HealthEquity

Security & Fraud Advancements

Following the series of security and fraud incidents in 2024, HealthEquity took decisive action. We identified gaps, invested in enterprise-level security and fraud enhancements, and strengthened our infrastructure with long-term resilience in mind. Key initiatives include the implementation of voice fraud detection, required passkey authentication, advanced identity verification, and bank account verification, along with other protections. We are delivering a more secure, stable experience for our partners and members with HealthEquity taking the lead as one of the most secure HSA providers in the market.

Fraud is an industry-wide challenge.

Cybersecurity threats affect everyone, every day. Our initiative is not only about responding to past incidents; it represents a critical step toward reducing systemic risk and reinforcing shared security across our ecosystem. 3 seconds of voice recording is all it takes for Artificial Intelligence (AI) to duplicate a voice and call in to change passwords or access accounts.[1]

- 45% of passwords are hackable on the dark web within 1 minute.
- 59% are hackable within an hour.[2]
- The FTC reported $12.5 billion in customer financial losses related to fraud in 2024, a 24% increase year-over-year.[3]

It starts with leadership.

We manage cybersecurity, physical security, identity management, fraud, and cyber risk under one Chief Security Officer (CSO), Sunil Seshadri, to deliver defense-in-depth of our products and services. With his leadership, we have charted the course to fortify every experience, expanded our security and fraud teams, and delivered on a robust roadmap for 2025. Sunil is a trusted and proven cybersecurity leader with experience at several of the world's largest financial and technology companies, including VISA and the New York Stock Exchange.

Enterprise security and fraud prevention are our top priorities.

We instituted bank-level security standards without the bank burden. HealthEquity has implemented fraud and cybersecurity protections that mirror the sophistication of leading financial institutions – like passkey authentication, behavioral risk analysis, and real-time credential monitoring – without introducing unnecessary complexity for clients or members.

We doubled down on resources to fortify our systems, introducing a series of targeted enhancements designed to eliminate vulnerabilities and safeguard financial transactions.

Security enhancements implemented in 2025

We deployed key capabilities to detect and prevent fraud over the voice channel (e.g. call center, IVR) with the new application Pindrop. We now can use voice and behavioral analysis during a phone call to assess risk based on context.

Our **Fraud Operations** team has doubled down on fraud detection, investigation, and training, with expanded teams to ensure advance detection and rapid response. With intelligence from Pindrop embedded in the screens of our

member services enterprise, we've educated our agents in fraud detection and put up a barrier to call center fraud by providing real-time risk scoring and deflecting high risk calls.

With Pindrop we've blocked more than 200 phone numbers and 26,000 calls.

Preventing EFT/fraud with bank account verification & identity verification with Plaid

We've implemented industry best-in-class fraud capabilities, which provide real-time bank account verification and fraud monitoring. By validating activity against trusted data sources before funds move, we closed a critical gap in our EFT security.

Who else uses these bank account and identity verification methods?[4] Bank of America; Wells Fargo; American Express; Airbnb; Robinhood; Credit Karma, and more.

Passkey authentication is now required for member accounts.

Passkeys replace traditional passwords and one-time passcodes (OTP) with cryptographic credentials (secure, encrypted keys stored on your device that verify your identity without ever being shared) that are resistant to phishing and credential theft. They work with familiar tools like Face ID, fingerprints, or PINs – delivering a faster, safer login experience. Transmit Security is our technology partner in delivery of phishing-resistant authentication, risk-based security, and a seamless user experience across our portal and mobile platforms.

Implementation started in September 2025 on our HealthEquity Mobile app and web experience and will extend to EZ Receipts in Q1 of 2026.

Also in 2026, we will expand passkey authentication to our voice channel, extend required passkey authentication to all non-member audiences, and address SSO/Passkey integration.

Passkeys are supported on nearly all devices following industry standards, and we join the ranks of leading retail, banking, healthcare, and technology companies like Adobe, Apple, Amazon, Bank of America, Best Buy, Caremark, Citi, CVS, eBay, Google, Home Depot, Instacart, LinkedIn, Microsoft, PlayStation, Shopify, Walmart, Wells Fargo, Uber, and more.

None of our HSA competitors currently offer passkey authentication or behavioral analysis features, giving HealthEquity a clear market leadership position in protecting accounts and building member trust.

Risk-based authentication with Prove

We have woven RBA into our processes, up to and including government ID and selfie photo requirements at the highest level.

Preventing Card Fraud

We know fraudsters never stop using compromised card numbers obtained thru breaches, stealing cards in transit, and attempting e-commerce fraud.

We've added team members and built more in-depth rules to prevent high risk fraudulent card transactions. Rules are constantly monitored and identify fraudulent behavior patterns – location, test transactions and enumeration attempts, among others – to prevent large scale card fraud before it happens.

HealthEquity

With transaction-level card verification in card-not-present scenarios, we evaluate the legitimacy of the charge based on location, item type, and purchasing behavior. Non-eligible purchases or geographically unusual transactions are automatically denied, even if reattempted, ensuring funds are used appropriately.

Mobile app defense with Appdome® Mobile Security

With mobile-based fraud and malware becoming more prevalent, we've implemented stronger mobile app security defenses with Appdome on the HealthEquity and EZ Receipts mobile apps, like other leading financial institutions.

