Pindrop®

2025

Voice Intelligence and Security Report

TABLE OF CONTENTS

Navigate the fraud story

CHAT WITH AN EXPERT

Introduction

State of the Industry

Security Landscape

Fraud by Vertical

Authentication Landscape

2025 Forecast

Fighting Fraud in an AI-First World

Conclusion

Understanding the landscape

The security question is no longer only *"Are you who you say you are?"*—now it's also *"Are you even human?"*

As recession fears grow and economic pressure intensifies, organizations are being forced to operate leaner than ever. At the same time, they're contending with a parallel crisis: a collapse in trust across digital and voice interactions, fueled by the rapid rise of generative AI (Gen AI). These two forces aren't happening in isolation—they're converging, compounding risk, and stretching security teams to their limits. Gen AI isn't just changing how we work—it's destabilizing long-held assumptions about identity, authenticity, and intent. In this dual-threat environment, efficiency cannot come at the expense of security. The ability to detect deepfakes at speed and scale is now mission-critical, both for stopping a new wave of AI-powered fraud and for safeguarding customer confidence in a world where the line between real and synthetic is rapidly disappearing.

The pace of change is staggering. In early 2023, synthetic voice fraud appeared in isolated bursts. Now, it's a flood of AI-powered deception, surging across industries and eroding trust in real time. In just one year, the rate of deepfake attacks has surged by more than 1,300%, up from one every two days to seven per day.[1] And with every new model released, the gap between what's real and what's generated continues to shrink.

Gen AI is no longer on the horizon. It's here, accelerating fast, reshaping industries, and redefining risk in real time. As macroeconomic pressures force organizations to do more with less, the rapid democratization of Gen AI is proving to be both a game-changer and a threat multiplier. With training costs plummeting and open-source tools readily available, highly sophisticated AI capabilities are now accessible to anyone, including fraudsters. According to Deloitte, Gen AI could help push fraud losses to $40 billion in the U.S. by 2027—more than tripling since 2023.[2]

> Gen AI could help push **fraud losses to $40 billion** in the U.S. by 2027—more than **tripling since 2023**.[2]

The scale and sophistication of AI-driven attacks are now directly impacting enterprise authentication and customer service. Voice remains a critical pillar of secure authentication —especially when paired with deepfake detection as part of a layered, multifactor approach. But legacy systems are increasingly vulnerable to AI-generated impersonation. To address the growing risk of cross-channel voice attacks, organizations should urgently reassess their authentication strategy and adopt platforms that integrate advanced voice biometrics and deepfake detection into a unified, real-time defense.

[1] Pindrop analysis of non-live calls and fraud data from more than 1.2 B calls in 2024 and 2023
[2] Deloitte, Deepfake Banking Fraud: Risk on the Rise, Financial Services Industry Predictions, 2024

CHAT WITH AN EXPERT

Introduction

State of the Industry

Security Landscape

Fraud by Vertical

Authentication Landscape

2025 Forecast

Fighting Fraud in an AI-First World

Conclusion

Deepfakes are becoming more **‘human’**

In mid-2023, Pindrop raised the alarm about the emergence of sophisticated deepfake threats. Before then, the limited capabilities of existing text-to-speech (TTS) engines and the robotic nature of synthetic voices and speech patterns made deepfakes relatively easy to detect.

ChatGPT, which had been recently launched, disrupted the landscape of how speech could be “generated” and made synthetic voices sound more human-like. Today, we have witnessed an explosion of synthetic audio creation and Gen AI-driven TTS tools that create a likeness that is indistinguishable from reality. In other words, they push deepfakes across the uncanny valley.

As synthetic speech becomes nearly indistinguishable from real voices, voice-based attacks are escalating. But voice authentication isn’t obsolete—it’s more critical than ever. The key is adapting: today’s solutions must detect deepfakes through advanced signal analysis and behavioral cues that go beyond traditional voice matching. Voice remains a powerful biometric—unique, dynamic, and difficult to replicate in real time. When combined with multifactor risk signals, it becomes a formidable defense against even the most convincing deepfakes.

3 key forces behind the growing speed and sophistication of deepfakes

1. The use of automated bots

Previously, speech generation tools had a 4-7 second delay between input and synthetic voice output. Today, large language models (LLMs) have reduced that delay to near real-time. This makes it increasingly difficult to distinguish synthetic voices from real ones. To counter this, Pindrop is training our deepfake detection system on commercial and open-source AI models, allowing it to detect not only synthetic speech but also identify the specific AI model or LLM behind it.

2. “Emotional-sounding” AI

Advances in synthetic speech have enabled TTS voices to convey emotions like joy, anger, empathy, and sadness. AI models can now learn and imitate emotional tones from human speech, making these synthetic voices even more convincing. To stay ahead, Pindrop is continually expanding our liveness detection training dataset to recognize the subtle artifacts and synthetic elements behind these emotionally expressive voices—ensuring accurate detection as TTS becomes more humanlike.

3. Real-time voice conversion

Companies like Respeecher have created tools for real-time voice conversion, allowing users to change pitch, timbre, and accent instantly. While this technology benefits voice dubbing, gaming, and content creation, it also makes it easier for fraudsters to evade voice recognition systems by masking their voice. In response to this emerging threat, Pindrop joined forces with Respeecher to create a better solution that can detect the use of real-time conversion software for fraudulent purposes.

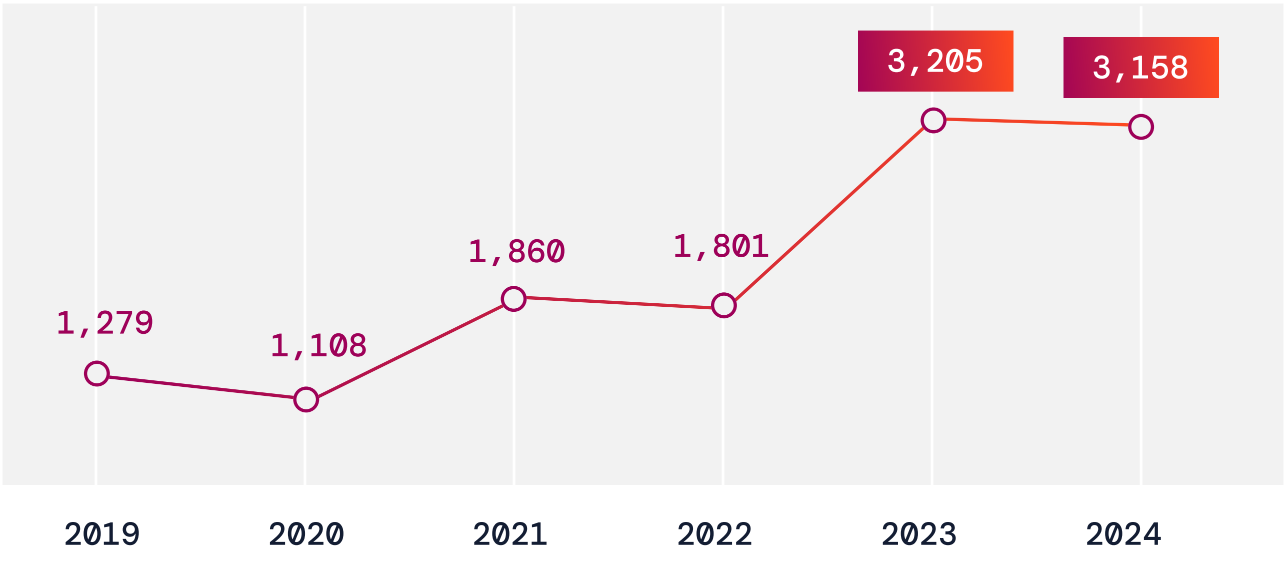
The real threat of the volume and sophistication of deepfakes lies in the ability for fraudsters to mount large-scale, automated attacks. These attacks can be replicated to target multiple enterprises simultaneously and at a low cost. Our 2024 Voice Intelligence and Security Report explains in detail how an attack of this nature can be constructed.

Data breaches have reached an all-time high

According to the 'Digital Privacy Survey Report 2024', nearly 61% of Americans have had their data breached on at least one of their accounts.[3] Data breaches and ID theft are leading indicators of fraud, particularly contact center fraud. Data breaches reached an all-time high of 3,205 in 2023 and continued at a record pace with 3,158 breaches in 2024.[4]

> Data breaches reached an all-time high of **3,205 in 2023** and continued at a record pace with **3,158 breaches in 2024**.[4]

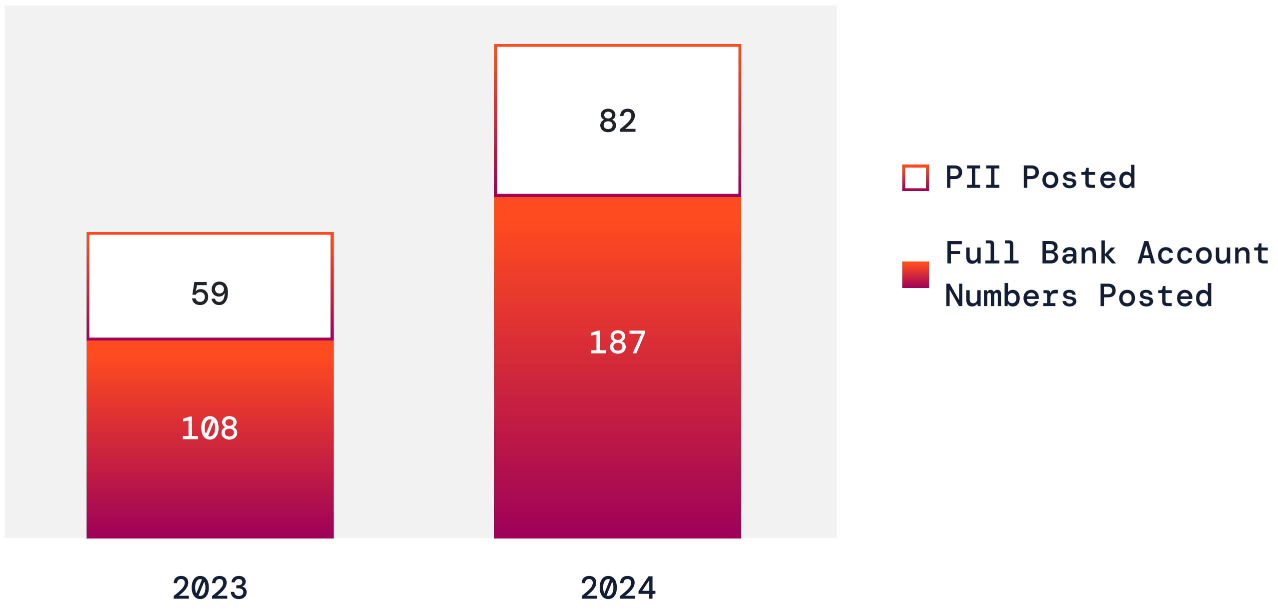
CONTINUED TREND OF DATA BREACHES



Increasingly, stolen data from breaches is posted to the dark web and other platforms. Personal Identifiable Information (PII) and bank account information were shared at a +61% higher rate in 2024 compared to 2023.[5]

This leak of personal information has affected a record number of people, with more than 1.7 billion notices sent out to victims of data breaches in 2024. This represents a 312% increase in victims from the previous year.[4] Most of the impact came from six "mega-breaches" that resulted in at least 100M breach notices being issued in each event.[4] To quantify the financial impact of these breaches, the average cost of a data breach in the U.S. reached an all-time high of $9.36 million in 2024[6], a 14% increase from 2019.[7]

STOLEN DATA POSTED ON THE DARK WEB



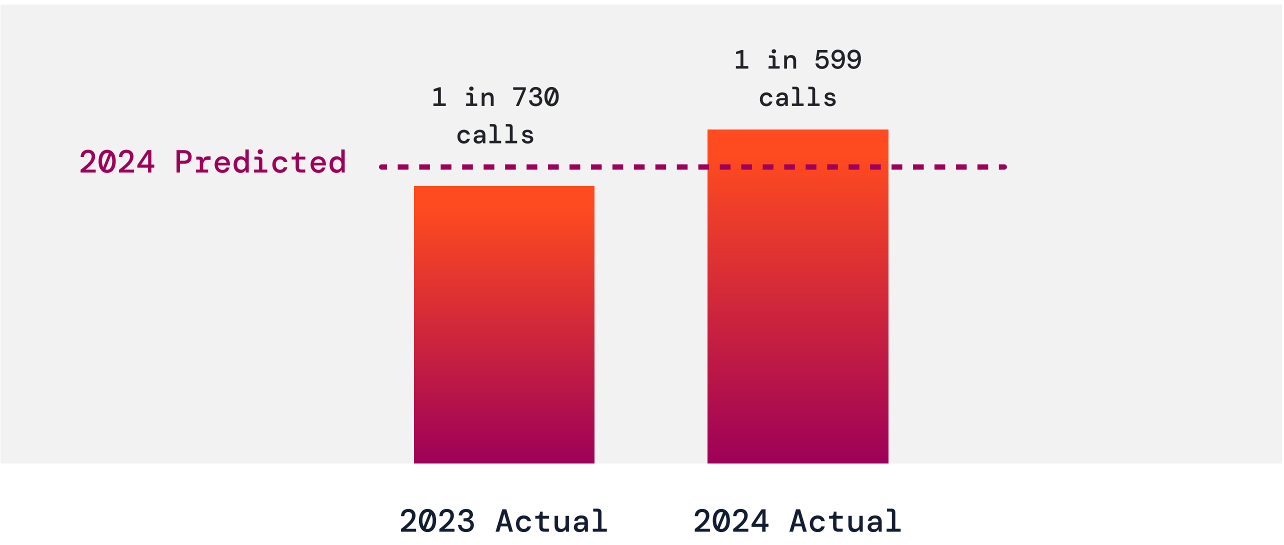
[3] U.S. News & World Report, "Digital Privacy Consumer Survey," 360 Reviews, 2024
[4] Identity Theft Resource Center, 2024 Data Breach Report , 2024
[5] Insikt Group, Annual Payment Fraud Intelligence Report: 2024
[6] KnowBe4, The State of Cyber Insurance: 2025 Global Report, 2025
[7] Digital Guardian, "What's the Cost of a Data Breach in 2019?", 2019

Fraud attempts increased by +26%[8]

Over the past two years, contact centers have been hit hard by rising fraud—driven by frequent data breaches and an unprecedented dump of personal data on the dark web. That's why the research team at Pindrop wasn't surprised to find that fraud attempts have increased by more than 26% in 2024 over the previous year.[8] Last year, Pindrop had predicted a 4% increase in fraud, but the actual increase outpaced our prediction by a massive +22%. Data breaches directly correlate with increased account reconnaissance and contact center fraud, as referenced in the 2023 Voice Intelligence and Security Report.

> In 2024, Pindrop saw a fraud rate of **1 attempt every 599 calls**, +22% higher than our prediction of 1 in 730 attempts.

2024 PREDICTIONS VS. ACTUAL FRAUD



3 accelerators driving the fraud spike

Data breaches and stolen personally identifiable information (PII): A surge in data breaches—and the growing volume and quality of personal data on the dark web—has made it easier for fraudsters to target victims across every communication channel.

1. Using low-cost AI tools to accelerate and amplify fraud

The accessibility and low cost of AI tools exacerbate fraud attempts, as they easily allow fraudsters to modulate their voices, create sophisticated deepfakes, deceive contact center agents, and bypass voice recognition systems.

2. Exploiting self-service channels for evasion and reconnaissance

Companies increasingly rely on self-service across both phone and online channels to improve customer experience and reduce operational costs. Fraudsters have started exploiting these channels through ongoing account reconnaissance in the IVR systems, with increasing use of high-scale synthetic voices for extracting information, bypassing voice recognition systems, and mimicking the IVR's operating patterns.

3. Bypassing outdated authentication methods with advanced spoofing

88% of caller interactions still rely on manual approaches,[9] like knowledge-based authentication (KBAs) and one-time passwords (OTPs). Meanwhile, fraudsters have evolved by spoofing back-end carrier metadata and exploiting OTPs with advanced tools. These methods are easy to bypass, giving attackers a clear path to commit fraud.

[8] Pindrop analysis of fraud data and call volumes across customers for the year 2024 and 2023
[9] Contact Babel: US Customer Experience, Decision Makers Guide, 2025

CHAT WITH AN EXPERT

The next generation of fraud is voice-first and AI-fueled

Synthetic voice manipulation, aggressive spoofing, and deepfake audio are now core tactics in the modern fraud playbook. These AI-driven techniques are reshaping voice channel threats—making attacks faster, more convincing, and harder to detect.

Tactic 1

Synthetic voice usage and pitch manipulation in evasion tactics

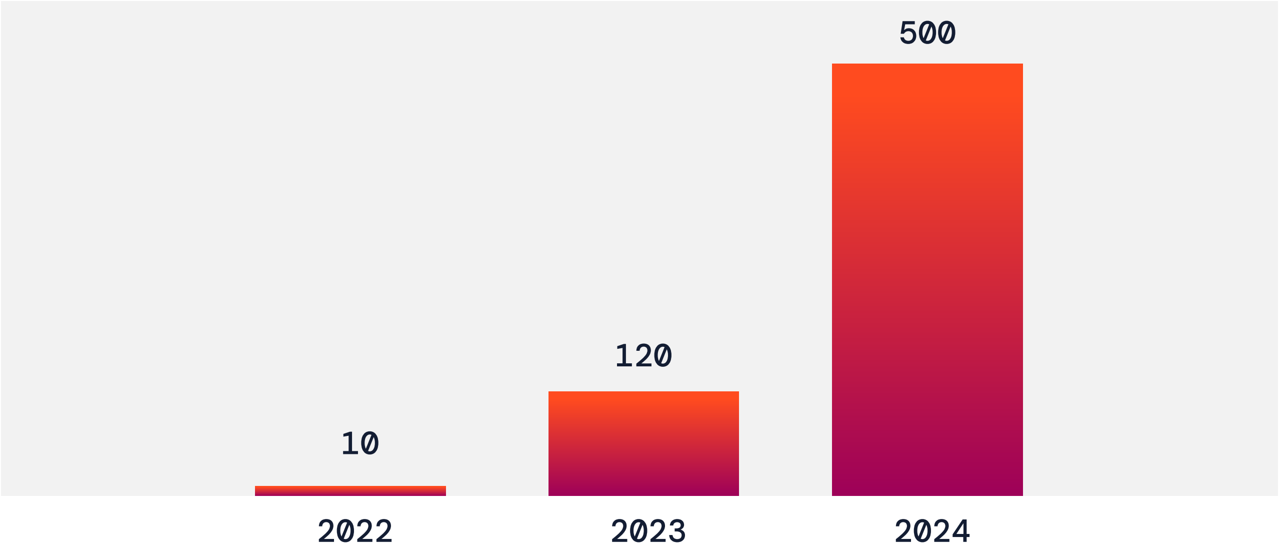
Pindrop® Pulse, our AI-powered liveness detection solution, analyzed 130 million calls and uncovered a sharp rise in synthetic voice activity. In Q4 2024, synthetic voices made up 0.33% of all contact center calls. While that number seems small, it represents an increase of +173% compared to Q1, driven by rapid advancements in voice generation technology.

Fraudsters are turning to voice modulation, manipulating their pitch, cadence, tone, and volume to imitate others or confuse agents. With easy access to voice-changing apps on mobile platforms, it's now simpler to mask their identity. For instance, a major U.S. retailer reported a surge in attackers posing as virtual legal assistants requesting account closures on behalf of customers.

Access to powerful AI platforms has removed the technical barriers to creating convincing deepfakes. In 2024 alone, Hugging Face hosted more than 2,400 TTS models and over 1,800 text-to-audio models. While these tools are powerful assets for developers, they're equally accessible to fraudsters looking to generate lifelike synthetic voices.

Pindrop is aware of this growing trend and prioritizes utilizing AI models to train our deepfake detection technology. Our training dataset now includes over 500 TTS engines, a fourfold increase from last year, significantly improving the detection accuracy of synthetic voices.

TEXT-TO-SPEECH (TTS) TOOLS USED BY PINDROP TO TRAIN AI MODELS



Source: Deepfake system TTS training list maintained by Pindrop for Pindrop® Pulse liveness detection

CHAT WITH AN EXPERT

Tactic 2

Caller ID spoofing and the erosion of metadata-based defenses

Malicious actors continue to use spoofing to mask their phone numbers and launch phishing and reconnaissance attacks. What was once a basic tactic has now become far more aggressive and sophisticated—enabled by access to breach data, dark web resources, and increasingly advanced tools.

Fraudsters are now:

- Using dark web tutorials on phishing and account takeovers (ATO)
- Exploiting readily available personal information from data breaches
- Relying on spoofing-as-a-service platforms
- Combining spoofing with synthetic voice technology
- Accessing tools that check phone status and bypass anti-spoofing solutions

Voice Authentication Remains a Critical Security Layer

Roughly 70% of all contact center interactions still happen over the phone[10], making voice a key channel for customer engagement—especially for urgent requests and across omnichannel journeys. As a result, authenticating customers through voice continues to play a vital role in the overall customer experience.

But the threat landscape is evolving. Generative AI tools and increasingly sophisticated fraud tactics are making voice-based attacks more frequent and harder to detect. Traditional methods like KBA and OTP are no longer enough—especially as enterprises work to improve both security and experience.
To stay ahead, organizations must strengthen voice authentication with deepfake detection. Passively analyzing audio to determine whether a caller is a real human—not an AI-generated voice—is a critical first step before verifying identity through voice biometrics.

[10] Contact Babel: US US Contact Centers 2024-2028 The State of the Industry & Technology Penetration

Introduction

State of the Industry

Security Landscape

Fraud by Vertical

Authentication Landscape

2025 Forecast

Fighting Fraud in an AI-First World

Conclusion

Advancements in AI

> The line between human and machine is blurring—and soon humans likely won't be able to tell the difference. While this phenomenon could have positive implications for commerce, art, and media, it also has a far-reaching impact on the ways that enterprises serve customers.

