Pindrop | HealthEquity

90% Drop in Fraud and a Smoother CX: How HealthEquity Did It

At a glance: HealthEquity anticipated AI attacks—and turned to Pindrop to strengthen its security strategy without losing sight of its member-first mission.

PROBLEM

HealthEquity knew AI fraud attacks would target their voice channel. They needed measures to catch the attacks, but refused to sacrifice their world-class customer experience.

SOLUTION

HealthEquity partnered with Pindrop, adding AI-powered risk analysis to the background of calls to detect fraud when it matters, so agents can focus on serving customers with empathy.

HealthEquity saw AI attacks coming and acted fast

HealthEquity, one of the nation's largest administrators of health savings accounts (HSAs), knew that traditional security measures were no longer modern enough to protect its voice channel.

Ajit Gaddam, SVP and Head of Fraud, Financial Crimes, and Trust Systems at HealthEquity, recognized early that today's biggest security gap is how trust is established.

TIP!

Many companies, just like HealthEquity, are contending with this reality: **if trust is easy to manipulate, and a company holds valuable data, fraudsters will try whatever it takes to get in.**

"For thousands of years, trust was based on perception, recognizing someone's voice or seeing someone face-to-face. We're now in an age where **trust can be synthesized.** AI has changed what we think of as proof."

Head of Fraud, Financial Crimes, and Trust Systems, *HealthEquity*
Ajit Gaddam

Top priority: Security can't come at the expense of CX

Healthcare contact centers are often the front line for members during stressful situations, medical events, urgent account access needs, or financial uncertainty. Agents are trained to treat callers with the utmost empathy and resolve their issues as quickly as possible.

> "They're not there to interrogate. They're there to help."
>
> **Head of Fraud, Financial Crimes, and Trust Systems, *HealthEquity***
> Ajit Gaddam

But as synthetic voice and automated attacks become the norm, a tension has emerged: how do agents provide fast, compassionate service while still establishing that the caller is legitimate?

Historically, agents relied on knowledge-based questions, like "What street did you grow up on?" to authenticate callers. Now, with stolen data from data breaches, fraudsters can answer these questions and gain access with ease.

> Knowledge-based questions are no longer sufficient. If you rely solely on stage-gate verification, you're not adapting to how attacks have evolved.
>
> **Head of Fraud, Financial Crimes, and Trust Systems, *HealthEquity***
> Ajit Gaddam

Facing these challenges, HealthEquity needed a way to strengthen authentication while maintaining excellent CX.

The future of authentication starts with continuous risk assessments

HealthEquity partnered with Pindrop to layer risk analysis in its contact center ecosystem.

Within the first month of Pindrop® Passport deployment, profile match rate in the IVR increased from 31% to 71% allowing HealthEquity to authenticate more callers in the IVR and enable better self-service for their members.

Once callers are routed to agents, the Pindrop® Platform operates passively in the background, analyzing signals such as spoofing indicators, device anomalies, and voice patterns to generate real-time risk scores. This led to an authentication rate of over 91%. That means more HealthEquity callers were verified quickly, giving agents confidence to focus on great customer service.

> We're not relying on perception alone anymore. We're giving our agents high-quality signals so they can make better decisions in the moment.
>
> **Head of Fraud, Financial Crimes, and Trust Systems, *HealthEquity***
> Ajit Gaddam

Agents receive clear, actionable notifications that help them quickly assess risk—without wasting time on KBAs that aren't sufficient in the first place. When risk indicators are elevated, calls are routed properly. When signals suggest low risk with high confidence, members move forward without additional interrogation.

TIP!

This is a shift from one-time "stage gate" authentication to continuous trust verification.

HealthEquity: Keeping security strong and ready for AI attacks

HealthEquity has already seen business results.

> From last year to now, we've reduced fraud over the voice channel by over 90%. We're continuously tuning and measuring, but the reduction has been significant.
>
> **Head of Fraud, Financial Crimes, and Trust Systems, *HealthEquity***
> Ajit Gaddam

Beyond fraud reduction, HealthEquity tracks customer satisfaction. They need to know that risk detection isn't coming at the expense of member experience.

The organization reports:

- Lower targeted voice fraud attempts
- More efficient calls for legitimate members

In the AI era, healthcare organizations can't afford guesswork

"Healthcare organizations should be preparing for the next phase of AI fraud. If you're interacting with customers over voice, you need to understand that exposure and quantify it." Head of Fraud, Financial Crimes, and Trust Systems, HealthEquity, Ajit Gaddam

Gaddam emphasizes that attackers are increasingly using AI to test and optimize impersonation strategies at machine speed. Defensive strategies must evolve accordingly.

"Security and experience aren't opposites. Great companies know how to deliver both."

Brand reputation, direct financial losses, and fines—that's what's at risk. When attackers spend every day looking for your security vulnerabilities, you can't hesitate to evolve your security measures.

The beginning of a healthcare cybersecurity shift

Vijay Balasubramaniyan, CEO of Pindrop, sees the HealthEquity relationship as part of a broader transformation across healthcare.

> Voice is becoming one of the most important identity surfaces in the enterprise. HealthEquity's approach demonstrates that organizations can strengthen fraud defenses with measurable impact while still prioritizing member experience. That balance is critical in today's AI-driven threat landscape.
>
> **CEO, Pindrop**
> Vijay Balasubramaniyan

For HealthEquity, the initiative shows their investment in modernization, reinforcing trust, strengthening resilience, and empowering agents with the data they need to make fast, informed decisions.

As AI continues to reshape both customer engagement and fraud risk, HealthEquity's experience underscores a central reality: identity must now be continuously verified. But that doesn't have to come at the cost of customer service.