Anti-malware, anti-bot, and fraud prevention protections safeguard user sessions from malicious activity. Account takeover protection blocks unauthorized access by detecting and preventing fraudulent login attempts. Seamless protection runs in the background, ensuring security without adding friction to the member experience.

Password strengthening for all users

We've increased our complexity requirements to 15 characters and 4 types required across all experiences for all audiences.

Significant investments in GenAI, AI, and modern engineering

We continue to invest in state-of-art capabilities and people to leverage AI and engineering to detect, respond, and prevent both cyber and fraud related threats while minimizing customer friction at the same time.

Impact

A once-potential vulnerability became the catalyst for transformation. By addressing weak points directly and acting decisively, we reshaped our security posture into a strategic advantage. Today, our security protocols aren't just effective – they're setting a new industry standard.

Zero EFT fraud losses

Since implementing our security enhancements, HealthEquity recorded **$0 in fraudulent EFT losses** in April and May 2025 – clear, measurable success.

Competitive advantage in fraud protection

Our security infrastructure now exceeds that of key competitors. For example, Fidelity does not yet offer passkey authentication or behavioral fraud detection. HealthEquity leads in both innovation and trust.

What this means

Members have greater peace of mind knowing their accounts and savings are protected at every step.

Clients benefit from reduced fraud risk and a more secure, trustworthy experience for their employees.

Partners/Brokers achieve stronger alignment with leading-edge security standards and reduced reputational risk.

HealthEquity has transformed what once might have been perceived as a weakness is now our superpower.

HealthEquity

Resilience and business continuity

HealthEquity's robust resilience and business continuity posture is anchored in our commitment to enterprise risk management practices, cloud infrastructure, and defense-in-depth cyber strategy.

The organization of HealthEquity risk and business continuity endeavors

We continue to emphasize the importance of obsessing about our clients and their members' needs as fundamental to prioritizing our resilience. Crisis management and business continuity are within the domain of Enterprise Risk Management at HealthEquity, fostering a global organizational view of all key risk measures and indicators. Enterprise Risk Management is independent of any one function at HealthEquity, thereby prioritizing risk, assessment, mitigation analysis, and strong governance.

With this approach, strict controls for risk are established across all HealthEquity functions, and we are able to better partner with the business on aligning risks and mitigation actions within their functions with our resilience work. It allows us to be strategically proactive in every part of our enterprise to identify, manage, mitigate, and respond to risk.

HealthEquity hired a new Business Resilience Director in Q1 to oversee business continuity and disaster recovery preparedness and lead our Crisis Management efforts.

We believe this enterprise approach supports greater transparency and cross-functional collaboration on business continuity and disaster recovery initiatives to document and test critical asset interdependencies, ensuring continuity of our operations.

Taken together, our strategic approach ensures security and resilience in our delivery of solutions for all HealthEquity stakeholders.

Cloud environment

In our pursuit of operational excellence and heightened security, we completed migration of our core platforms to the Microsoft Azure cloud. By leveraging the power and scalability of multiple Azure availability zones, we have enhanced the protection and resiliency of our systems and data. Further, we have bolstered our defenses against evolving cyber threats with deployment of immutable backup data restoration services.

The Azure cloud infrastructure offers robust built-in security features that ensure the confidentiality, integrity, and availability of our critical assets in geo-redundant clouds. And with geo-redundancy, scheduled failover in alternating regions will become a regular practice to support disaster recovery preparedness.

Telephony

Aligned with our cloud strategy, we are migrating all telephony applications that support service call centers to the CISCO cloud environment before end of 2025. Here too, the embedded redundancy, security, and recovery measures enhance operational excellence and uninterrupted delivery of a critical service for our members and clients.

HealthEquity

Observability

To protect our systems, we want to see performance changes in real time and more quickly be alerted to abnormalities. HealthEquity is in phase 2 of implementing Dynatrace as our observability platform; deployment began in early 2024. We will advance to Phase 3 elevating our service level indicators and objectives across our enterprise.

Dynatrace is a best-in-class strategic observation platform that gathers telemetry across all HealthEquity systems. With hyper modal AI, it gathers thousands of metrics, providing baseline measures of operation, identifying deviations, and sending alerts to our teams. We are deploying Dynatrace across all systems, including non-production environments to support end-to-end resiliency of our solutions.

We anticipate full hardening of the telemetry system by year end, significantly enhancing our business continuity insights and disaster recovery capabilities.

People, process, data center stabilization

In December 2024, HealthEquity experienced an unplanned data center outage that led to services being temporarily degraded or unavailable. The incident resulted from an internal maintenance issue and was not due to malicious activity. All HealthEquity systems were fully restored. We have migrated impacted services to Azure environments and will complete shutdown of this data center within the next year.

Foundational to our resilience process improvements is updating our business impact analyses for critical processes and increasing engagement of essential personnel to support continuity and disaster recovery.

We are strengthening our focus on identification and validation of recovery time objectives for all critical HealthEquity applications and essential partners.

With this relentless focus on internal collaboration across product lines, IT, Member Services, information security, disaster recovery, and business continuity, we are enhancing our culture of preparedness.

[1] Source: 2024 Verizon Data Breach Investigations Report

[2] Secureframe password statistics

[3] 2024 Verizon Data Breach Investigations Report

[4] DataCaptive: Top 10 Companies That Use Plaid in the USA