Gen AI has changed the role of 'voice' in customer interactions

New tools are making it easier and more efficient for contact centers and enterprises to manage voice interactions. With increased use of chatbots, interactive voice assistants (IVAs), emotional analysis, and transcription, many organizations are shifting toward self-service across both the phone and digital channels.

> Traditional biometric systems **must evolve** into multifactor, AI-driven solutions to keep pace with emerging threats.

Business decisions aimed at streamlining operations are creating unintended risks. The most pressing concerns include:

Significant rise in injection attacks

An injection attack consists of an attacker introducing digital content to the biometric process, bypassing the sensor (camera). IProov reported a +704% increase in face swap attacks and a +255% increase in mobile web injection attacks in the second half of 2023.[11] Gartner warns that these attacks can bypass biometric defenses and give the attacker access to sensitive data.[12]

Weakness of single-factor voice recognition

Standalone voice biometrics struggle against deepfakes. A University of Waterloo study demonstrated that voice recognition detection accuracy ranges from 38% to 88% due to vulnerabilities like silence manipulation, spectral tweaks, and TTS spoofing. These systems can flag voice mismatches but can't reliably determine if a voice is human.

Open-access models are enabling rapid deepfake creation and malicious use

Freely available AI models have made synthetic voice generation widely accessible—shifting it from a specialized capability to a tool anyone can misuse. Fraudsters can now train neural networks on large voice datasets to synthesize realistic speech that closely mimics a target's voice, making impersonation attacks more convincing and accessible.

The release of DeepSeek, an open-source AI reasoning model, caused a stir in the tech industry. Unlike standard LLMs, DeepSeek uses a chain-of-thought process to work through complex problems.[13] This gives attackers the ability to process and analyze massive datasets, detect anomalies, and exploit system vulnerabilities in real time, making it a formidable tool for identifying vulnerabilities in complex systems.[14]

Fraudsters are also using models like OmniHuman-1 from Bytedance to generate highly realistic videos from a single audio clip and image, further enhancing the realism of synthetic content. As these tools become more powerful and easier to access, the deepfake threat landscape continues to expand.

[11] IProov: Threat Intelligence Report, 2024
[12] Gartner: How to Mitigate Deepfake Identity Impersonation Attacks, 5 February 2025
[13] Trend Micro, "Exploiting DeepSeek R1: Threat Actors Abuse AI Model for Phishing and Fraud," Trend Micro Research, 2 April 2025
[14] Anthony Kimery, "China's DeepSeek AI Poses Formidable Cyber, Data Privacy Threats," Biometric Update, 24 January 2025

Agentic AI is disrupting identity verification and creating new security threats

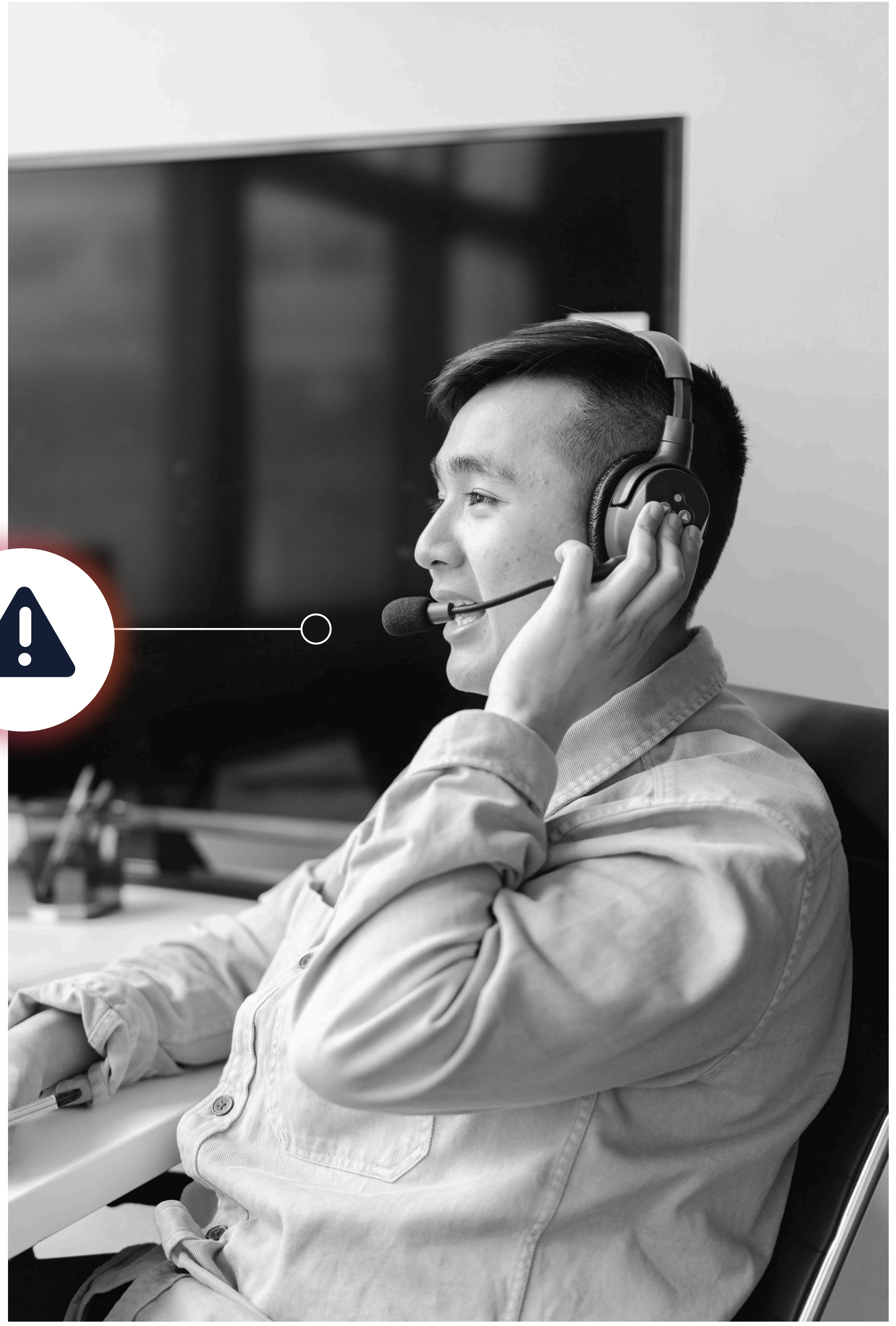
A new wave of autonomous AI systems is emerging—powered by the fusion of LLMs, machine learning, and enterprise automation. Known as agentic AI, these systems can analyze data, set goals, and act with minimal human input. This shift is poised to disrupt identity verification and introduce new security risks. Gartner estimates that by 2026, five billion connected products will exist worldwide with the potential to behave as customers, shopping for services and supplies for themselves and their owners.[15] By 2029, more than 50% of these "machine customers" will operate autonomously (up from less than 10% in 2024).[15]

Pindrop is already seeing virtual assistants placing calls on behalf of users to request tasks like account closures. What was once viewed as suspicious may soon be legitimate agentic AI behavior, blurring the line between trusted AI agents acting on behalf of a customer and agents acting with malicious intent. Agentic AI can also expose organizations to advanced cyberattacks, injection attacks, and smart malware, making advanced fraud detection critical.

In addition to enabling new forms of attack, agentic AI is being used to scale fraud strategies—generating rapid, convincing speech with deepfake voices and introducing threats like smart malware and injection attacks. On the enterprise side, agentic AI can significantly benefit contact centers by reducing the cost of human agents and improving the customer experience with a personalized support model.

Organizations must focus on passive, secure customer authentication to safely unlock this potential. They must also address the emerging challenge of distinguishing between the "*real human*" and the "*right human*."

> Organizations must also address the **emerging challenge** of distinguishing between the *"real human"* and the *"right human."*



[15] Gartner: Emerging Tech: Use Agentic AI to Transform Machine Customers, November 2024

AI is amplifying fraud across sectors, channels, and tactics

> Fraud activity in the U.S. hit record levels in 2024. According to IPX 1031, 30% of Americans reported being scammed, with an average loss of $1,600 per victim—impacting Baby Boomers, Gen X, and Gen Z alike.

The financial sector saw some of the most significant spikes. Signicat found an +80% surge in overall fraud attempts in the financial industry over the last three years, with AI-driven fraud now making up 42.5% of all fraud attempts, and an estimated 29% of those attempts considered successful.[16] Alloy's 2024 Financial Fraud Statistics report echoed these findings, with over 50% of banks, fintechs, and credit unions reporting a rise in both business and consumer fraud attempts.[17]

Much of this surge can be associated with fraudsters' use of AI, which is accelerating the scale, speed, and success rate of attacks across industries.

Most common types of reported fraud[17]

Bust out fraud

A fraudster opens a credit line using a synthetic identity, builds a typical usage pattern, then maxes out the account and disappears.

Authorized push payment (APP) fraud

The victim is tricked into sending funds to a fraudster by posing as a legitimate payee.

Account takeover (ATO)

A fraudster gains unauthorized access to a victim's bank account and performs transactions in their name.

Check fraud

Fraudsters use forged or stolen checks to steal funds. This tactic has doubled in prevalence since 2020.

Traditional biometric systems must evolve into multifactor, AI-driven solutions to keep pace with these emerging threats.

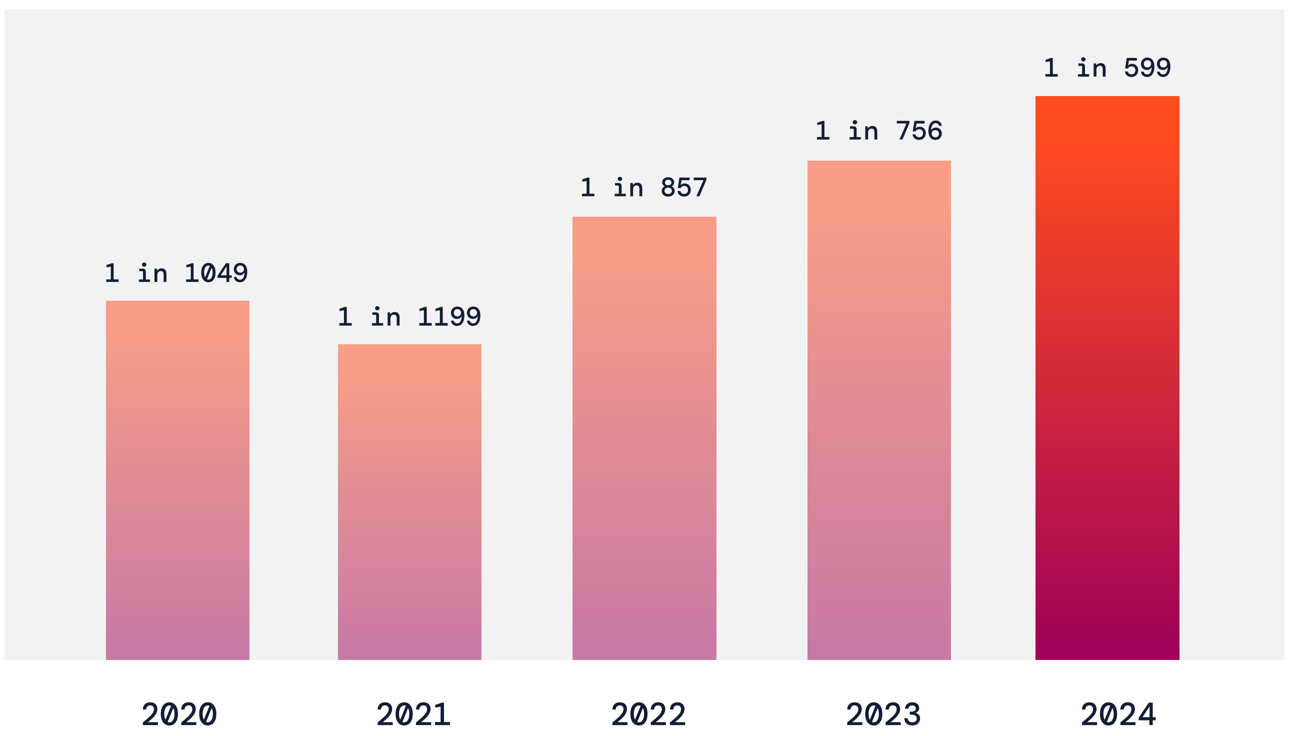
Contact center fraud reaches a 6-year high[18]

Pindrop data shows that fraud in contact centers has reached its highest level in six years, occurring in **1 in every 599 incoming calls**, or a **fraud rate of 0.17%**. While this number may look small, it represents a **+26% increase year-over-year, and a 100% increase compared to 2021**. Today, fraud attempts occur **every 46 seconds** in the contact center, and are expected to rise in 2025.

> +26% increase year-over-year, and a 100% increase compared to 2021 in fraud in contact centers.

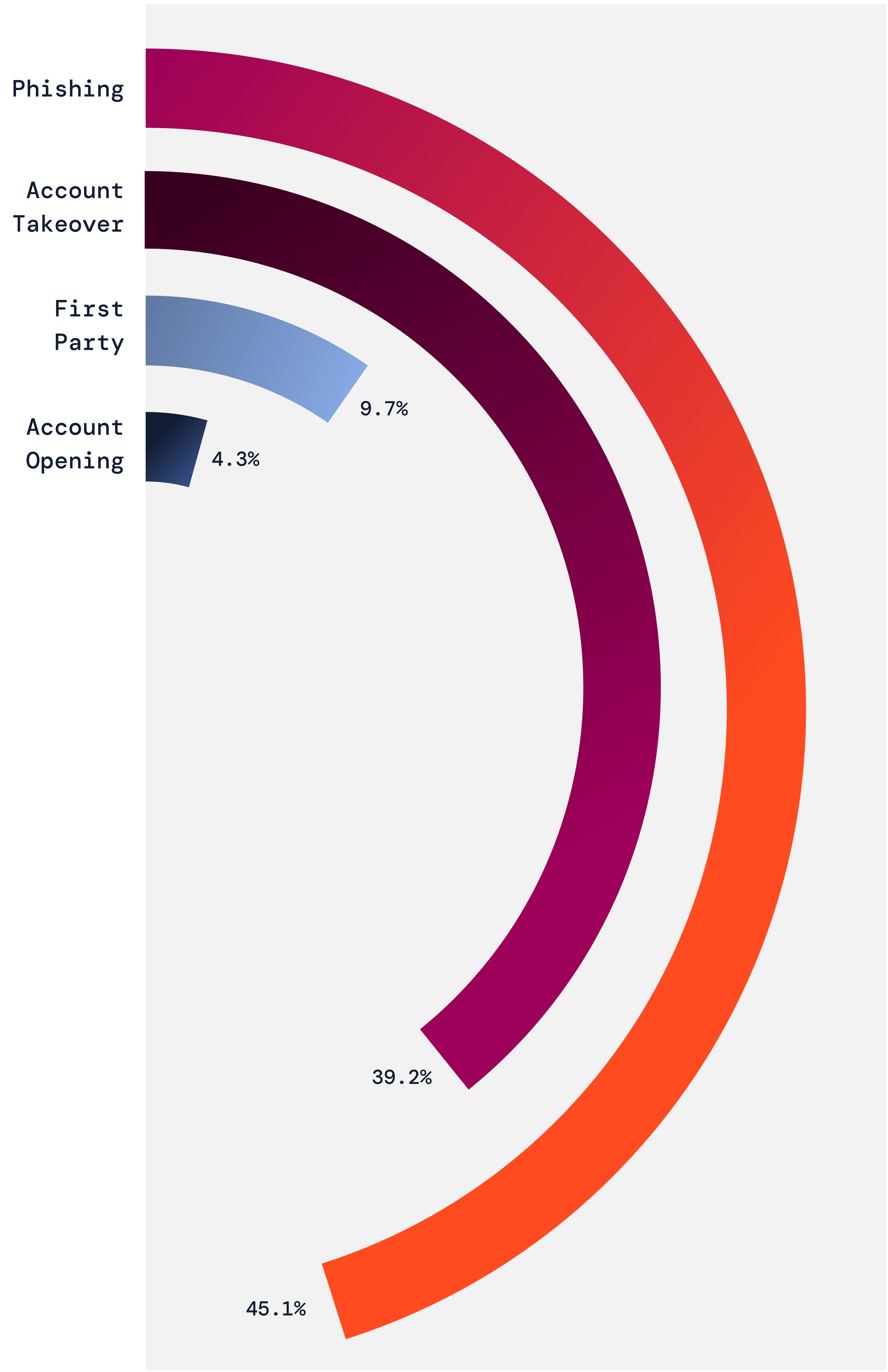
FRAUD RATE TREND

Fraud rate at 1 in x calls



[16] Signicat; The Battle Against AI-driven Identity Fraud
[17] Alloy: Infographic: 2024 Financial Fraud Statistics for Banks, Fintechs, and Credit Unions
[18] Unless otherwise noted, all data in this section is from Pindrop analysis of fraud and call volumes across 79 customers from 2019 – 2024

MOST DOMINANT FRAUD TYPES



Top fraud tactics: Phishing and ATOs

Based on internal data and customer feedback, our analysis of fraud types reveals that phishing and ATOs dominate contact center fraud.

🟥 **45% of fraud calls involve phishing, including:**

- **Pretexting:** Creating a fake scenario or "pretext" to trick victims into divulging sensitive information by making them believe they are interacting with a trusted source.
- **Vishing:** Voice phishing through deceptive phone calls.
- **Confirming or gathering information:** Calls to either gather or confirm personal details.
- **Credential requests:** Attempts to obtain login or sensitive account information for future attacks.

🟦 **10% involved first-party fraud**, where real account holders misrepresent themselves for financial gain.

🟪 **39% of fraud calls are ATO attempts**, often involving requests like:

- Resetting or requesting credentials for online account access (ID + password)
- Changing the PII on file (phone, address, email)
- Assistance with or initiating funds transfer (e.g., wire, ACH, or P2P transfer like Zelle)
- Reinstating blocked or fraud-restricted accounts
- Issuing new debit or credit cards

⬛ **4% of calls are linked to fraudulent account openings**, often using stolen identities.

CHAT WITH AN EXPERT

Introduction

State of the Industry

Security Landscape

Fraud by Vertical

Authentication Landscape

2025 Forecast

Fighting Fraud in an AI-First World

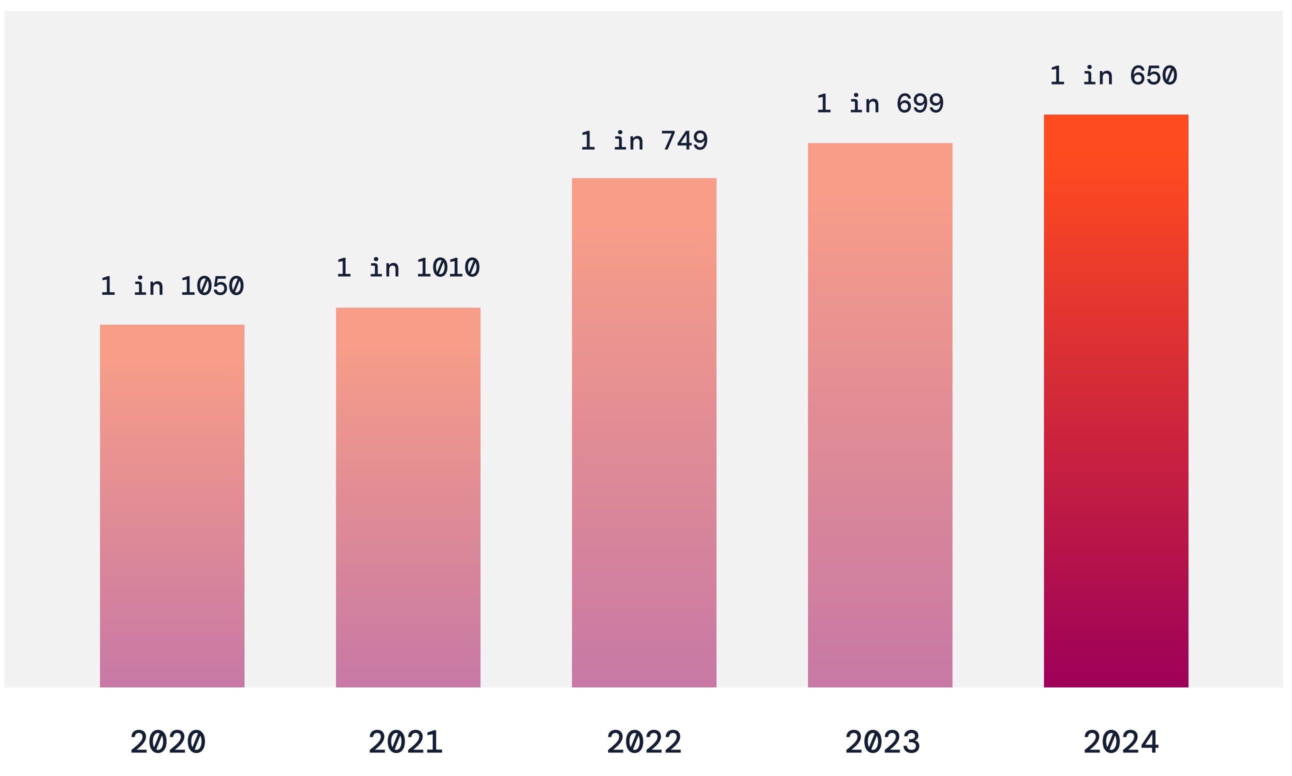
Conclusion

+61% increase in bank fraud

U.S. banks continue to experience a steep rise in contact center fraud. In 2024 alone, there was an **+8% year-over-year increase** in fraud attempts. Since 2020, this represents a **cumulative increase of +61%**, with fraud occurring in **one out of every 650 calls** to a U.S. bank. This persistent upward trend highlights the growing appeal of the phone channel as a weak link for fraudsters looking to exploit gaps in authentication and human oversight.

