



Continuous identity verification for the AI era

Deepfakes are moving through every business channel you rely on—which means identity can't be verified just once anymore. Pindrop gives CISOs one continuous layer of trust across voice, video, and digital interactions.

Identity is the new security perimeter

GenAI lets attackers sound, look, and behave like trusted customers, employees, and vendors. Traditional controls weren't designed to catch this deception, leaving enterprise security teams struggling to identify and respond to the threats against their systems.

The Real Human + Right Human™ platform

Pindrop provides the continuous AI identity verification layer across audio and video that restores trust in every real-time communication. It integrates into high-trust interactions, like your customer voice channels, to help answer three critical questions.



Machine or human?

Detect synthetic speech, bots, and recorded or replayed audio the moment a call or meeting connects.



A bad actor?

Score every interaction for attack risk using device, network, behavior, and consortium signals.



Your customer?

Passively authenticate legitimate callers across voice, device, and deepfake signals.

The AI threat by the numbers

\$40B

Projected GenAI-amplified fraud losses in banking by 2027¹

62%

Of companies already hit by a deepfake²

13.9×

Growth in AI attacks since Q4 2024, as of Q1 2026³

One identity layer for real-time communications

For enterprise security leaders, Pindrop is **the** continuous identity verification layer. The platform combines deepfake detection, risk detection, and passive authentication across voice, video, and digital workflows—so institutions can reduce risk, lower operating costs, and improve legitimate customer and employee experiences.

REFERENCES

¹Deloitte Center for Financial Services, projected GenAI-amplified fraud losses in U.S. banking by 2027.

²Gartner, "Data View: What is the Impact of GenAI on the Attack Landscape?," August 2025

³Pindrop analysis of AI attack growth, Q4 2024 – Q1 2026.

Four products, one trust platform

Solutions to the AI identity problem map to Pindrop's four products: deepfake detection in meetings, deepfake detection in calls, risk detection, and passive, multifactor authentication.

Pindrop Pulse® for Meetings

Real human. Right human. Right location.

PROBLEM

AI and human impersonation in virtual meetings, including fake candidates, executives, and vendors.

HOW IT WORKS

Real-time video and audio deepfake detection, plus location intel, integrated into your existing meeting platform.

USE

Defend against AI attacks during high-risk business interactions, including remote hiring conversations.

<1% false positive rate · 75 deepfake patents
· 99% audio deepfake detection against known engines⁴

Pindrop Pulse® for Calls

Bot? Blocked. Human? Welcome.

PROBLEM

Bots, recorded or replayed calls, and synthetic callers that agents and IVR systems can't reliably identify.

HOW IT WORKS

Detects non-live calls in the IVR and at the agent leg; supports risk reduction from AI-backed attacks in the contact center.

USE

Restrict IVR self-service, raise verification requirements, and flag risky transactions.

<1% false positive rate · 75 deepfake patents
· 99% audio deepfake detection against known engines⁴

Pindrop® Protect

Real-time risk score. Real-time answers.

PROBLEM

Risk detection must catch bad actors without punishing legitimate callers.

HOW IT WORKS

Voice, device, behavior, network, and risk, distilled into one clear signal fraud teams can act on.

USE

Defend against attacks and fraudulent calls in the contact center.

\$3.4B fraud losses prevented · 3.4M fraud calls detected · 2.52M unique fraud profiles⁵

Pindrop® Passport

Seamless authentication. Better CX.

PROBLEM

Legacy authentication frustrates real customers and can still fail when attackers have the right answers.

HOW IT WORKS

Passive authentication using voice, device, behavior, and network signals.

USE

Elevate IVR self-service, reduce agent verification time, and lower reliance on OTP/KBA.

45 sec average handle time saved · +1.5% IVR containment · ~\$4M average yearly savings⁶

REFERENCES

⁴Pindrop, "Exposing the Truth about Zero-Day Deepfake Attacks," (<https://www.pindrop.com/article/truth-about-zero-day-deepfake-attacks/>) July 2023 and Pindrop analysis of call data of Pulse customers from Q4 2024 to Q2 2025.

⁵Pindrop internal data analysis.

⁶Forrester Consulting Report, <https://go.pindrop.com/resources/report/total-economic-impact-study-of-pindrop/>

The real business outcomes

With fraud detection, deepfake detection, and multifactor authentication across CX and employee experiences, Pindrop helps you bring trust back to the conversation—and better defend your bottom line.



Reduce risk

Detect deepfakes, attackers, replay attacks, spoofing, synthetic voice, and account takeover signals before money moves.



Lower operating costs

Improve IVR decisions, reduce manual investigation work, and give feedback to agents with real-time risk and authentication signals.



Improve CX

Authenticate legitimate customers with passive, multifactor signals instead of forcing more questions or OTPs.

Backed by 15 years of experience

14 of 20

Top financial banks served

1.3B+

Interactions analyzed annually

2.5M+

Known fraudsters in consortium

300+

Patents across portfolio

CUSTOMER OUTCOMES

First National Bank of Omaha

BANKING

47% decrease in average ATO loss per account; >75% decreased OTP usage; 4–5K monthly fraudulent calls relieved from the agent queue.⁷

Virginia Employment Commission

PUBLIC SECTOR

\$560K estimated fraud losses avoided in 8 months; \$840K potential annualized savings.⁸

Leading healthcare company

HEALTHCARE

>30,000 bot calls identified and neutralized; >\$73M HSA account balances defended; 94.3% reduction in bot calls, Jan.–Apr. 2026.⁹

Michigan State University Federal Credit Union

BANKING

58 seconds faster authentication; \$2.57M reduction in fraud exposure; and 10% increase in member satisfaction.¹⁰

REFERENCES

⁷First National Bank of Omaha case study, <https://www.pindrop.com/research/case-study/first-national-bank-omaha/>

⁸Virginia Employment Commission case study, <https://www.pindrop.com/research/case-study/virginia-employment-commission-reduced-fraud-within-months/>

⁹Anonymous leading healthcare organization and Pindrop customer.

¹⁰Michigan State University Federal Credit Union, <https://www.pindrop.com/research/case-study/msufcu-minimizes-fraud-exposure-by-millions/>