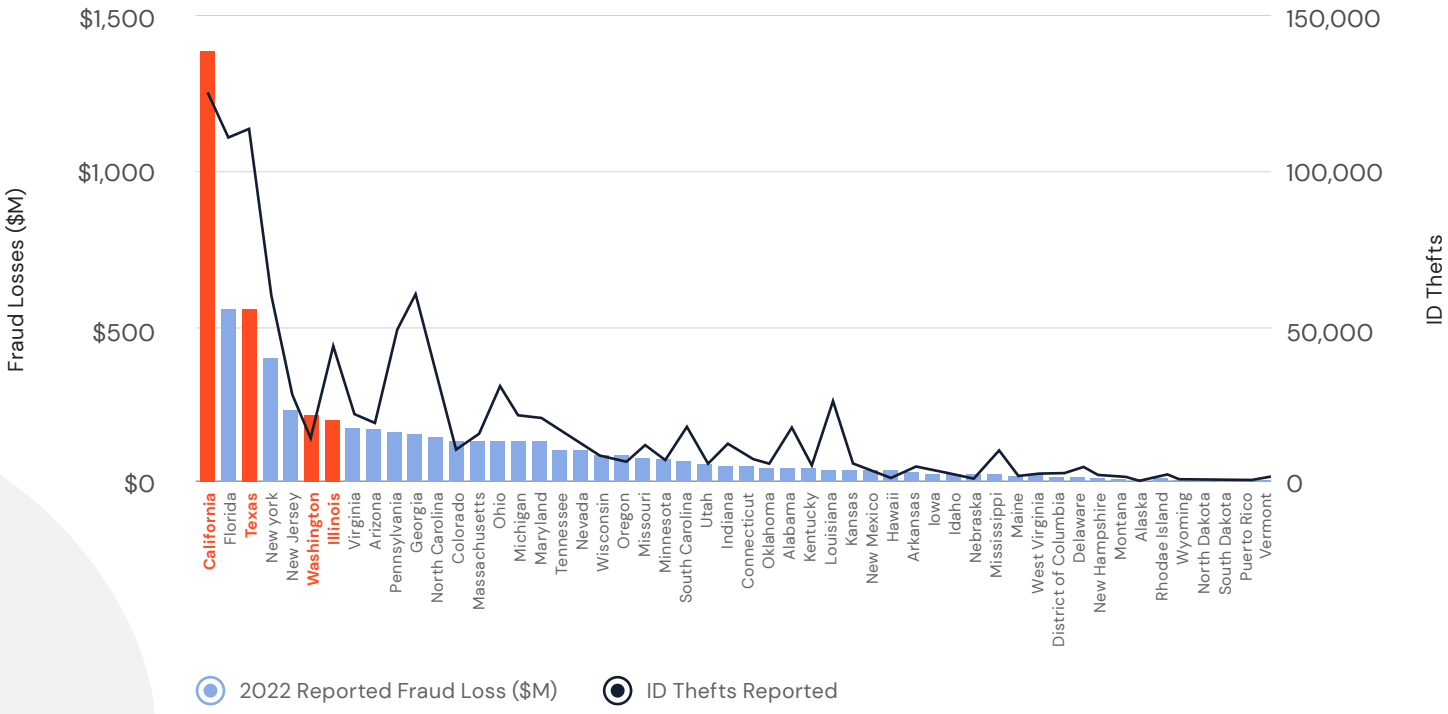
Privacy is Critical - How to Balance it Against Safety?

People care about privacy, especially anything that involves giving anyone access to personal information, including but not limited to biometrics. Surveys show that people are willing to act (i.e., switch companies) over data sharing policies.[43]

Laws regulating personal information have been enacted in the US at State levels, including in Washington, Nevada, Virginia, Connecticut, Colorado, Utah, California, Texas, Illinois and other States also have similar privacy bills in various legislative stages. Regardless of which State a company is located in, these state laws are drafted to protect the residents of that state. While these privacy laws aim to ensure the safety and privacy of consumers by placing conditions and restrictions on the access, use and exchange of personal information, fraudsters appear to be capitalizing on the unintended consequences of real-world application of these laws.

Figure 26:

Reported Fraud Loss & ID Theft by State



Source: Federal Trade Commission, Consumer Sentinel Network Data Book, 2023

[43]Cisco Cybersecurity Series 2019, Data Privacy, November 2019

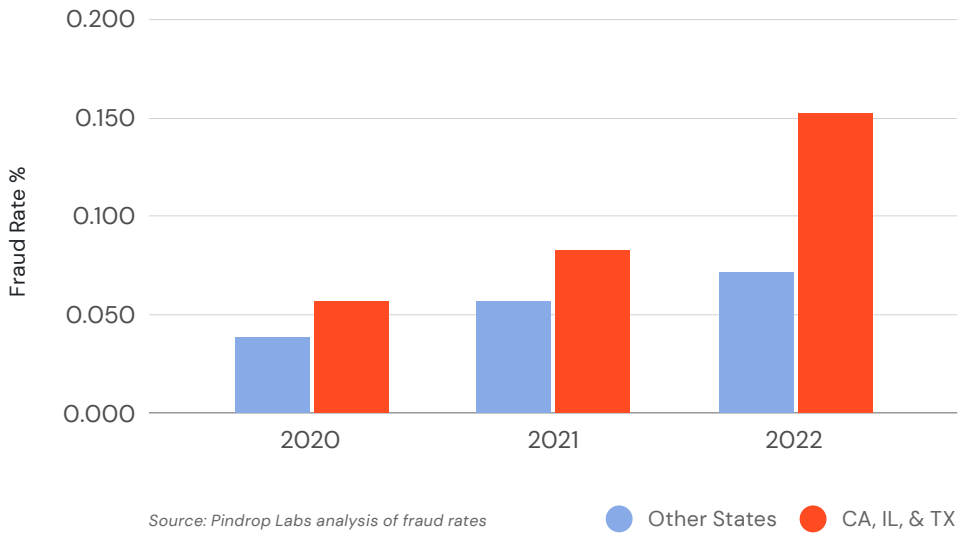
Looking at the chart above (figure 26) from the FTC Consumer Sentinel Databook, 2023, in terms of fraud losses reported, the States of California, Texas, Illinois, and Washington, which all have privacy laws that include enhanced restrictions on use of biometrics, are ranked in the top 10 where residents suffer these fraud losses. These States contribute to 36% of all fraud loss reported in the US as per the FTC.[44] The same report identifies California, Texas, and Illinois as also one of the highest in terms of ID thefts reported.

Amongst banking customers of Pindrop (figure 27), we see an interesting pattern emerge. Comparing the fraud rate in California, Illinois, and Texas vs all the other States combined, there is a clear widening of the gap between the two groups from 2020 onwards. In 2020 the combined fraud rate in California, Illinois, and Texas was 0.06% which was close to 0.04% combined fraud rate for all other States. However the gap between the two groups has widened considerably to 0.15% vs 0.07% respectively by 2022 which means that fraud is 2x more likely in those three States compared to all the other States.[45]

There is significant fraud activity originating in these three States resulting in substantial losses, and higher incidences of identity theft. We are keeping a close eye on this trend in 2023 and going forward.

Privacy laws are crucial and lawmakers need to make every possible attempt to protect consumers from unwanted use of their personal information. However, both legislators and regulators also need to consider how these laws may be used by fraudsters to attack and harm the same consumers the laws aim to protect. The human voice remains a vital factor that can be leveraged for purposes of fraud detection. However, as more states consider bills regulating voice without notable security or fraud-prevention exemptions, companies will rely on other factors such as behavior patterns, carrier signal data or risk feedback to assist in fraud detection, though with limited efficacy.

Figure 27:
Fraud Rate in Banking with Special Requirement States



Source: Pindrop Labs analysis of fraud rates

[44]FTC Consumer Sentinel Databook, 2023
[45]Pindrop Labs analysis of origination of call fraud rates by state

SECTION 12

Conclusion: The Most Critical Focus Areas to Combat Fraud in 2023

Early 2023 Data Breaches Raise Concerns for the Year Ahead. Central banks worldwide are currently holding interest rates and tightening fiscal spending. Meanwhile, ChatGPT is gaining popularity, with both regular individuals and fraudsters getting innovative with it. Recent reports indicate the emergence of new deepfake and synthetic audio attacks. Fraudsters are equipped with sophisticated technologies that enable them to execute smishing attacks, harvest data from the IVR, and collaborate with other fraudsters to treat the entire organization as a fraud surface.

Organizations are making the right investments in cloud technology, security enhancements, automation, and AI. However, a better understanding of the interconnected nature of fraud is needed. It's not the hundred different calls or interactions that pose a risk, but the one account they all target that poses a significant risk.

It's imperative for businesses to adopt a multi-dimensional approach to fraud prevention in order to effectively identify and prevent fraudulent activity. Pindrop is committed to providing organizations with advanced solutions and expertise to effectively combat fraud and protect their customers.

Pindrop helps contact centers detect fraud attempts throughout their organization by analyzing risk on live calls and customer accounts providing added protection against fraud attempts.

Pindrop solutions leverage real-time risk analysis for all inbound calls and monitor the contact center as well as the IVR and can help alert on at-risk customer accounts that show subtle signals of account takeover. Its precise voice identification technology recognizes unique identifiers within the human voice that can enable its customers to prevent more fraud and deliver exceptional customer experiences in call centers, obtain information from smart devices and even activate cars. A privately held company, Pindrop is venture-backed by Andreessen Horowitz, Citi Ventures, Felicis Ventures, CapitalG, GV, IVP, and Vitruvian Partners. Since its inception, Pindrop has analyzed more than 5 billion voice utterances, detected over 3 million fraud calls, and saved our customers more than 2 billion dollars and counting.
Visit pindrop.com for more information.

Follow us

Pindrop @PindropSec @Pindrop @Pindrophq

pindrop.com