FRAUD RATE: BANKING

Fraud rate at 1 in x calls



Attackers are increasingly exploiting the contact center to bypass security measures. Financial institutions rely on customers to verify suspicious transactions, and fraudsters take advantage of this dependency through sophisticated social engineering tactics. These bad actors manipulate customer service representatives into lifting fraud restrictions, resetting online banking credentials, or overriding previously declined transactions.

A persistent and troubling trend in 2024 was using phone channels to reinstate fraud-restricted accounts or gain access to online banking. Impersonating legitimate customers, these actors used stolen PII to deceive agents into removing security holds, resetting credentials, or approving transactions previously declined because of suspected fraud. According to Pindrop research, 34% of ATO fraud calls involved attempts to remove account restrictions or push through blocked transactions, while 19% targeted access to online banking accounts.

As threat actors continue refining their tactics, financial institutions must strengthen authentication measures, enhance fraud detection capabilities, and train contact center representatives to identify and combat social engineering attempts. Proactive investment in fraud detection technologies and agent awareness will be critical in mitigating these growing threats.

How is fraud behavior changing?

Deceptive tactics are evolving rapidly—growing in scale, speed, and sophistication. To keep pace, enterprises must move beyond human judgment and embrace advanced detection tools capable of identifying threats in real time.

Emerging behavioral patterns reshaping fraud

- **Frequent phone number rotation**, which undermines the effectiveness of static blocklists and blacklists
- **Manipulation of registration details**, compromising OTP-based authentication by redirecting verification messages away from legitimate customers
- **Voice alteration using digital tools**, enabling attackers to mask characteristics like age, gender, and accent—making inconsistencies harder to detect

CASE STUDY

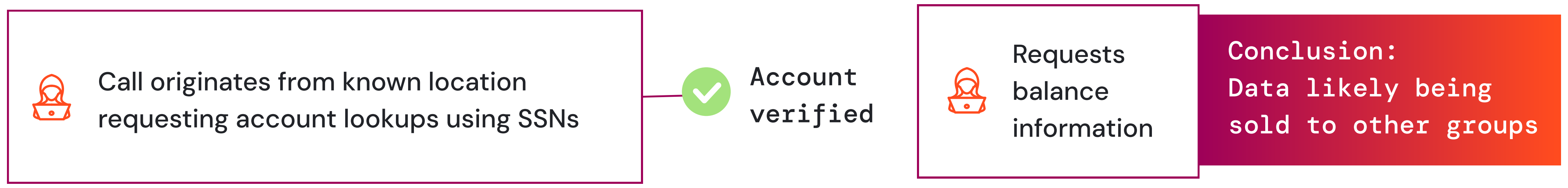
How fraud rings exploit IVRs to harvest and sell customer data

At a well-known regional bank, a fraud ring conducted high-volume reconnaissance to map customer PII and verify account balances. Their operations were relatively unsophisticated, as they did not attempt to disguise their phone numbers, and their calls originated from a known location. Rather than attempting ATOs directly, they requested account lookups using Social Security Numbers (SSNs), suggesting they were still in the early phase of data collection. Once an account was identified, they asked for balance information, likely to be sold to other groups carrying out the fraud. This group placed hundreds of calls monthly, signaling an organized effort to harvest and monetize customer data.

At another large regional bank, fraudsters engaged in IVR-based reconnaissance. Using a single phone number, one bad actor placed nine calls over three days, spending 137 minutes in the IVR and testing over 400 SSNs. Although they were not customers, the IVR's behavior made it easy to confirm valid accounts, so they could make quick work of the list of accounts they were targeting.

Deploying fraud detection in the IVR can be a valuable strategy. Pindrop provided nightly reports on suspicious behavior and detected reconnaissance in real time, allowing the bank to intervene before attackers reached live agents. While some vulnerabilities were due to IVR design, even mature systems remain susceptible to automated, large-scale reconnaissance unless proactive fraud defenses are in place.

TACTIC 1:



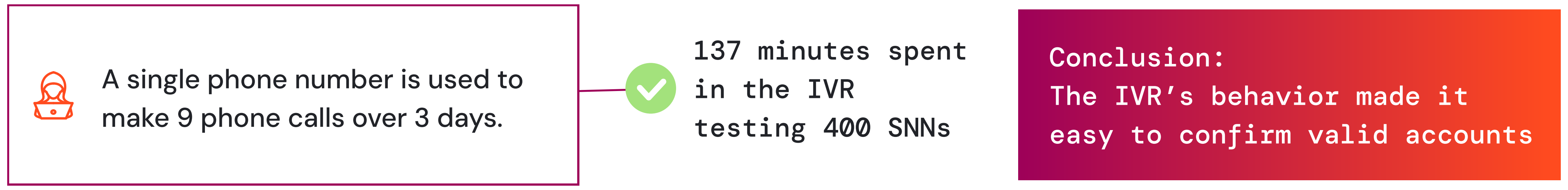
Call originates from known location requesting account lookups using SSNs

Account verified

Requests balance information

Conclusion:
Data likely being sold to other groups

TACTIC 2:



A single phone number is used to make 9 phone calls over 3 days.

137 minutes spent in the IVR testing 400 SNNs

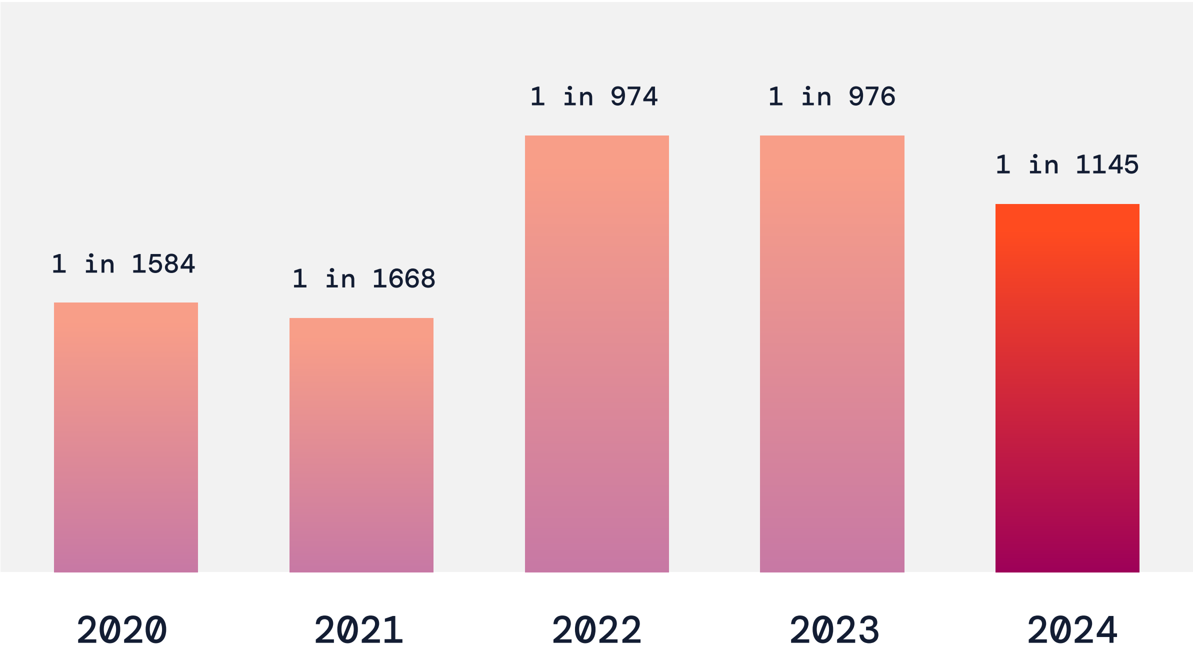
Conclusion:
The IVR's behavior made it easy to confirm valid accounts

38% increase in credit union fraud since 2020[19]

While credit unions saw a **15% decline in fraud attempts in 2024**, translating to **one fraud attempt for every 1,145 calls**, the overall threat remains high. Compared to 2020, fraud has risen **38% cumulatively**, highlighting a long-term upward trend.

FRAUD RATE: CREDIT UNIONS

Fraud rate at 1 in x calls



Fraud patterns at credit unions closely mirror those seen in retail banks, but with one notable difference: **first-party fraud is significantly lower**. Less than 5% of fraud cases at credit unions involve first-party activity, compared to 10% across the broader client base.

Fraud rates also correlate with call volume. Credit unions with under **1 million annual agent calls** experience approximately **one fraud call per 1,600 calls**, while those handling **more than 1 million** see **fraud rates over 55% higher**. As membership and volume grow, so does the institution's exposure to fraud.

This pattern holds across smaller retail banks. Larger institutions—especially those with more assets under management—naturally attract fraud, offering fraudsters more opportunities to match stolen PII to real accounts. Meanwhile, smaller firms often lack the technology and staffing to detect and respond to fraud effectively.

As fraud tactics evolve, credit unions must stay proactive by investing in advanced detection tools, improving authentication measures, and equipping employees with the training to identify and respond to emerging threats.

> "Pindrop just seemed to be more forward-thinking than the other vendors we looked at. For example, their work surrounding deepfakes was considerable, and it seemed like they were leading the charge more so than the competition."
>
> **Colleen Cole**
> *VP of Call Center, MSUFCU*

86-Year-Old Credit Union **Cuts Authentication Time in Half** in First 90 Days of Pindrop Implementation

Read case study →

[19] Unless otherwise noted, all data in this section is from Pindrop analysis of deepfake activity across over 130 million calls from customers for the year 2024

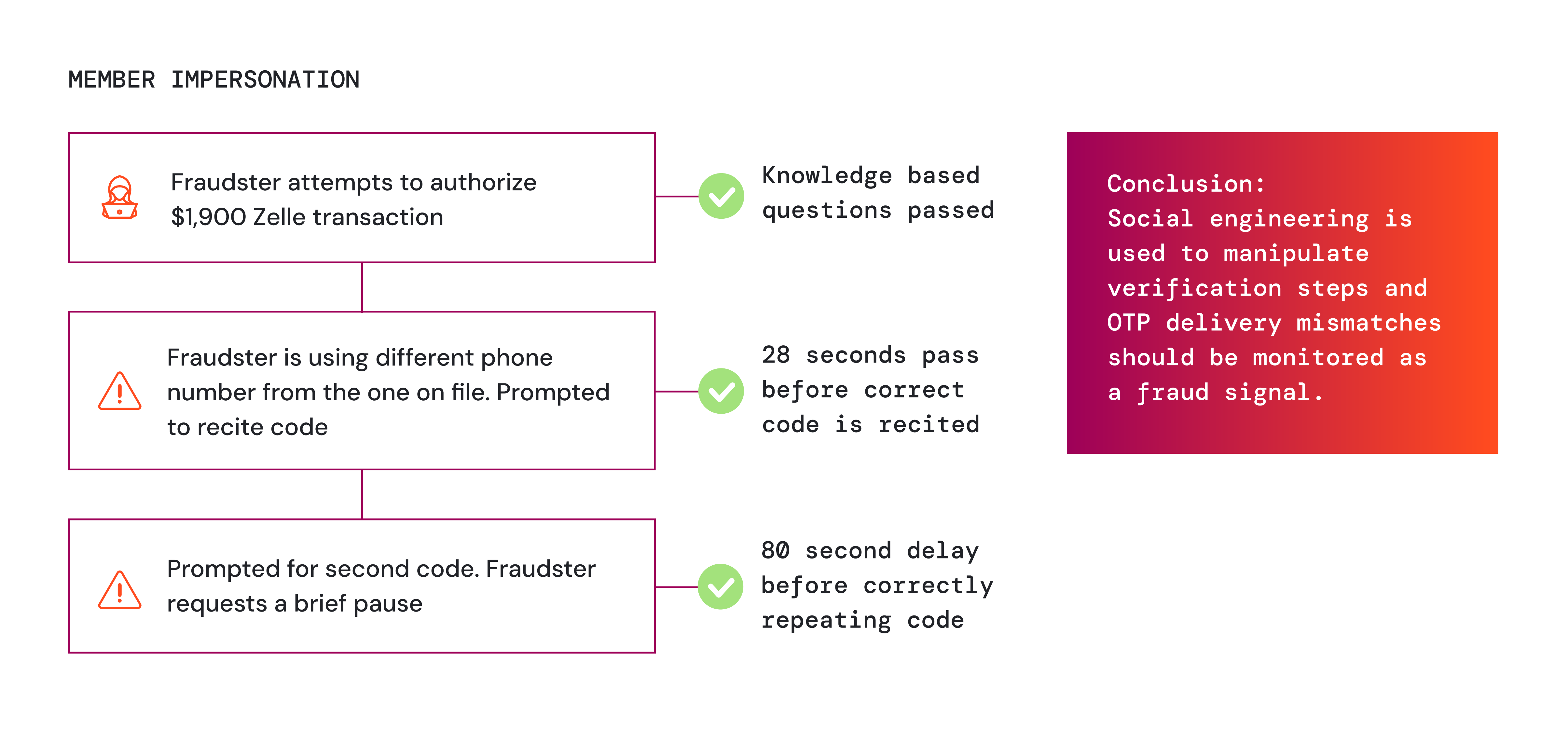
CASE STUDY

How social engineering bypassed OTP defenses

At a leading Midwest credit union, a fraudster attempted to authorize a $1,900 Zelle transaction by impersonating a member. The caller successfully passed knowledge-based challenge questions but was prompted twice—once before and once after being transferred to the online team—to read back an SMS one-time password (OTP) sent to the account holder's registered number.

A key red flag emerged: The caller used a different phone number than the one on file to receive OTPs. The caller hesitated for 28 seconds during the first prompt before reciting the code. On the second prompt, just before the OTP was sent, the caller asked about its expiration time and requested a brief pause to "use the bathroom." After an 80-second delay, he asked for the OTP be sent and then correctly repeated the code.

The credit union later confirmed the fraudster had been texting the legitimate account holder, tricking them into sharing the OTP through impersonation. This case underscores how social engineering is used to manipulate verification steps and highlights the need to monitor OTP delivery mismatches as a critical fraud signal.



MEMBER IMPERSONATION

Fraudster attempts to authorize $1,900 Zelle transaction

✓ Knowledge based questions passed

Fraudster is using different phone number from the one on file. Prompted to recite code

✓ 28 seconds pass before correct code is recited

Prompted for second code. Fraudster requests a brief pause

✓ 80 second delay before correctly repeating code

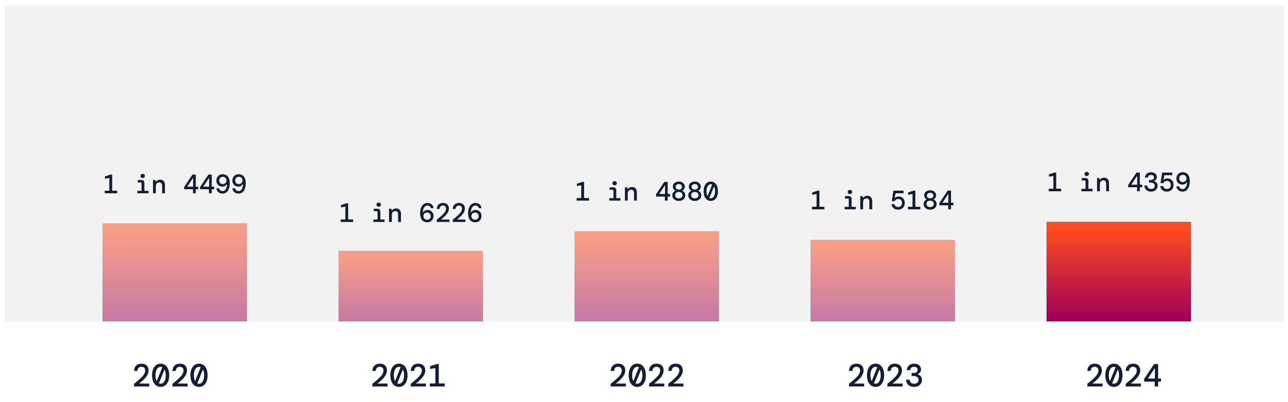
Conclusion:
Social engineering is used to manipulate verification steps and OTP delivery mismatches should be monitored as a fraud signal.

Insurance fraud is increasing in cost, complexity, and impact

In 2024, insurance fraud rose **19% year-over-year**, with a fraud rate of **1 in every 4,359 calls (0.02%)** across life, health, and property casualty sectors. While this rate is lower than banking's 0.17%, the **average fraud exposure in insurance is 20 times higher**, making each incident significantly more costly.

FRAUD RATE: INSURANCE

Fraud rate at 1 in x calls



Insurance fraud differs from traditional retail banking fraud in both frequency and approach.

First-party fraud is relatively rare, but **familiar fraud**, where attackers exploit personal connections, accounts for **7% of fraudulent call activity**. When ATO occurs, the most common abuse involves policy loans and annuity withdrawals. Fraudsters often update ACH or mailing address details to divert funds, enabling them to take out loans or withdraw from annuities without the policyholder's knowledge.

As these tactics grow more sophisticated, insurance providers must strengthen authentication protocols, deploy advanced fraud detection, and maintain continuous monitoring to protect customers and minimize losses.

Phishing and reconnaissance are far less common—**only 23% of insurance fraud cases** involve these tactics, compared to approximately **45% across all Pindrop clients**. This is likely due to the static nature of insurance account balances, reducing the need for repeated probing.

> "Pindrop has helped us tremendously by improving the user experience for our callers, and is a critical part of our caller authentication ecosystem."

FRAUD OPERATIONS HEAD

Huge U.S. insurance company tapped Pindrop to help **improve customer relations**

Read case study →

CASE STUDY

Attack precision is outpacing preparedness

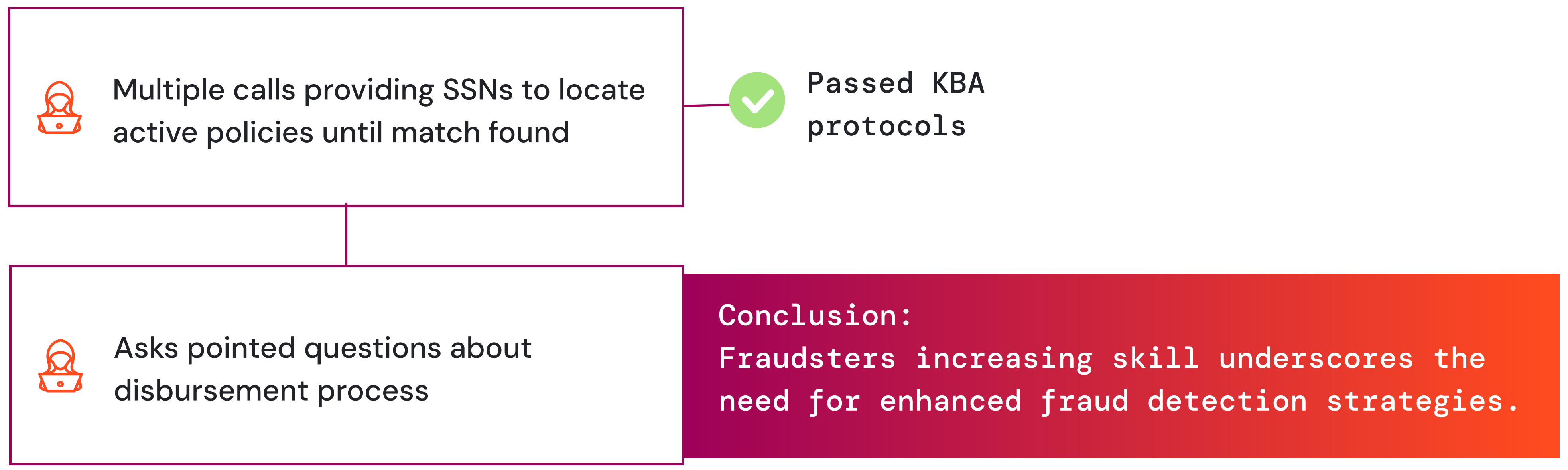
A persistent fraud scheme targeting a major West Coast insurance provider illustrates the increasing sophistication of fraudsters.

The core tactic remains familiar—probing for policy details and attempting unauthorized withdrawals—but the level of preparation has notably escalated. The scheme typically begins with multiple calls from foreign actors providing SSNs to locate active policies. If no match is found, they disconnect quickly. When a match is identified, the fraudster confidently navigates knowledge-based authentication (KBA) protocols, signaling strong familiarity with standard security checks.

Once authenticated, the caller's objective was to determine the policy's value and explore withdrawal options. They asked pointed questions about the disbursement process, like ”What steps are required? Are forms needed? Must they be sent to a third-party administrator? Does an employer need to complete any sections?” Their inquiries were methodical, often extending to requests for a good call-back number or an email address to receive withdrawal forms.

While these types of attacks are not new, the increased proficiency of fraudsters presents a growing challenge. Their ability to exploit procedural knowledge, anticipate verification methods, and adapt to countermeasures underscores the need for enhanced fraud detection strategies. Strengthening authentication protocols, implementing real-time risk analysis, and continuously training contact center representatives to recognize evolving fraud tactics remain critical defenses against these increasingly skilled adversaries.

FRAUD BY THE SCRIPT



Multiple calls providing SSNs to locate active policies until match found

Passed KBA protocols

Asks pointed questions about disbursement process

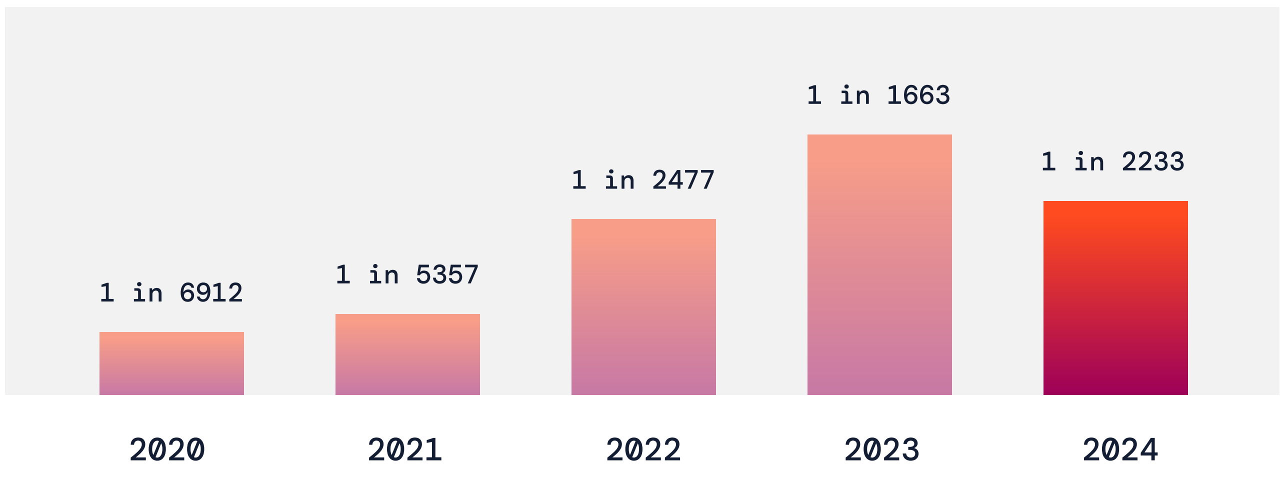
Conclusion:
Fraudsters increasing skill underscores the need for enhanced fraud detection strategies.

Brokerage fraud may be less common—but can be far more damaging

The brokerage sector, which includes wealth management, retirement, and investment firms, saw a **26% year-over-year decline in fraud** in 2024. However, with **1 in every 2,233 calls identified as fraudulent**, the **cumulative fraud rate has surged +209% since 2020**.

FRAUD RATE: BROKERAGE

Fraud rate at 1 in x calls



Brokerage fraud often mirrors tactics seen in banking but with some key distinctions. Rather than focusing on card or transactional abuse, fraudsters in this sector typically target unauthorized online access, check processing, and wire or ACH transfers. These types of fraud pose a greater risk as recovery is often more difficult, particularly for wire and ACH fraud.

Brokerage accounts usually hold higher balances, adding to the risk. This makes successful fraud attempts significantly more damaging.

> On average, **brokerage losses are over three times higher** than in retail banking fraud.

What makes brokerage fraud particularly damaging is the value at stake.

These accounts often hold significantly higher balances, making each successful attempt disproportionately costly. On average, losses in brokerage fraud are over three times higher than those in retail banking.

Despite the drop in incident volume, the sector remains a **high-reward target** for attackers. The combination of **looser real-time alerting, static security questions**, and **delayed disbursement processes** creates exploitable gaps, especially for those with access to compromised credentials or insider knowledge.

Looking ahead, the next wave of brokerage fraud may be powered by **AI-generated identities**, enhanced **impersonation capabilities**, and **automated withdrawal planning**. For institutions, proactive investment in identity verification and continuous transaction monitoring will be critical to help protect high-value accounts from increasingly surgical attacks.

+209% increase in cummulative fraud rate since 2020

CASE STUDY

KBA success, security failure

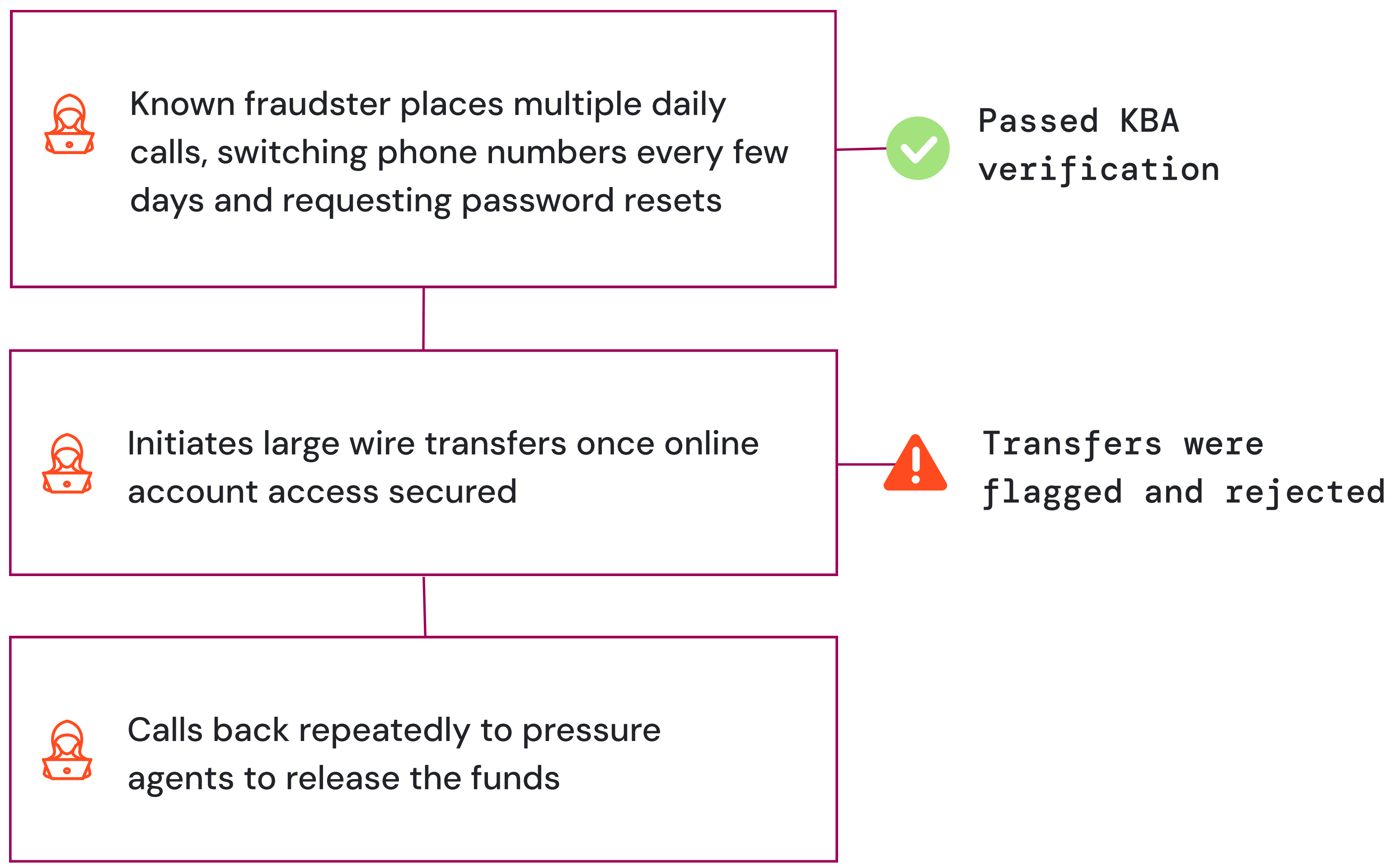
> How one attacker drained funds through repetition and persuasion

A known fraudster repeatedly targeted one of the largest U.S. brokerage firms, placing multiple daily calls while cycling through different phone numbers every few days. Their primary tactic was requesting password resets to gain online account access. Despite an apparent demographic mismatch, they consistently passed knowledge-based authentication (KBA) verification.

Once they secured access, the fraudster quickly initiated large wire transfers, often in the tens of thousands of dollars. When transfers were flagged and rejected for fraud, they called back repeatedly and used urgency, persuasion, and social engineering to pressure agents into releasing the funds.

This case underscores how fraudsters exploit contact center processes, using persistence and manipulation to override security protocols and carry out high-value transactions.

FRAUDSTER PLAYBOOK



Known fraudster places multiple daily calls, switching phone numbers every few days and requesting password resets

✓ Passed KBA verification

Initiates large wire transfers once online account access secured

⚠ Transfers were flagged and rejected

Calls back repeatedly to pressure agents to release the funds

Conclusion:
Bad actors exploit contact center processess using persistence and manipulation to override security protocols.

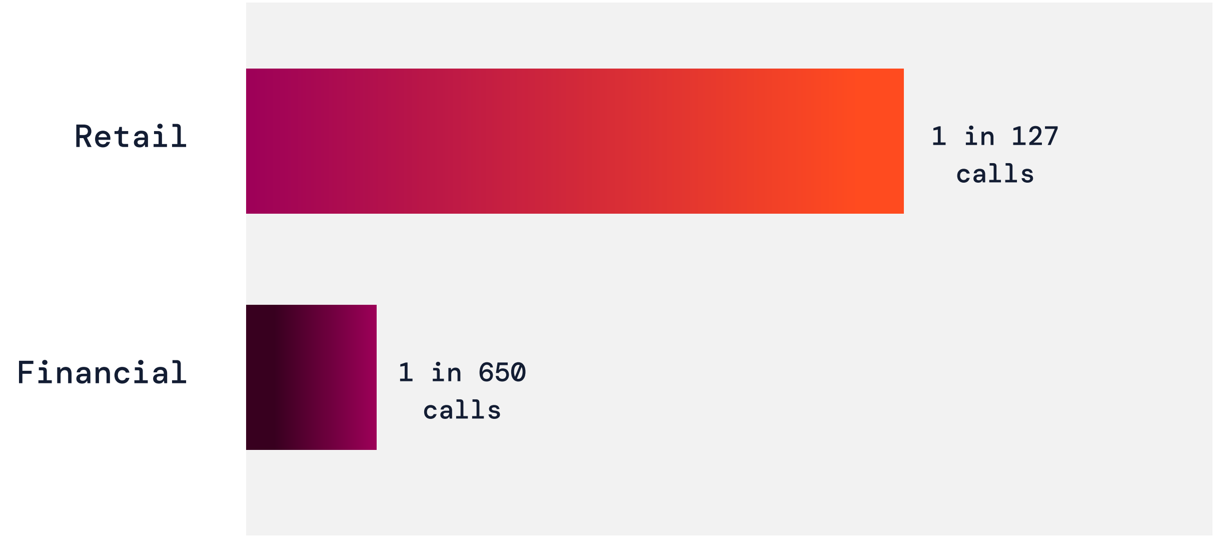
CHAT WITH AN EXPERT

Retail is under siege

> The sector leads in fraud density, with rates doubling year-over-year

In 2024, retail emerged as the most fraud-dense sector across our customer base, driven by fraud rates doubling year-over-year. While the average fraud rate in the finance sector is 1 in 650 calls, the retail and e-commerce sectors experienced fraud in **1 in every 127 calls**, or **5 times higher**.

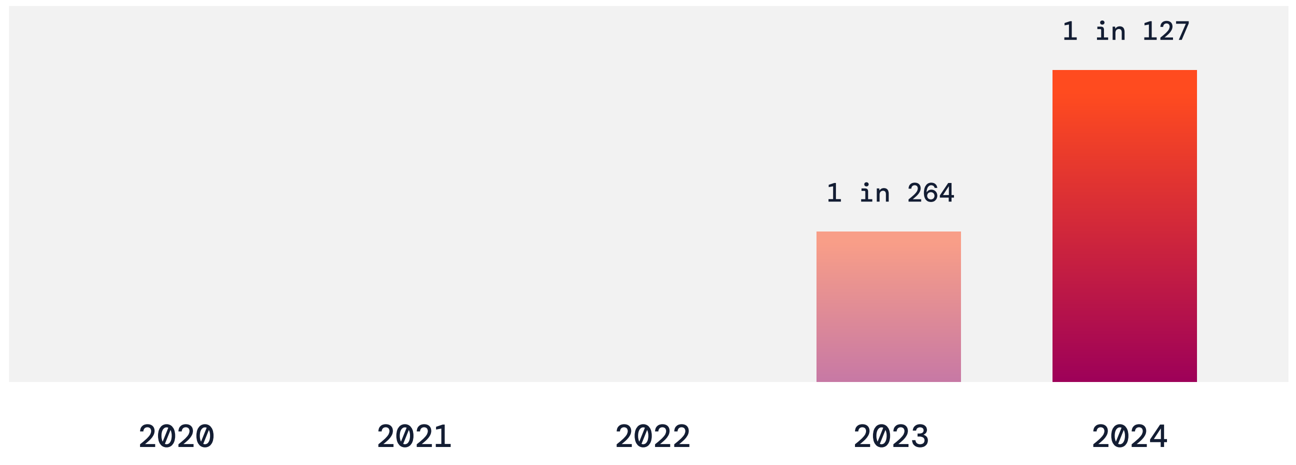
COMPARATIVE FRAUD RATE



Retail fraud nearly doubled in 2024, rising from **0.38% to 0.79%**. This surge was driven by returns fraud and the growing use of synthetic voice and replay attacks.

FRAUD RATE: RETAIL

Fraud rate at 1 in x calls



Fraudsters are increasingly targeting e-commerce due to its rapid growth and retailers' ongoing challenge in balancing customer service with fraud prevention. Key trends observed include:

- **Higher fraud rates** across both call volume and high-risk interactions compared to other sectors
- **“Death by a thousand cuts”** - individual losses per event are relatively low ($100–$250), but high volume makes overall exposure significant
- **High fraudster success rates**, as refund and return requests are easier to exploit than financial transfers
- **Multiple good accounts** (in the thousands) are nested or purchased by fraudsters to utilize for fraud activity
- **Playbooks and social engineering scripts** are designed to manipulate agents into approving fraudulent refunds or returns

As retail fraud becomes more frequent and effective, organizations must adopt advanced fraud detection strategies to protect both revenue and customer experience.

GUIDE

5 Steps Retailers Should Take to Mitigate Return Fraud

Fraudsters favor the phone—making contact centers a prime target.

Read the guide →

CASE STUDY

High-volume refund fraud exposes retail's voice vulnerability

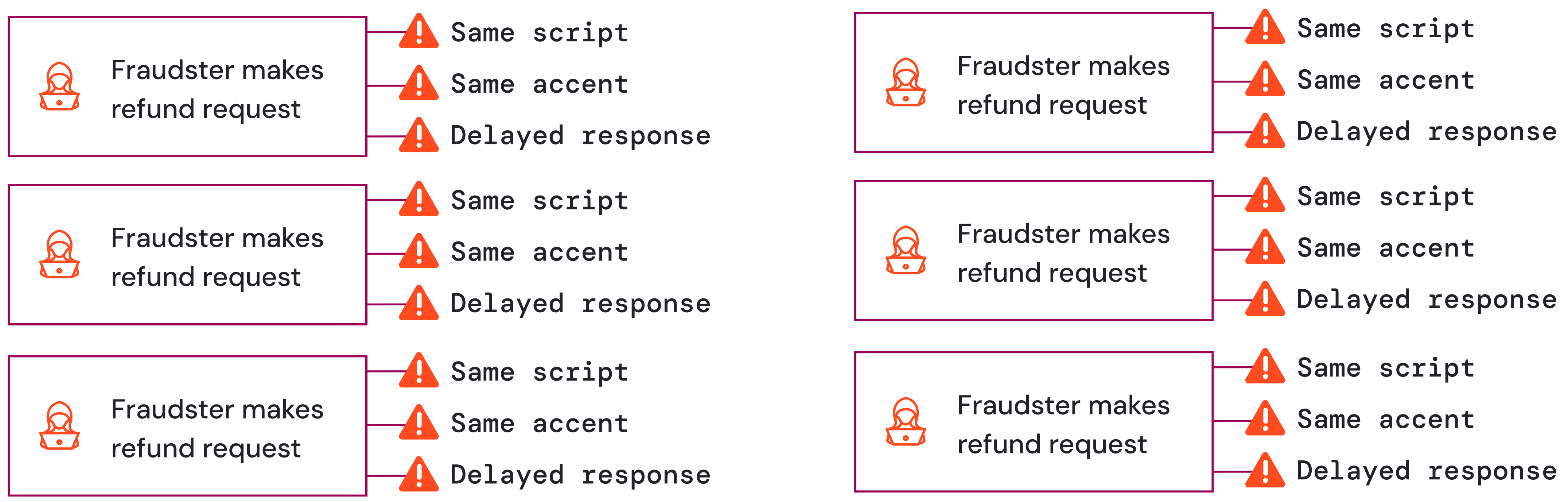
A major global retail client of Pindrop was inundated with tens of thousands of fraudulent refund requests coming through their contact center each month. After a closer investigation, a troubling pattern emerged. Known fraudsters called an average of 10 times per month, frequently rotating phone numbers every few calls to avoid detection.

The refund requests followed a predictable, scripted format. Calls would open with a friendly introduction—"Nice to meet you. My package is missing, and I need your help. Thank you!"—followed by a nearly identical request after verification: "I didn't receive the package. Can you give me a refund? Thank you!"

While these calls initially seemed routine, further analysis raised red flags. Many callers shared similar accents, suggesting potential coordination by an overseas fraud ring. Even more concerning was the growing use of TTS technology. A noticeable 10-20 second delay between a representative's question and the caller's response suggested the use of automated tools, likely to mask identities or overcome language barriers.

Although these callers did not appear to be AI bots, their tactics allow non-native speakers to file fraudulent refund requests convincingly at scale. This case underscores the evolving nature of phone-based fraud and the need for enhanced detection measures to combat increasingly sophisticated schemes.

A PREDICTABLE PATTERN



Fraudster makes refund request
- ⚠ Same script
- ⚠ Same accent
- ⚠ Delayed response

Fraudster makes refund request
- ⚠ Same script
- ⚠ Same accent
- ⚠ Delayed response

Fraudster makes refund request
- ⚠ Same script
- ⚠ Same accent
- ⚠ Delayed response

Fraudster makes refund request
- ⚠ Same script
- ⚠ Same accent
- ⚠ Delayed response

Fraudster makes refund request
- ⚠ Same script
- ⚠ Same accent
- ⚠ Delayed response

Fraudster makes refund request
- ⚠ Same script
- ⚠ Same accent
- ⚠ Delayed response

Conclusion:
AI tools likely enabled an overseas fraud ring to coordinate and execute sophisticated schemes at scale.

Deepfake activity doubled in a single quarter[20]

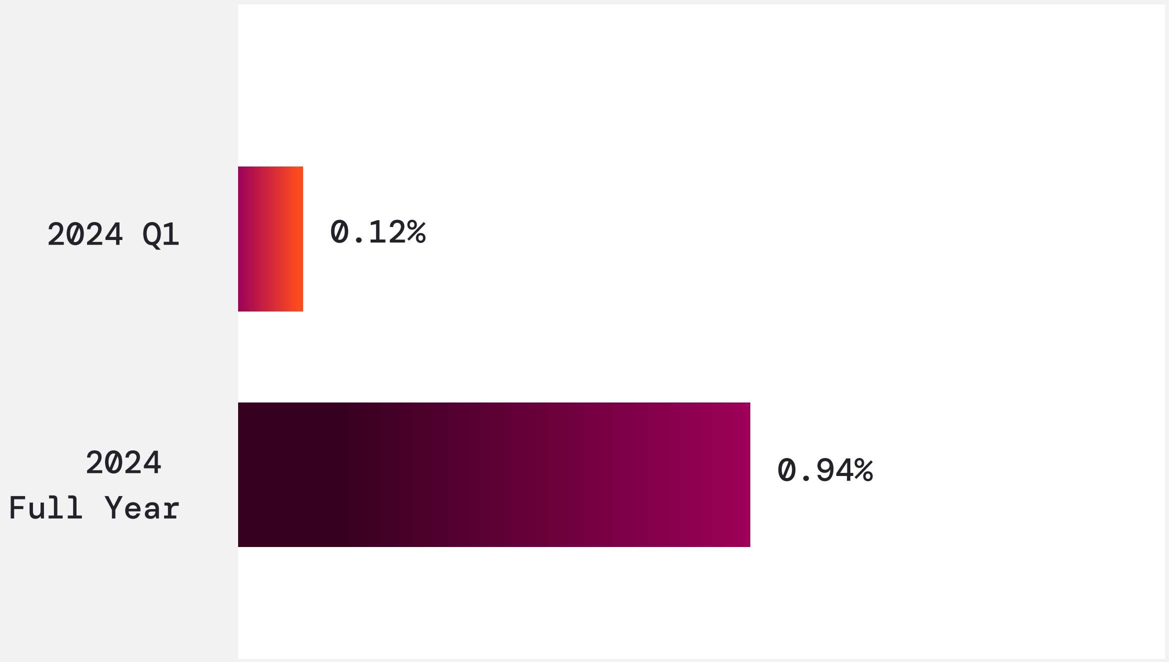
Early signs of deepfake activity began appearing in contact centers in 2023, including reconnaissance attempts, bot interactions, IVR mimicry, and replay attacks. By early 2024, **1 in every 833 calls (0.12%)** was flagged as "non-live", or calls exhibiting signs of synthetic voices or replays. However, deepfake activity accelerated rapidly. By the end of 2024, **non-live calls increased by 6.8x**, accounting for 0.94% of all calls, or **1 in every 106 calls**. This sharp rise highlights deepfake threats' growing scale and pervasiveness in just one year.

A breakdown of these non-live calls shows a **1:2 ratio between synthetic voice attacks and replays**. While replays remain easier to construct and execute, the significant volume of synthetic voice usage underscores how quickly deepfake tools are evolving and becoming more accessible.

The scale of this deepfake activity has grown throughout the year. While the first quarter of 2024 showed a similar pattern of deepfake activity compared to 2023 (0.12% of all calls were deepfake), that number rapidly increased up to Q3, before **doubling in the fourth quarter**, surpassing **2% of all calls**.

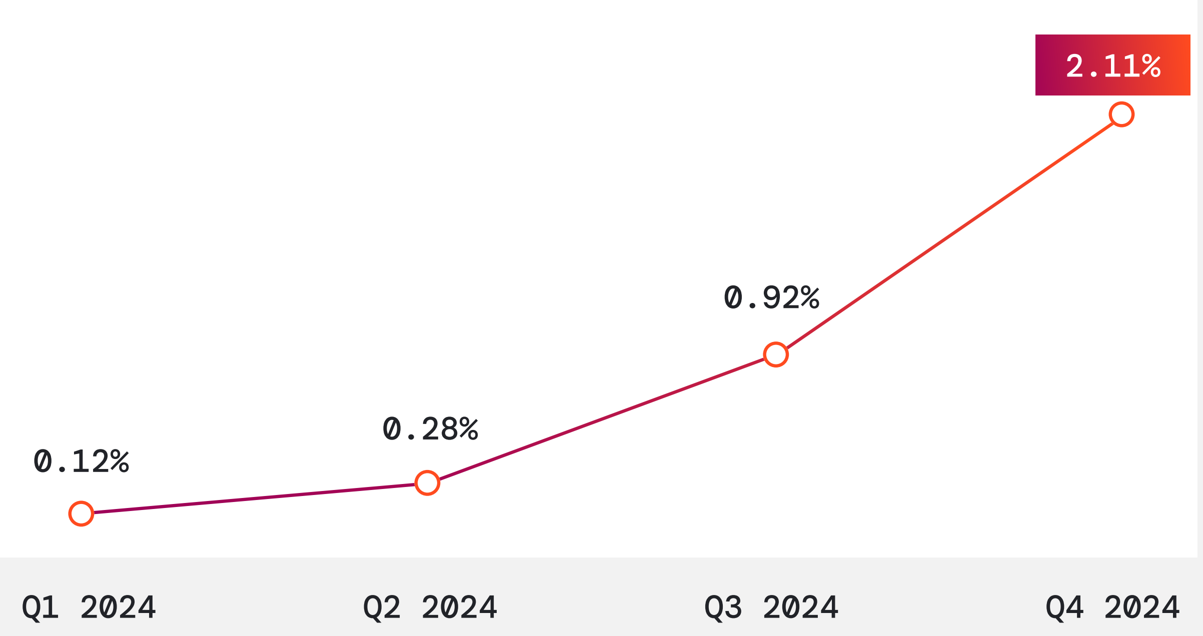
We saw the same rapid growth pattern across four of our financial institution (FI) customers, where deepfake activity surged by an average of **+354% year-over-year**. One FI reported a **12x increase** in deepfake activity in 2024 alone.

ALMOST 1% OF ALL CONTACT CENTER CALLS ARE "NON-LIVE"

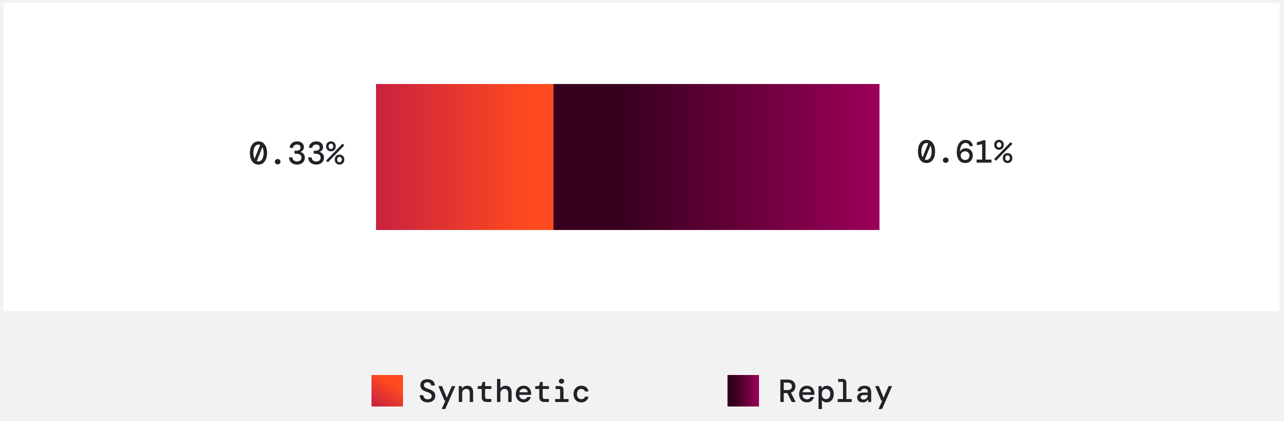


MACHINE-GENERATED VOICE CALLS GREW CONTINUOUSLY

Quarterly Trend of Non-Live Calls as % of Total Call Volume

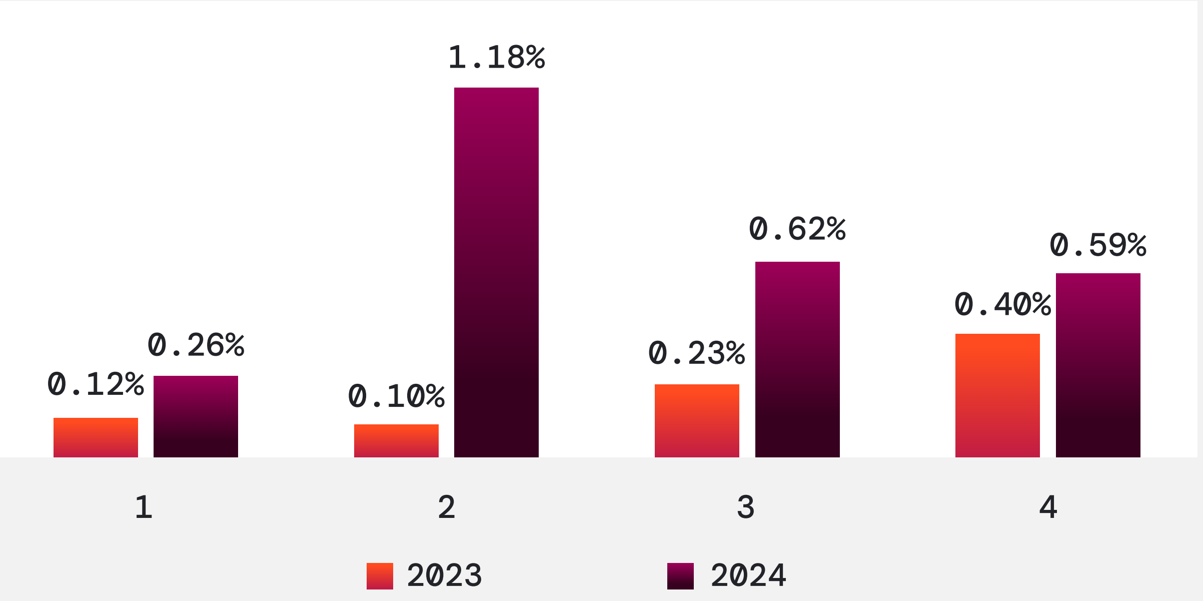


REPLAY VOICES ARE MORE PREVALENT, BUT SYNTHETIC CALLS ARE GROWING



DEEPFAKE ACTIVITY SPIKED AN AVERAGE OF +354% YOY ACROSS FOUR PINDROP CUSTOMERS

Non-Live Calls as % of Total Calls



[20] Unless otherwise noted, all data in this section is from Pindrop analysis of deepfake activity across over 130 million calls from customers for the year 2024

The surge in synthetic voice fraud reveals a more complex threat landscape

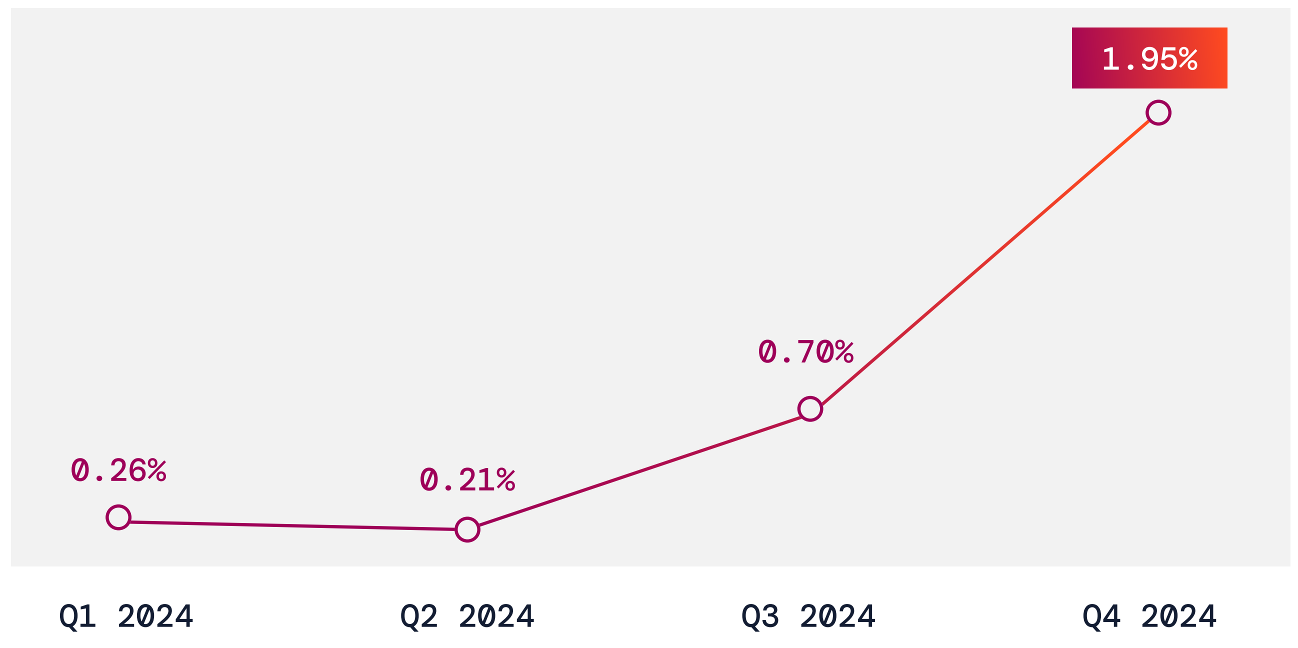
> Not all voice anomalies signal an attack—but when deepfakes are used in fraud the consequences can escalate fast, especially in finance and insurance.

While deepfake activity has surged, we should note that not all synthetic voices or replays are malicious. There are several legitimate uses of synthetic voices, including voice cloning for individuals with disabilities or to protect personal privacy. Some replay detections could also stem from benign background audio, like a television or radio playing in the background of a call.

However, the impact becomes clear when deepfake calls are linked to confirmed fraud. Pindrop found that machine-generated voices (synthetic or replayed) accounted for 0.90% of all confirmed fraud. Notably, there is a growing trend of fraudsters using deepfakes to manipulate representatives in the agent-handled portion of fraud calls. We saw a massive spike in deepfake fraud in Q4 2024, with fraud rates reaching almost 2% of all fraud cases.

MACHINE-GENERATED VOICE FRAUD SPIKED IN THE 2ND HALF 2024

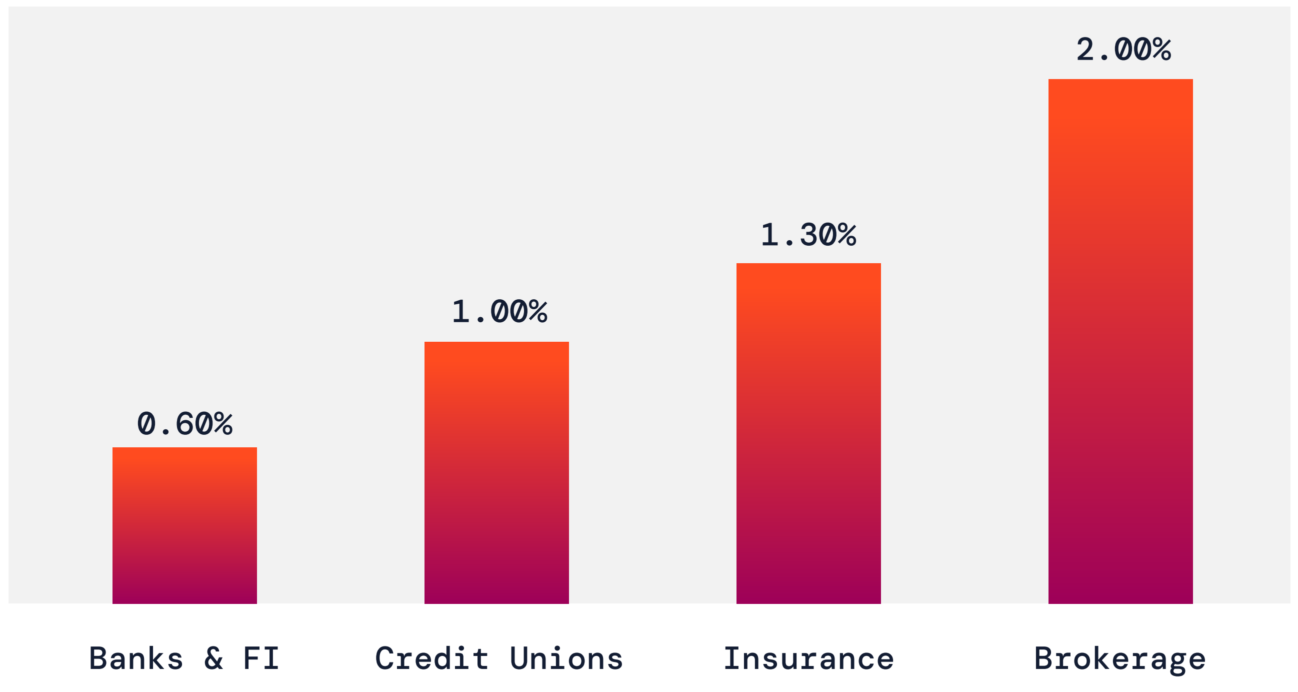
Machine-Generated Voice Fraud as % of Total Fraud (Agent Leg)



The industry vertical breakout of deepfake fraud data conveys that brokerage and insurance sectors had a higher incidence of deepfake fraud (2% and 1.3%, respectively).

INSURANCE AND BROKERAGE FIRMS HAVE HIGHER SHARE OF FRAUD FROM MACHINE-GENERATED VOICES

Synthetic and Replay Voice Fraud as % of Total Fraud by Vertical

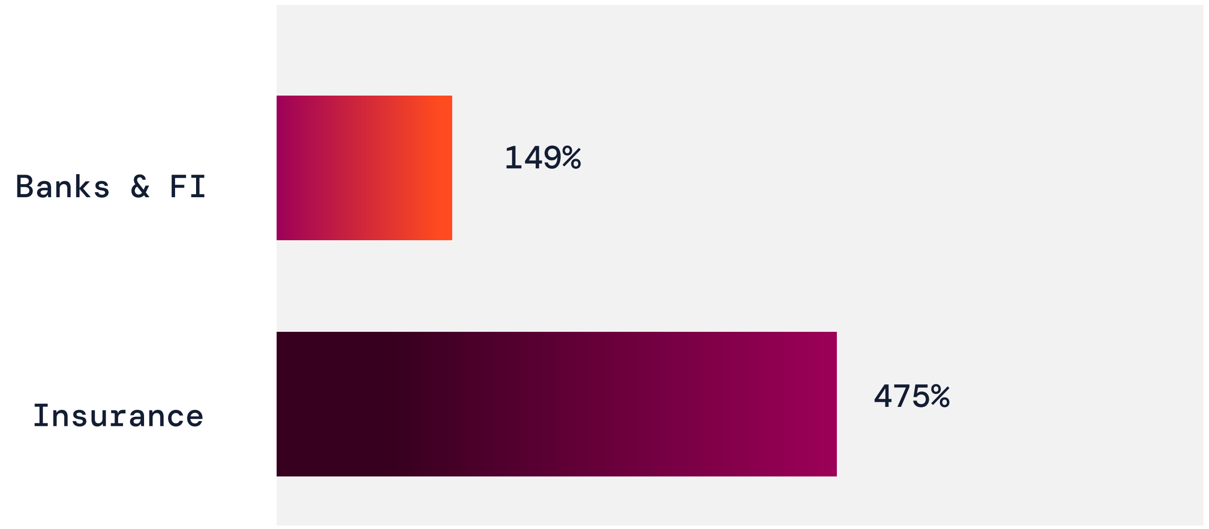


Synthetic voice fraud is an even bigger threat. Fraudsters can use synthetic voices to bypass authentication, manipulate agents, or conduct large-scale IVR reconnaissance without human involvement.

In 2024, synthetic voice fraud attacks increased by **+149% at banks** and **+475% at insurance companies**, signaling a sharp escalation in using automation to carry out fraud.

SHARP RISE IN SYNTHETIC VOICE FRAUD

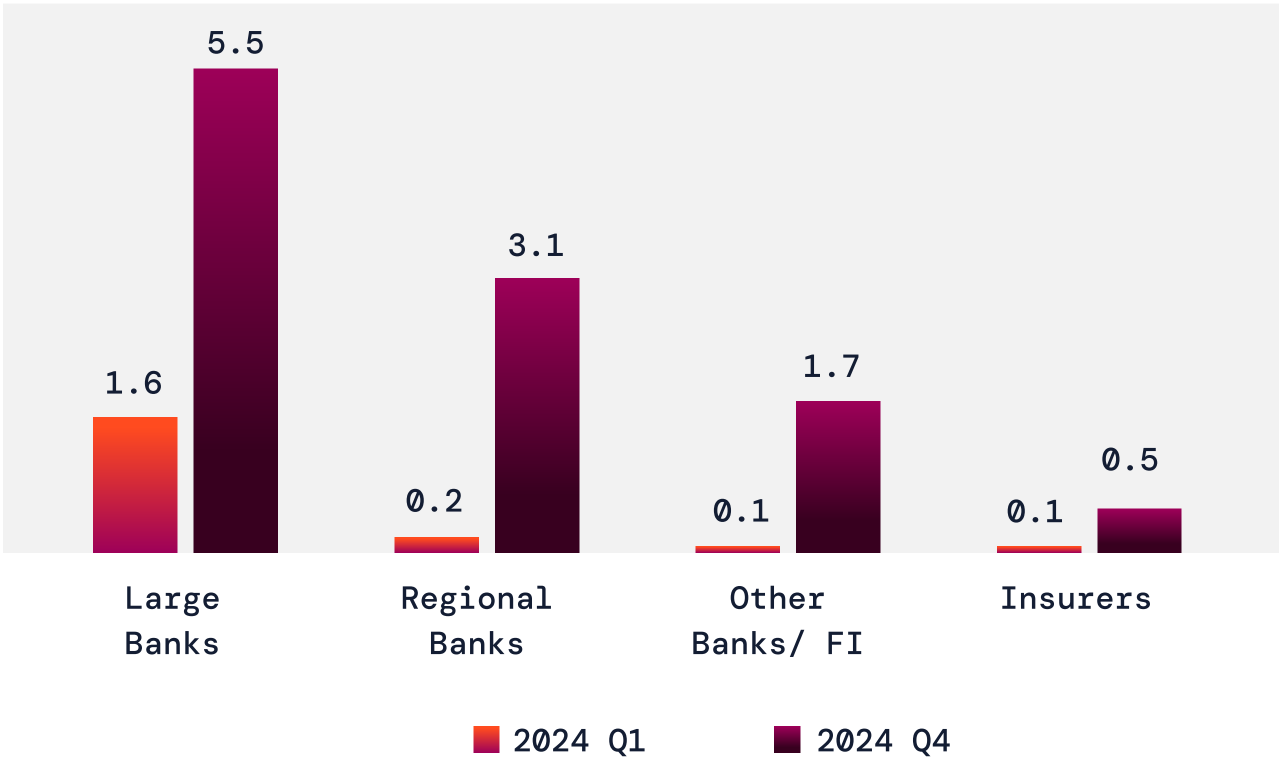
% Rise in Synthetic Voice Fraud Attacks During 2024



Large national banks face disproportionately higher deepfake fraud activity within the banking sector, with **5.5 attacks per day in Q4 2024**, up from 1.6 per day at the beginning of the year. Regional banks followed closely with 3.1 attacks per day in the same period. The insurance sector is also seeing a sharp rise, averaging **one deepfake attack every other day—a more than 5x increase** compared to Q1. Historically, fraud trends often emerge first in large and regional banks before spreading to insurers, and deepfake-driven fraud is following the same path.

SIGNIFICANT RISE IN DAILY FRAUD ACTIVITY ACROSS VERTICALS

Machine-Generated Voice Fraud Attacks per Day



Pindrop has identified a growing trend of fraudsters using voice modulation in contact centers. We analyzed 4,215 confirmed fraud calls across nine financial institutions and found that 952 calls (23%) showed evidence of voice manipulation.

What counts as synthetic voice manipulation?

Synthetic voice manipulation refers to any technique used to alter, generate, or replay a voice in a way that masks the speaker's true identity or intent. Common methods include:

- **Replay attacks** using pre-recorded or intercepted voice clips
- **TTS synthesis** to generate speech from written input
- **Voice cloning software** to mimic a specific person's voice
- **Live voice modulation** to change characteristics like pitch, tone, or accent in real time

CHAT WITH AN EXPERT

Synthetic voices, real consequences[21]

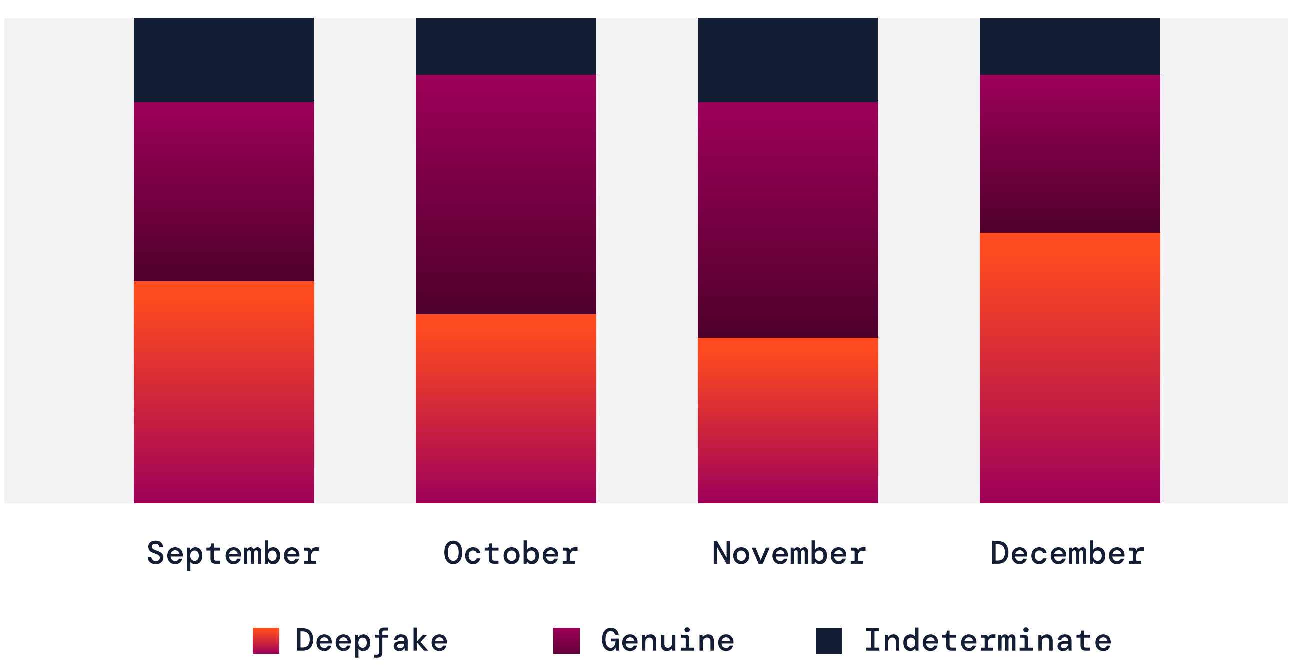
> Deepfake media surged online during the U.S. election cycle—Pindrop analysis reveals how fraudsters are optimizing for speed, believability, and detection evasion.

The Pindrop liveness detection solution for media can be used across social media and fact-detection platforms, and analyzes thousands of media files uploaded by users.

A deeper analysis of files uploaded during the four months surrounding the U.S. elections (Sep-Dec 2024) revealed that **40% of social media content was identified as deepfakes**, while only 45% confirmed as genuine. Deepfake activity climbed steadily through November, peaking during the election cycle before declining in December.

40% OF ANALYZED MEDIA FILES WERE DEEPFAKES

% of files

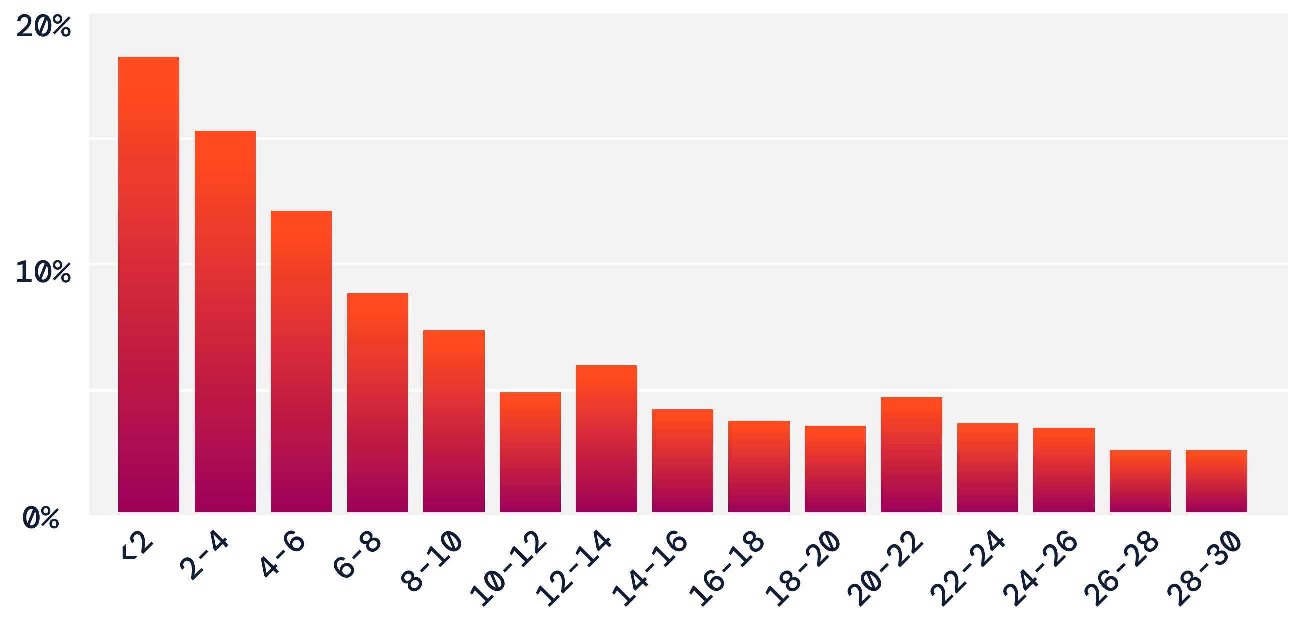


The net speech duration within each file is a critical factor in detecting deepfakes. Among the deepfakes analyzed, 67% were under 30 seconds, and over 80% of those were longer than 2 seconds—a duration sufficient for Pindrop models to deliver high-confidence detection. Some deepfakes extended beyond 6 minutes, showing that fraudsters are experimenting with various formats and lengths. This data helps us fine-tune our detection models to align with the evolving nature of online synthetic media.

The duration of the net speech available in these files is a crucial indicator of not only how accurately the Pindrop solution can detect these deepfakes but also how little time fraudsters need to create them to make them as realistic as possible.

DISTRIBUTION OF NET SPEECH OF DEEPFAKE FILES

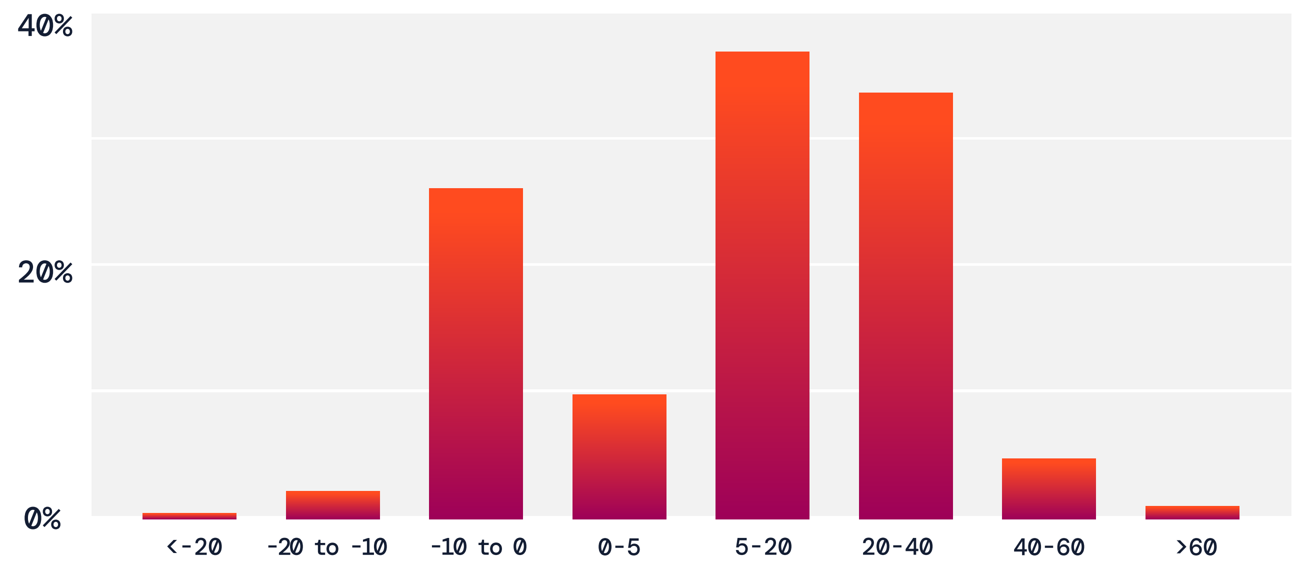
% of Files Under 30 Seconds That Belong in the Net Speech Category



The Signal-to-Noise ratio (SNR) also plays a key role in detection accuracy. SNR indicates the relative strength of the audio-visual cues that indicate a deepfake (the "signal") compared to the noise present. Higher SNR indicates better audio quality, improving the reliability of authenticity assessments. In our sample, 67% of media files had an SNR above 5, the benchmark for good audio quality.

DISTRIBUTION OF SIGNAL TO NOISE RATIO

% of Files That Fell Into the SNR Category



[21] Unless otherwise noted, all data in this section is from Pindrop analysis of social media data from customers for four months between Sep-Dec 2024

Introduction

State of the Industry

Security Landscape

Fraud by Vertical

Authentication Landscape

2025 Forecast

Fighting Fraud in an AI-First World

Conclusion

The evolving security landscape is reshaping how organizations and consumers engage. In times of heightened security risk, organizations often default to stricter security protocols, which can lead to frustrating customer experiences. Consumers increasingly expect interactions that are fast, seamless, and low-friction, yet still secure enough to protect their accounts, data, and identity.

This balancing act between security and customer experience strongly impacts identity verification and authentication processes.

Average handle time reveals the cost of complexity

Longer calls often point to friction in verification or resolution—AHT helps quantify what slows customers down.

To evaluate how authentication method influences average handle time, we examined three call types across 29 organizations:

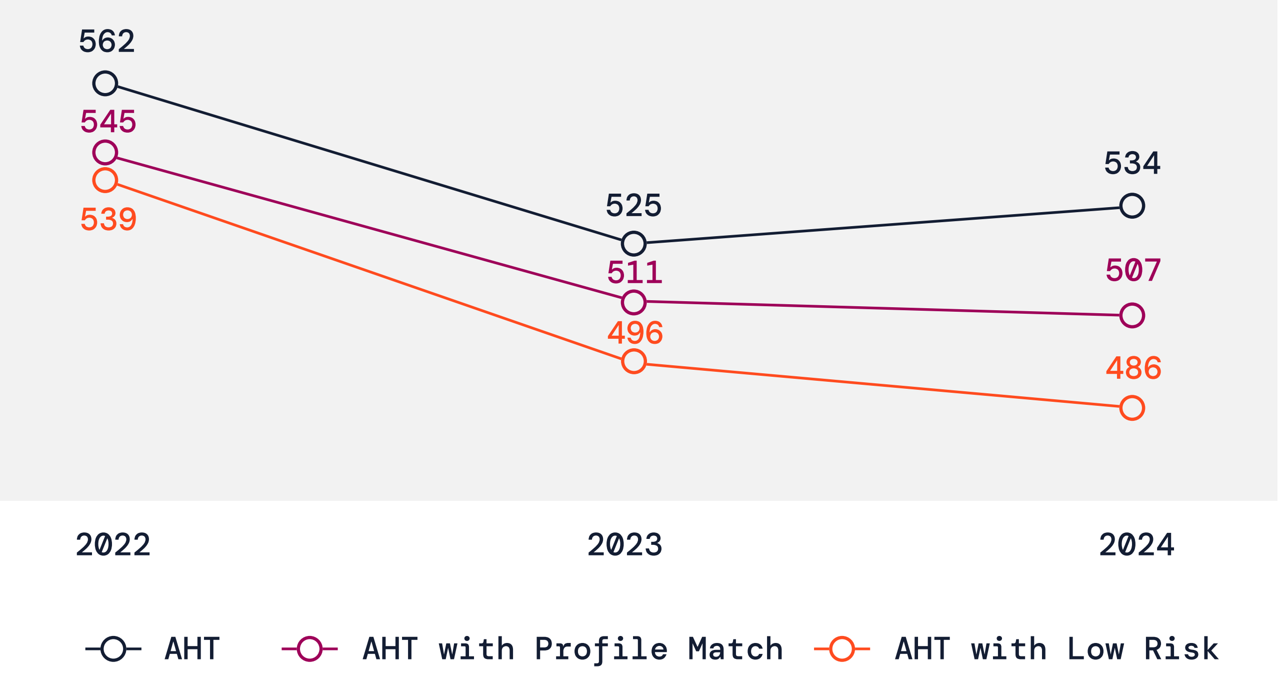
1. **Calls without authentication**
   No authentication signals applied; full KBA process required.

2. **Calls with full profile match**
   Enrolled device, voice, and behavior profiles matched—allowing agents to skip more than two KBA questions.

3. **Calls with low-risk assessment**
   Caller ID, spoof detection, and risk scoring applied early—enabling agents to reduce KBA by 1–2 questions before any profile matching.

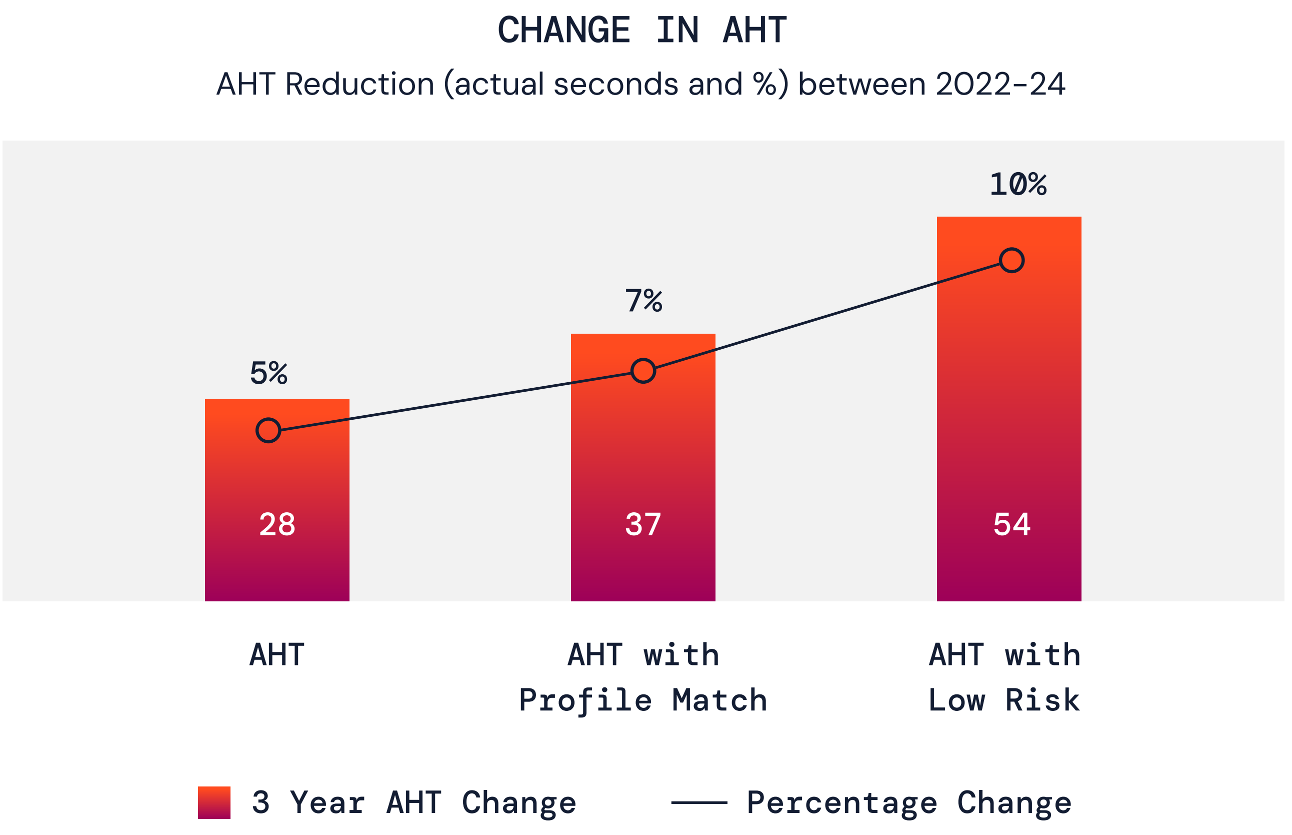
AVERAGE HANDLE TIME TREND

Agent handled call time (seconds)



Across Pindrop's customer base, AHT has steadily improved from 2022 to 2024:

- Pre-verification AHT dropped from **562 to 534 seconds** (9:22 → 8:54)
- Full profile match AHT decreased from **545 to 507 seconds**
- Low-risk caller AHT dropped even further, to **486 seconds** (8:06)—a **14% reduction overall**



Over the three years, Pindrop **multifactor authentication** reduced AHT by an additional **9 seconds**, while **low-risk assessments** saved **26 seconds** per call.

For a contact center handling 10M calls each year, this decrease in AHT equates to an estimated **$4.1M in annual savings**.

Why caller ID can't be trusted

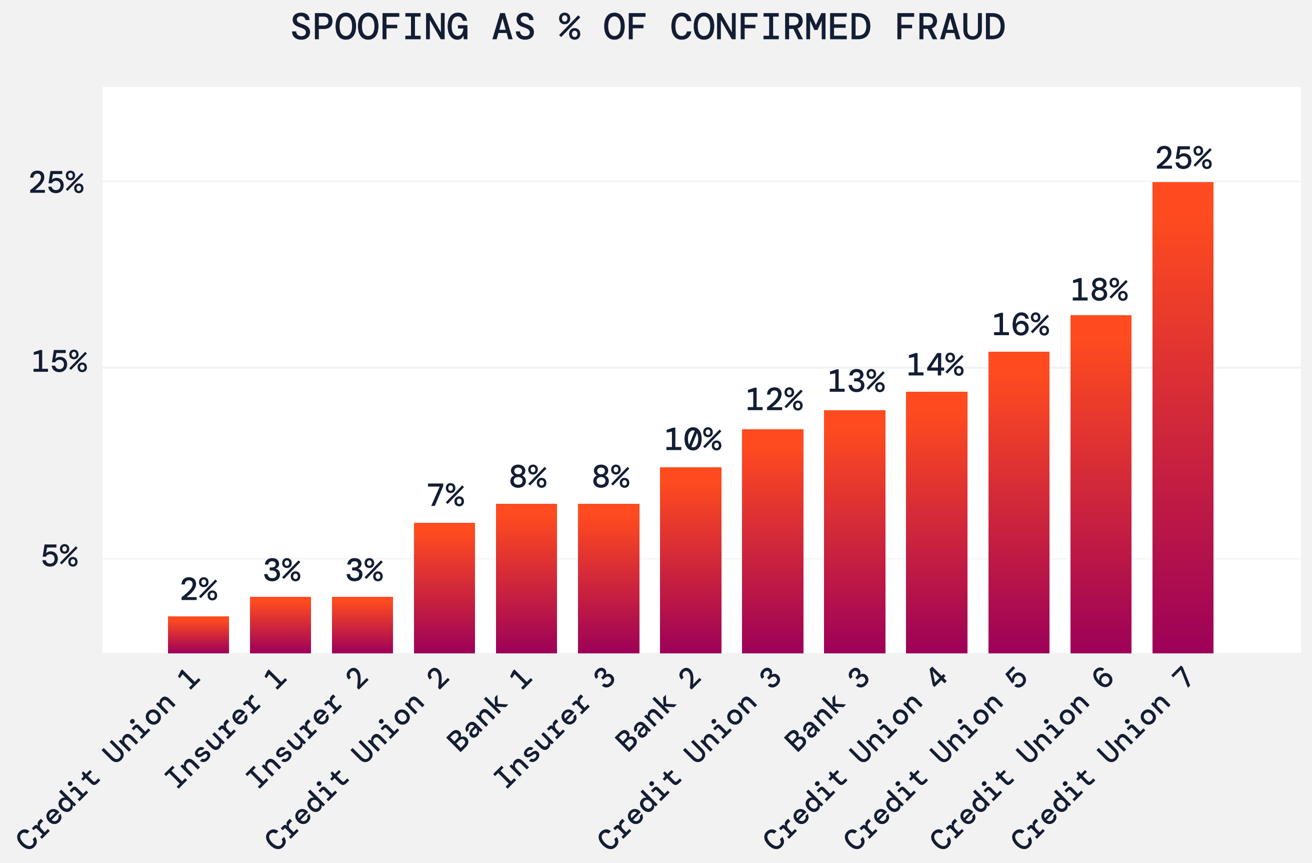
Many businesses rely on caller ID matching as a fast-track method to reduce handle time and streamline caller authentication. But this shortcut is increasingly exploited by attackers using techniques that make the phone number appear legitimate—while masking their true intent.

Common manipulation tactics include:

- **Spoofing**, which disguises the attacker's number to appear as a trusted contact
- **SIM swapping**, achieved by tricking mobile carriers into transferring a victim's number to a fraud-controlled device
- **Number porting**, used to reroute a victim's phone number to a new network under the attacker's control

These techniques undermine the reliability of caller ID, allowing attackers to bypass traditional authentication methods.

> Pindrop analyzed 4,635 confirmed fraud calls across 13 clients and found that roughly 1 in every 6 fraud calls involved some form of caller ID manipulation.



This growing trend highlights the need to move beyond ANI-based matching. Institutions should adopt real-time risk assessment methods that incorporate call paths, carrier metadata, audio characteristics, and originating locations to better evaluate caller legitimacy and reduce exposure to fraud.

CHAT WITH AN EXPERT

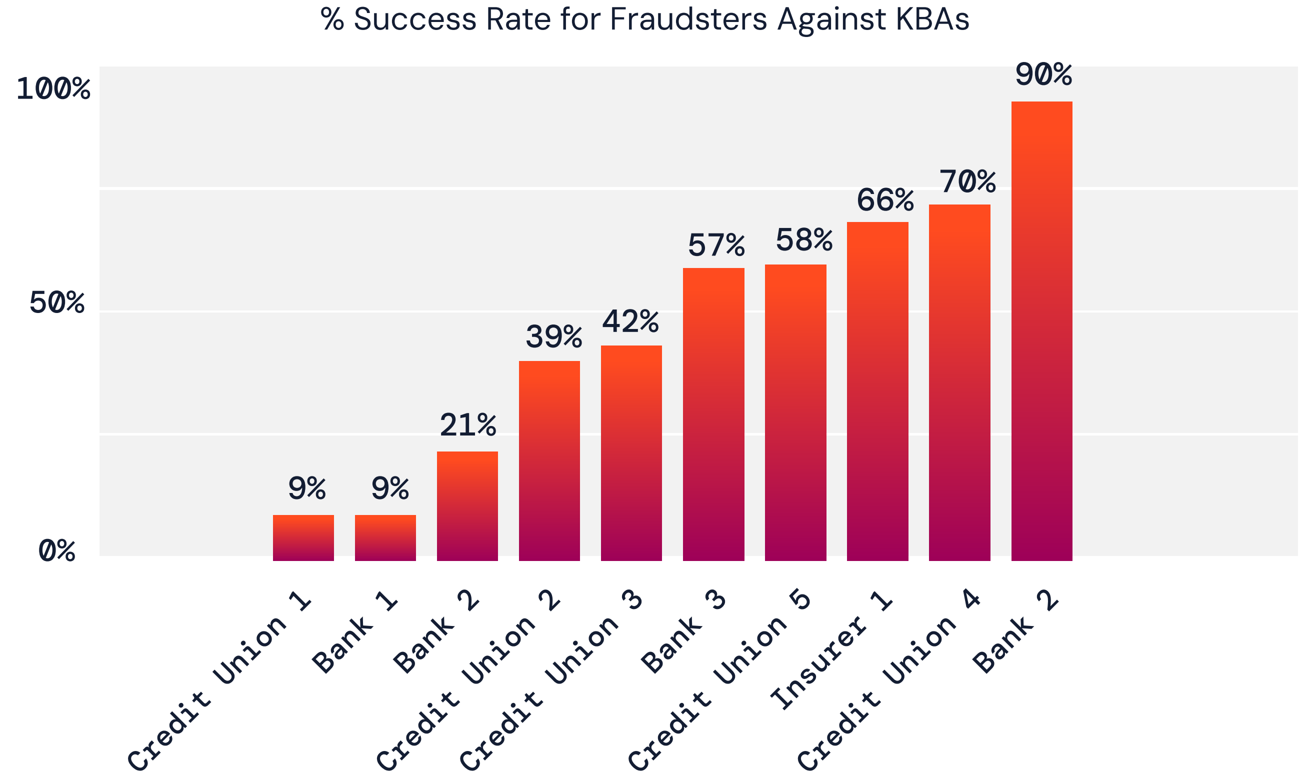
Outdated verification methods are fueling ATOs

> KBA and OTP are increasingly vulnerable—fraudsters succeed in up to 90% of KBA attempts and nearly 25% of OTP challenges.

Pindrop analyzed **2,490 fraud calls** across **10 financial institutions** to identify fraudsters' success rate patterns when prompted for a KBA response. On average, attackers succeeded **53% of the time**, depending on the business and the data available to the fraudster.

To evaluate the effectiveness of OTPs, Pindrop also analyzed **8,618 confirmed fraud calls** at a major financial organization. Over **1,300 fraudsters successfully passed the OTP challenge**, yielding a **22% success rate—nearly 1 in 4**.

FRAUDSTERS SUCCESSFULLY PASS KNOWLEDGE-BASED AUTHENTICATIONS (KBA)



By mimicking trusted channels and automating the attack, fraudsters turn the organization’s own security process into a tool for compromise. When OTPs are used as the sole authentication method, accounts remain exposed—especially in the absence of a layered or risk-aware strategy.

To reduce exposure, organizations must move beyond legacy methods like KBAs and OTPs and invest in multifactor authentication strategies that are more adaptive and significantly harder to exploit.

How OTP phishing bots work

A growing driver of ATO fraud is the use of OTP phishing bots—automated tools sold on dark web marketplaces and commonly deployed in social engineering campaigns. These bots allow fraudsters to intercept OTPs in real time, often without ever speaking to the victim.

A typical bot-powered attack unfolds like this:

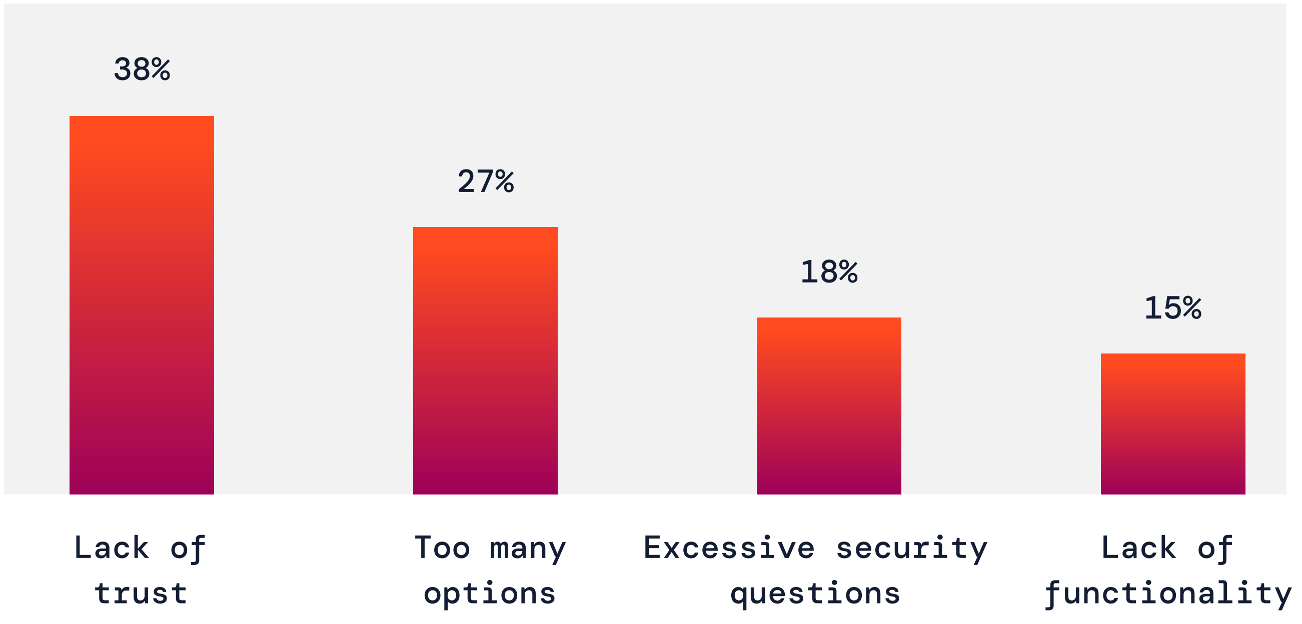
- **Spoofing the bank’s phone number** to make the call appear legitimate
- **Playing an automated message** that prompts the victim to take action
- **Triggering an OTP request** through the bank’s IVR or website
- **Asking the victim to provide the OTP** under the guise of verification
- **Capturing and displaying the code in real time** so the fraudster can complete the takeover instantly

Increased self-service requires customer-friendly authentication

Self-service is a key component of an organization's customer service arsenal. While the phone channel remains preferred for complex interactions, younger consumers and others tend to prefer web and mobile self-service for urgent transactions. The experience must be simple, efficient, and free from excessive security hurdles for self-service to work effectively.

TOP REASONS FOR WHY CUSTOMERS ABANDON PHONE SELF-SERVICE

% of Customers Who Rated A Particular Reason as Strong Driver for Abandonment



Source: Contact Babel: The Inner Circle Guide to Omnichannel (2023-24)

According to Contact Babel, "excessive security questions" is the third most common reason users abandon phone-based self-service and opt to speak with a live agent—a behavior known as "zeroing out."[22] In 2024, **9% of all self-service calls were abandoned**,[22] driving up contact center costs when agents needed to step in. Effective authentication, particularly methods that minimize KBA questions, directly reduces abandonment and improves self-service adoption.

Agentic AI promises intriguing opportunities to enhance self-service, with the potential to offer a concierge-like customer experience on the phone. These AI agents could anticipate user needs, recall past interactions, and streamline services. However, this potential is blocked by the need for secure and passive authentication. Without moving beyond outdated methods like KBAs and OTPs, the promise of intelligent, intentional self-service cannot be fully realized.

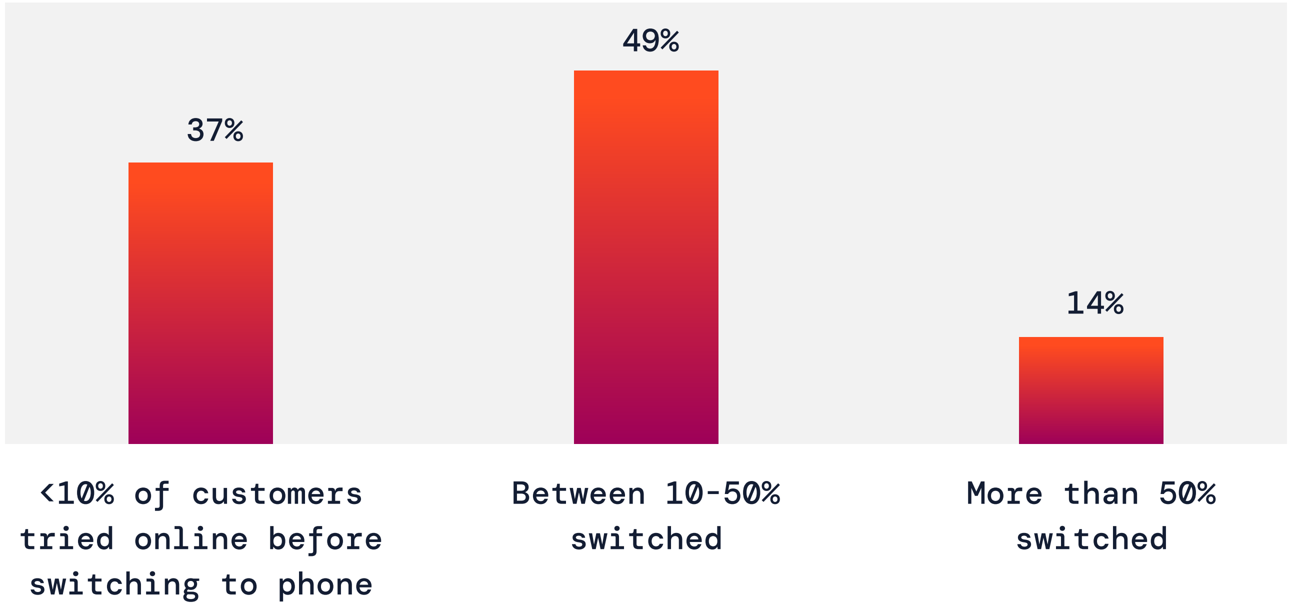
Enroll once, authenticate everywhere

An 'omnichannel' customer experience is crucial as customers increasingly prefer to interact with an organization through their channel of choice (e.g., phone, web, mobile, social). A well-crafted omnichannel strategy can drive better business outcomes.

According to Contact Babel, 75% of respondents felt that having an omnichannel approach improved the customer experience.[21] Despite the rise of digital channels, the phone remains a critical part of the journey. Contact Babel Omnichannel data shows that most consumers start online but often escalate to a phone call, especially when an issue becomes complex. Most contact centers found that up to 50% of customers switch between web and phone channels.[21]

THE VITAL ROLE OF PHONE IN OMNI-CHANNEL STRATEGY

Frequency of Contact Centers That Had Customers Switch from Web to Phone



Authentication that easily facilitates customers transferring across channels delivers a more seamless experience. For example, callers authenticated in the phone channel can be offboarded for a chat experience without re-authenticating, opening up channels like chat or SMS, which lack strong authentication methods.

[22] Contact Babel, "The Inner Circle Guide to Omnichannel (2023-24)"

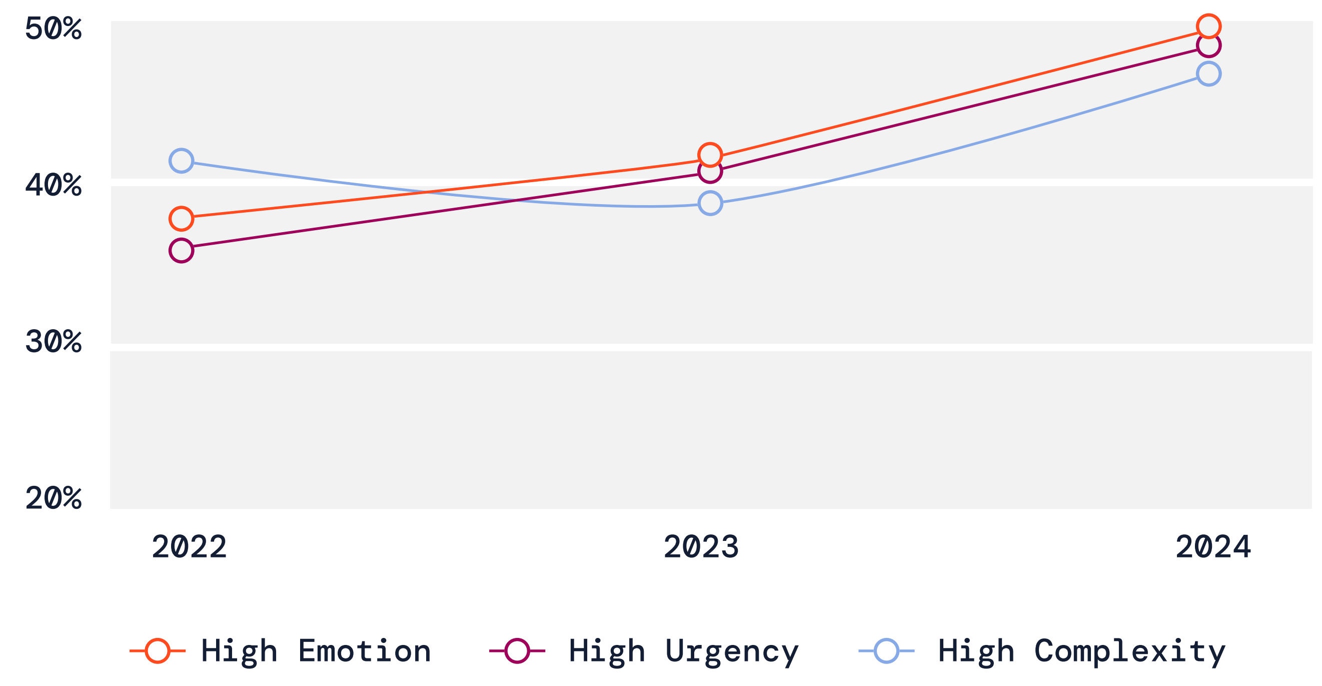
CHAT WITH AN EXPERT

Voice is the backbone of secure authentication

Amidst the rising adoption of omnichannel platforms, voice calls are still a cornerstone for crucial customer interactions. Between 2022 and 2024, Pindrop's cloud customer base witnessed a substantial 15.5% surge in voice call volumes[23], solidifying voice as the preferred choice for high-stakes, time-sensitive, or emotionally charged scenarios.

VOICE CALLS GROWING FOR HIGH INTENSITY INTERACTIONS

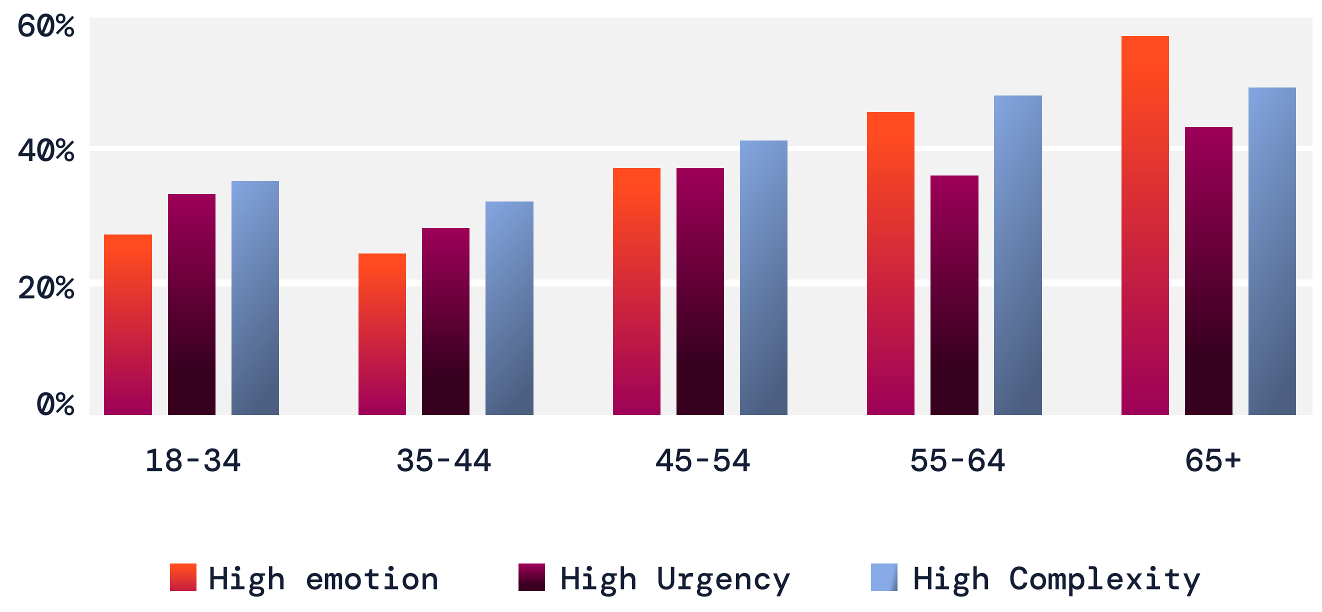
% of Customers Who Prefer Voice Channel



Voice remains the leading channel for complex service needs among older consumers (+55), who comprise 30% of the U.S. population. Even among younger demographics, more than 20% still prefer voice for high-impact interactions.

OLDER GENERATIONS PREFER VOICE CHANNEL

% of Customers Who Prefer Voice Channel



Market shifts reflect this continued relevance. Over the last 12 months, most leading conversational AI providers—including Sierra, Talkdesk, and ElevenLabs—have launched voice-enabled agents, expanding beyond text-based chatbots and reaffirming the importance of voice across all forms of customer communication.

However, as the voice grows in strategic importance, so does its risk profile. The increased use of synthetic voice, both legitimate and malicious, has significantly expanded the attack surface. Voice-based threats are no longer limited to the contact center. In multiple incidents, fraudsters have impersonated senior executives to deceive finance teams and operations staff outside traditional support channels.

Organizations that rely on passwords, KBAs, OTPs, and standalone voice biometrics must reassess their security posture. Voice-based attacks are now moving into less-protected areas of the enterprise, where legacy methods fall short. In industries like engineering and manufacturing, often outside the D2C spotlight, companies have reported average losses of $14 million per incident due to voice fraud[24].

As the threat of voice-based attacks continues to rise, Pindrop customers are investing significantly in voice authentication. This proactive approach helps them meet the growing threat and strengthens their defenses with deepfake detection. Even new adopters, who had not previously deployed voice biometrics, are now recognizing the urgent need for a secure voice authentication and deepfake detection platform.

It's becoming increasingly clear that the key to accurately distinguishing real customers from synthetic threats lies in the strategic combination of technologies. As voice continues to be central to customer engagement, securing this channel is not just critical—it's essential. This approach is effective not only in preventing fraud but also in protecting trust and delivering safe, seamless customer experience.

[23] Pindrop analysis of call volumes from customers between 2022-24
[24] https://www.cyberdefensemagazine.com/exploring-the-vishing-threat-landscape/

CHAT WITH AN EXPERT

Introduction

State of the Industry

Security Landscape

Fraud by Vertical

Authentication Landscape

2025 Forecast

Fighting Fraud in an AI-First World

Conclusion

In 2024, fraud continued its upward trajectory. According to the FTC, reported losses rose **25% year-over-year**, reaching **$12.5B**.[25] The Identity Theft Resource Center (ITRC) predicts that declining victim support and reduced law enforcement focus will lead to a further rise in identity fraud in 2025.[26] Meanwhile, Gartner projects a 300% increase in fraud attempts by 2027 compared to 2023—potentially driving organizations to layer on more complex security, often at the expense of customer experience.[27]

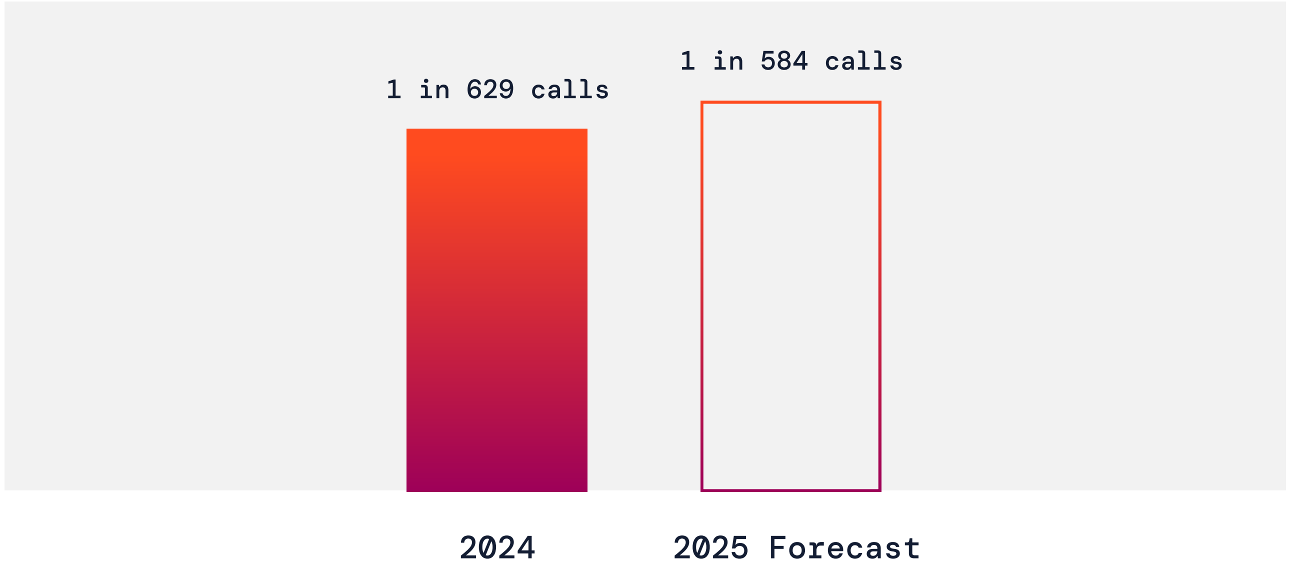
PINDROP PREDICTION

Contact center fraud is projected to grow +8% in 2025

Pindrop observed a significant increase in contact center fraud across banking, insurance, and retail sectors in 2024. Based on early data from January-February 2025, this trend shows no signs of slowing. We predict that the fraud rate will continue to grow by 8% year-over-year, with **1 in every 584 calls being fraudulent**.

FRAUD FORECASTED TO GROW BY +8% IN 2025

% of Incoming Calls That Are Fraudulent



At these levels, **contact centers in the U.S. could potentially be exposed to a fraud risk of $44.5B in 2025**. Organizations need to adopt the technologies, processes, and structural changes that could help defend against this new wave of AI-driven fraud.

How leading contact centers are fighting back

- Unpack 5 real-world tactics to harden contact center defenses
- Trace how MFA and deepfake detection play out in practice
- Demystify what's actually working to shut down phone fraud

Take a closer look ⟶

[25] Federal Trade Commission, Consumer Sentinel Network: Data Book 2024 (Washington, DC: Federal Trade Commission, 2024).
[26] https://www.idtheftcenter.org/wp-content/uploads/2024/12/ITRC_2025Predictions_Report.pdf
[27] Gartner: Predicts 2025: Voice-Based Customer Service Isn't Going Anywhere, 6 December 2024

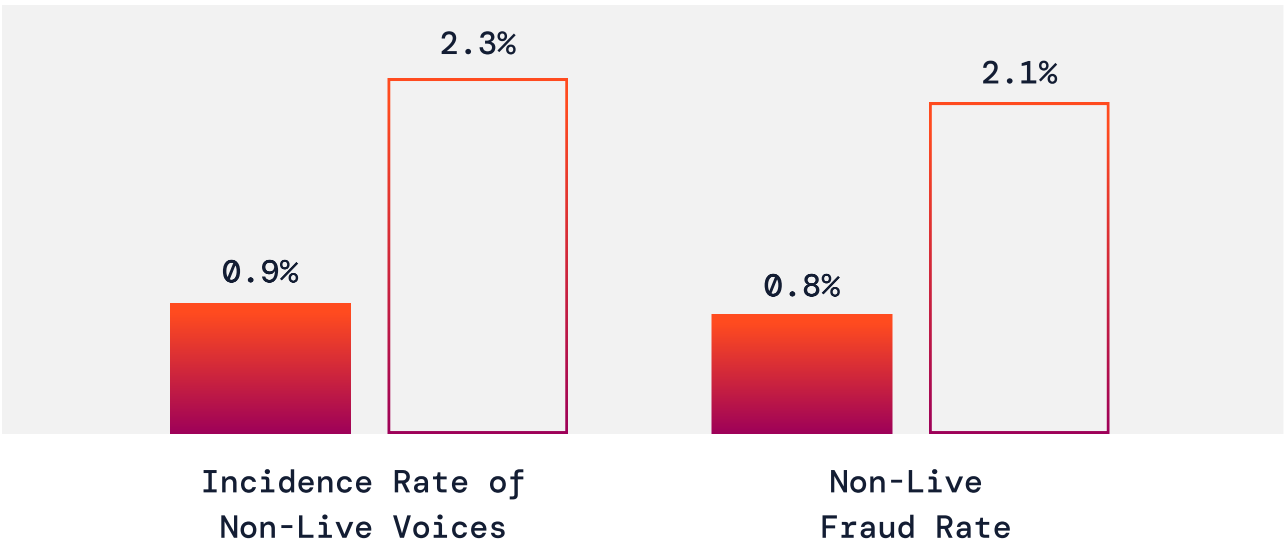
PINDROP PREDICTION

2025 deepfake fraud forecast shows +162% increase

According to Signicat, 42.5% of fraud attempts are now AI-driven. Deepfake fraud spiked across our customer base in 2024, and we project it will keep rising. We predict that deepfake activity will increase by +155%, and deepfake-related fraud will grow +162% by the end of 2025.

DEEPFAKE FRAUD FORECASTED TO RISE IN 2025

Non-Live Calls % of Total Calls / Non-Live Fraud as % of Total Fraud



The line between real and fake is vanishing—voice security must adapt

From open-source voice tools to small language models (SLMs), six emerging trends are poised to accelerate fraud and redefine how organizations protect trust in voice.

1. **Rise of open-source voice synthesis tools**
Open-source TTS and voice cloning models are reducing the time, cost, and expertise required to create hyperrealistic deepfakes—enabling fraud at scale.

2. **Increased risk of audio breaches**
Fraudsters are exploiting vulnerabilities in microphones, headsets, and connected devices to capture private audio. These intrusions raise the risk of data leaks, brand damage, and reputational loss.

3. **Targeting of high-value individuals**
Executives, public figures, and high-net-worth individuals are being targeted with deepfakes designed for fraud, extortion, and industrial espionage.

4. **Erosion of consumer trust**
As deepfake incidents grow, failure to secure customer data and interactions may lead to declining consumer confidence, lost revenue, and long-term brand harm.

5. **Limits of watermarking and self-regulation**
While commercial AI models have introduced watermarking and detection partnerships, open-source tools remain largely unregulated, allowing fraudsters to bypass protections. Detection systems must evolve to handle both commercial and open-source threats.

6. **Emergence of small language models (SLMs)**
Domain-specific AI tools like Deepseek R-1 are easier to run, tune, and control—making them attractive to attackers seeking low-cost, hyper-targeted fraud strategies using consumer-grade hardware.

PINDROP PREDICTION

AI advancements will continue to open new doors for fraud

The rapid evolution of AI—particularly in human-like speech, video, and autonomous agents—is blurring the line between real users and synthetic activity. Fraud teams are already seeing signs of AI-powered deception that blends seamlessly into trusted workflows, making it harder than ever to distinguish between legitimate customers, authorized AI agents, and malicious actors.

Emerging technologies like agentic AI (which can perform tasks independently), operator AI (which navigates across systems), and cost-effective models like DeepSeek are placing powerful capabilities in the hands of attackers. What once required technical skill and budget is now accessible with open-source tools and minimal infrastructure.

These advancements are powering a new generation of fraud that is faster, cheaper, and harder to stop:

- **AI agents can now execute multi-channel attacks** that slip past legacy fraud systems without triggering alarms.
- **Machine learning is being used against defenders**, identifying and bypassing security controls in real time.
- **Hyper-realistic impersonation is no longer expensive**, allowing attackers to mimic voices and behavior at scale with minimal effort.

As AI continues to integrate into authentication and transaction processes, distinguishing between legitimate and fraudulent activity becomes less about surface cues and more about identifying intent. Organizations will need to shift from static defenses to intelligent systems capable of recognizing patterns, context, and anomalies in real time.

Pindrop

What Agentic AI Means for the Future of Fraud

The Deepfake Threat Playbook

Explore real-world use cases, emerging risks, and what security teams need to know.

Read the guide →

PINDROP PREDICTION

Emerging risk: Deepfakes in real-time communications

A significant risk factor on the horizon is the use of deepfakes in real-time communication systems like virtual conferencing. Considering that 14% of U.S. employees work fully remote[28] and 62% of U.S. companies offer a hybrid work model,[29] securing platforms like Zoom and Microsoft Teams is crucial to a company's overall cybersecurity posture.

Deepfakes are now a major threat to remote collaboration. A recent Medius survey found that 92% of all businesses have experienced some financial losses due to deepfakes.[30] It also showed that 44% of companies lack confidence in detecting deepfakes. Across industries, businesses have lost an average of nearly $450,000 to deepfakes, with 28% reporting losses exceeding $500,000.

Pindrop analysis of customer data shows that the average business has $343,000 in deepfake exposure in the contact center phone channel alone, while the exposure to the entire company may range between $1.5M and $2M. Fraudsters are exploiting synthetic audio and video in virtual meetings, and our customers have concerns about the impersonation of executives, customers, partners, new employees, and hiring candidates.

Nearly 40% of cybercriminals use Microsoft Teams and Zoom as the mechanism to contact their targets as part of multi-channel attacks after initiating the attack through email phishing.[31] Compared to the previous year, fraud via Microsoft Teams is up 104.4%, and fraud via Zoom increased 33.3% in Q1 2024 alone.[32]

As deepfakes evolve, organizations must act swiftly to secure real-time communications channels. Failure to do so could leave a critical vulnerability open, one that fraudsters are already exploiting at scale.

PINDROP PREDICTION

Retail fraud to more than double in 2025

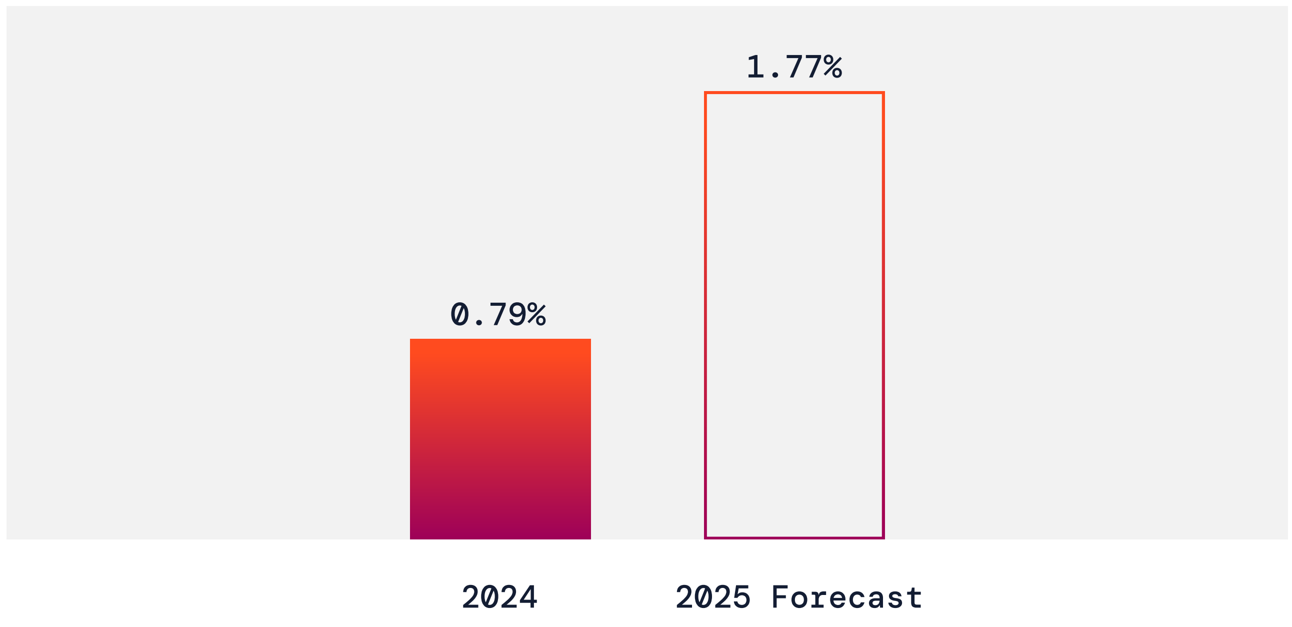
According to Pindrop data, retail fraud surged +107% between 2023 and 2024. We anticipate this rate to more than double again in 2025, fueled by increased use of automation, synthetic voices, and voice modulation by fraudsters.

> The research team at Pindrop predicts retail fraud activity could reach **1 in every 56 calls** in 2025.

Over 200 major U.S. retailers are in the crosshairs, with an estimated $23B in fraud exposure.[33] Fraudsters are actively exploiting customer-friendly returns policies offered by e-commerce vendors. With tactics evolving and call volumes rising, the threat to retail contact centers is only expected to grow.

RETAIL FRAUD FORECASTED TO DOUBLE IN 2025

% of Calls That Are Confirmed Fraud



[28] Pindrop, The $23B Fraud Problem in Retail, 2025.
[29] Neat, "Top Remote Work Statistics for 2024," Neat.no, accessed April 8, 2025.
[30] Zoom, "Hybrid Work Trends: Flexibility, AI, and the Office," Zoom Blog, February 6, 2024.
[31] Stacey James, An Accounting of Financial Professionals, webinar, Medius
[32] Egress: Phishing Threat Trends Report, 2024 (Teams was used in 30.8% attacks and Zoom in 8.9%, thus adding to nearly 40%)
[33] Egress: Phishing Threat Trends Report 2024

Introduction

State of the Industry

Security Landscape

Fraud by Vertical

Authentication Landscape

2025 Forecast

Fighting Fraud in an AI–First World

Conclusion

Fraudsters are rapidly adopting new AI tools to automate, scale, and evolve their attacks. Enterprises must defend themselves and their customers from fraud at a new level of speed, scale, and sophistication. As attack vectors become more agile and complex, the challenge for enterprises isn't just keeping up but staying ahead.

Even as organizations strengthen their defenses, they must not lose sight of the bigger picture: delivering a secure and seamless customer experience.

The path forward lies in deploying advanced detection technologies that can outpace fraudsters while defending your enterprise and your customers. In an AI-first world, the winners will be those who strike the right balance between trust, security, and experience.

Defend your enterprise against deepfakes

As AI becomes more accessible, fraudsters have a growing arsenal of tools to launch attacks on multiple fronts.

Organizations must take proactive steps to defend themselves, particularly in three high-risk areas:

1. CONTACT CENTERS

Deepfake activity targeting contact centers has surged, with fraudsters using increasingly sophisticated voice synthesis and manipulation tools. It's essential for organizations to accurately determine whether a human is on the other end of the phone call. Pindrop recommends following best practices:

1A. Use AI-based liveness detection with multi-signal risk analysis

Traditional voice recognition systems and human agents are ill-equipped to detect deepfakes accurately. AI-powered liveness detection, trained to identify machine-generated artifacts, offers significantly higher accuracy. Detection capabilities are further strengthened when combined with independent risk signals like device, behavior, and network metadata.

1B. Train detection systems on known AI models

Most fraudsters use commercial or open-source TTS and voice conversion models to create attacks. By training deepfake detection systems on a wide variety of these tools, organizations improve their ability to identify synthetic audio accurately.

1C. Implement source tracing

Detection systems should be capable of identifying the source components, such as the TTS engine (e.g., ElevenLabs), acoustic model (e.g., Tacotron), and vocoder (e.g., Wavenet) used to create the deepfake. This insight helps refine detection accuracy and provides valuable intelligence for risk mitigation.

1D. Use deepfake signals in authentication

Deepfake detection should be an input for both the caller's enrollment and authentication. Any presence of synthetic audio, especially when combined with other risk factors, should trigger "do-not-authenticate" protocols and prevent the creation of fraudulent profiles.

CHAT WITH AN EXPERT

2. ONLINE MEDIA

Organizations handling user-generated content, like media outlets, social platforms, and public institutions, face increased risk from deepfakes and misinformation.

Pindrop data reveals widespread deepfake activity surrounding significant events like elections. To prevent misinformation, brand damage, and audience churn, these organizations should implement liveness checks on all uploaded content to verify authenticity in real time.

3. REAL-TIME COMMUNCATIONS

With remote work now widespread, virtual conferencing tools such as Microsoft Teams, Zoom, and Webex are vital. However, fraudsters using synthetic audio and video are also increasingly targeting these tools.

Emerging threats include:

- Executive and customer impersonation
- Fake job candidate interviews
- Corporate espionage in sensitive meetings
- Deepfake-led social engineering for financial gain

Gartner advises organizations to "explore real-time deepfake detection for videoconferencing platforms, but recognize that this is still nascent and unproven," while also to “harden business processes to protect employees against deepfake-augmented social engineering attacks.”[31]

Recommended safeguards include:

- Real-time liveness detection for synthetic audio and video
- Continuous monitoring throughout the interaction
- Fast detection and alerting during time-sensitive engagements (e.g., hiring, high-value transactions, internal strategy sessions)
- Detailed forensic insights, including when and where a deepfake was detected in the interaction

This layered approach empowers cybersecurity teams to intervene before fraudsters can act, closing a critical gap in today’s real-time communication infrastructure.

[31] Gartner: How to Mitigate Deepfake Identity Impersonation Attacks, 5 February 2025

CHAT WITH AN EXPERT

Advance the fight against fraud

AI-driven deepfake detection is vital for any fraud defense. Enhancing your fraud detection strategies to help fortify your enterprise against unforeseen threats from multiple angles is equally important. Some key strategies include:

AI for fraud detection

AI can be a very effective tool for automating fraud detection and investigation. By integrating speech recognition tools and LLMs into your fraud case management tools, you can boost the productivity of fraud analysts. AI can automatically transcribe cases, identify key risk indicators, and summarize risk factors for quick review. These capabilities help reduce review time, prioritize critical cases, and mitigate false positives, allowing analysts to focus on what matters most.

Fraud 'look-back' technology

A real-time fraud detection and investigation system is essential, but it is only part of the solution. Organizations also need the ability to review past calls using new insights uncovered during fraud investigations.

Fraud often isn't isolated. One case can be part of a more extensive network of related activity, linked by shared caller IDs, voiceprints, or account behavior. For example, the same synthetic voice or spoofed number used in a new fraud case may appear in past calls that initially went undetected.

Today, some of this analysis is performed manually, in batch mode, which is less efficient. Fraud look-back technology automates this process, allowing organizations to re-score past calls in real time within a specific time window and helps flag additional high-risk calls. This rescoring can help uncover up to 22% more fraud and save millions of dollars in fraud exposure.[34]

Robust device analysis

Analyzing risk signals from a caller's device yields valuable intelligence, especially when integrated into a multifactor risk detection framework. As fraudsters increasingly manipulate caller ID, organizations must strengthen their ability to detect suspicious behavior at the device level.

One effective strategy is to use non-speaker audio signals such as microphone and device type, codec, carrier, and network type. These signals can reduce reliance on carrier signaling metadata or DTMF keypresses and extract risk signals passively. By integrating advanced device analysis, organizations can stay ahead of evolving fraud tactics and catch more threats.

[34] Derived from Pindrop data from beta of large national bank; alert rate of rescored calls that were fraudulent compared to alert rate of original fraud calls

CHAT WITH AN EXPERT

Strengthen authentication to enhance the customer experience

Authentication and fraud defense go hand-in-hand. As customers increasingly expect an easy, omnichannel, and secure experience, enterprises should ensure their identity verification strategies meet (or exceed) those expectations.

Reduce OTP dependence with passive device authentication

OTPs are not only an expensive way to authenticate, but they are also actively being targeted by fraudsters. OTPs also add additional steps in the authentication process, which can detract from the customer experience.

Each caller's device emits a range of audio, metadata, and DTMF signals that can be used to build a trusted profile and detect risk, without interrupting the experience. By replacing OTPs with passive device authentication, organizations can speed up authentication and improve the customer experience.

Enhance voice authentication with liveness detection

Voice remains an important channel for customer interactions. In a recent survey of 21 Pindrop customers, voice authentication was ranked as the most preferred way of authenticating users, followed by device analysis. PINs and passwords were less favored, while OTPs and KBAs ranked lowest.

It is important to add liveness detection to voice and device analysis to keep voice authentication secure and frictionless. This supports a passive and user-friendly experience for customers.

Enable advanced spoof detection without metadata

Fraudsters are increasingly manipulating carrier metadata to bypass spoof detection. However, non-speaker audio signals like device type, audio spectrum, compression, and other call characteristics are much harder to fake.

By analyzing these signals in real time, organizations can:

- ✓ Detect spoofing attempts without relying on carrier metadata
- ✓ Increase validation and spoof detection rates by using multiple factors
- ✓ Shorten call durations while improving fraud detection

This approach helps catch more spoofing attempts while reducing the call duration by eliminating keypresses.

Support omnichannel authentication

Customers use voice in multiple channels, including speech-to-text or natural language interaction with digital applications.

To streamline the user experience and reduce excessive security questions, organizations should implement cross-channel authentication that:

- Passively authenticates users in one channel based on a combination of voice and liveness
- Carry that trust forward to other channels, reducing repeat authentication steps
- Enables smoother transitions to digital self-service options and emerging tools like agentic AI

This approach minimizes friction, supports omnichannel journeys, and builds trust through consistent and secure experiences.

Introduction

State of the Industry

Security Landscape

Fraud by Vertical

Authentication Landscape

2025 Forecast

Fighting Fraud in an AI-First World

Conclusion

From insight to action

Today's fraud landscape is layered—built not from a single threat but from a convergence of pressures: economic instability, automation, and the widespread accessibility of Gen AI. These forces don't operate in isolation—they compound, creating attack chains that are more scalable, more deceptive, and harder to detect.

Voice, once considered a strong signal of trust, is now under direct threat. Synthetic speech generation, real-time voice conversion, and bot-driven interactions are readily available and increasingly effective. Fraudsters are layering these tools to impersonate individuals, manipulate systems, and exploit gaps in traditional security frameworks.

In response, defenses must evolve rapidly. No single control is sufficient. Organizations must adopt a layered approach—combining liveness detection, voice and device intelligence, behavioral analysis, and real-time risk signals. Just as fraud tactics now operate across multiple vectors, security systems must do the same to remain effective.

The core question has changed. It's no longer just, "Is this the right person?"—now it's also, "Is this even a human?" In a world where synthetic voices can replicate emotion, tone, and nuance, the voice is no longer a guaranteed marker of authenticity. It can be generated, cloned, or manipulated—making it both a high-value signal and a high-risk surface.

About Pindrop

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

Pindrop®