HealthEquity®

VISA

Raising the bar in fraud prevention while advancing trust, security and innovation in healthcare payments

Healthcare cost of fraud is estimated at 3% - 15% of total $5.6T spend – upwards of $100 billion.[1,2]

Introduction

Digital transformation has reshaped how healthcare dollars move. From virtual care and online pharmacies to mobile wallets and contactless payments, account holders now expect fast, seamless experiences, especially in urgent moments.[3] But the same channels that deliver convenience have also accelerated the evolution of fraud. Systemic healthcare fraud is on the rise; as evidenced by the 2025 National Health Care Takedown resulting in charges against 324 defendants for over $14.6 billion of systemic fraud.[4] Healthcare fraud and credit card fraud often intersect through identity theft, with stolen medical records being highly prized on the black market – often worth 10 times more ($260–$310 per record) than standard credit card data ($30–$50).[5] In 2024, credit card fraud accounted for 43.9% of all identity theft reports.[6] Attackers rely on enumeration, bot-driven credential testing, AI enabled attacks, and sophisticated card-not-present tactics that exploit gaps in traditional controls.[7]

Organizations across the healthcare ecosystem face a difficult balance: protect rapidly emerging threats without introducing friction that can disrupt the payment experience. For HealthEquity, safeguarding account holders' healthcare dollars is not an option, it is foundational to achieving its mission.

HealthEquity is uniquely positioned within this landscape. As one of America's leading health benefits administrators,[8] HealthEquity supports 17 million account holders across Health Savings Accounts (HSA), Flexible Spending Accounts (FSA), Health Reimbursement Arrangements (HRA), commuter benefits, and COBRA programs. These programs represent tens of billions of dollars in annual healthcare transactions.[9] Protecting them requires both scale and precision. To strengthen this foundation, HealthEquity partnered with **Visa**, whose global payment network processes hundreds of billions of transactions annually and helps drive some of the

world's most advanced AI fraud-detection models. Visa's broad, diverse behavioral signals shaped by global patterns across merchants, give visibility into subtle, emerging fraud patterns often invisible to standalone solutions.

Together HealthEquity and Visa built a layered intelligence-driven defense capable of detecting attacks earlier, reducing false positives, and delivering smooth experiences for legitimate users. The result is a top tier fraud prevention program that delivers earlier attack detection, reduced false positives, and helps to ensure a smooth customer experience with higher card authorization rates.[10] This whitepaper outlines the approach, operating model, and outcomes, further demonstrating how this partnership is raising the standard for trust, security, and performance in healthcare payments.

The challenge: A complex and accelerating fraud & threat landscape

Healthcare dollars now move with the speed of digital commerce and fraudsters are keeping pace. Account holders now rely on online pharmacies, virtual care platforms, digital marketplaces for healthcare products, and e-commerce + contactless payments, which has created both greater convenience and greater exposure. Fraudsters target these same channels because they allow them to operate at high velocity and with scale. Enumeration, credential testing, and automated bot-driven attacks have become defining patterns in the healthcare payments risk landscape, particularly in card-not-present transactions where visibility is limited.[7]

Healthcare payments can present unique challenges for fraud detection. Many legitimate transactions share characteristics – merchant categories, price points, recurring patterns – that can resemble fraudulent behavior. This overlap makes distinguishing genuine activity from automated attacks significantly more complex. At the same time, the shift to digital health has increased transaction velocity, broadened the attack surface, and intensified the need for sophisticated, context-aware analytics.[7]

Account holders rely on uninterrupted access to their healthcare dollars, often during urgent or emotionally sensitive moments. Excessive friction undermines trust and can compromise benefits utilization. "HealthEquity made a deliberate choice: stronger protection cannot come at the expense of account holder experience."

said Sunil Seshadri, EVP and CSO. To meet this challenge, HealthEquity needed a defense model that was not only intelligent and adaptive, but also precise enough to preserve the smooth and streamlined experience that account holders expect.

The solution: Layered intelligence, real-time defense across the fraud lifecycle

To achieve this balance, HealthEquity implemented a bundled defense strategy that integrates Visa's advanced AI-powered models —Visa Advanced Authorization (VAA) and Visa Account Attack Intelligence (VAAI) — directly into its fraud operations and enabled HealthEquity to detect, score, and mitigate risk in real time across both card-not-present (CNP) and card-present (CP) channels. This approach leverages Visa's enormous global network that processes 320B+ transactions annually, across 4B+ credentials issued and 150M+ merchant locations in more than 220 countries and territories[11] — providing a robust data foundation for fraud detection.

For over three decades, Visa has been building and refining AI fraud models, pioneering innovations that now help drive some of the industry's most advanced risk-scoring technologies.

- **Visa Advanced Authorization (VAA)** – HealthEquity deployed Visa's flagship AI model and easy to use risk score to make smart, fast and informed authorization decisions. Refined over three decades and powered by VisaNet — which processes billions of transactions globally each year — VAA uses advanced artificial intelligence and machine learning with predictive analytics to analyze over 500 risk attributes on transactions in milliseconds. **VAA helped to enable a significant reduction in card fraud and gains in transaction authorization, protecting accounts and improving the card experience.**
- **Visa Account Attack Intelligence (VAAI)** – Built to detect enumeration risk in Card Not Present activity, VAAI enabled HealthEquity to identify account -testing early and help stop downstream fraud. By using machine learning to surface subtle velocity and behavioral patterns, the model revealed bot-driven testing patterns that would have blended into normal healthcare transactions. **This early visibility allowed HealthEquity to intervene sooner, reduce exposure, and prevent fraud before authorization stage controls were triggered.**

- **Visa Risk Manager (VRM)** – VRM gave HealthEquity the flexibility to tailor controls to healthcare specific transaction patterns. **By tuning policies** for digital wallet behavior, tokenization, and merchant/acquirer identifiers – including scenarios where testing was masked as legitimate spend – **HealthEquity deployed precise, low friction controls that targeted fraud without disrupting legitimate member activity.**

Together, these components – VAA, VAAI, and VRM – form a **comprehensive, multi-layered intelligence** stack. VAAI surfaces early attack indicators, VAA evaluates risk at authorization layer with contextual intelligence, and VRM tailors the final decisioning layer. For HealthEquity, Visa's multi-model stack created a more resilient fraud lifecycle. Detection timelines shortened, signal clarity improved, and model-driven controls began intercepting high-risk behaviors earlier – without introducing friction to the experience of legitimate users. The result is a modern fraud prevention framework grounded in Visa's global visibility and optimized through HealthEquity's fraud management and domain expertise.

How HealthEquity put it to work: Operationalizing intelligence and delivering best-in-class results

HealthEquity operationalized Visa's intelligence into action through a disciplined operational model designed to intervene precisely where risk was highest. Using Visa Risk Manager (VRM), fraud teams configured targeted rules tuned to healthcare specific patterns balancing protection with account holder experience. These controls incorporated parameters across merchant IDs, acquirer IDs, and card-acceptor patterns enabling HealthEquity to identify fraudulent test transactions including those masked within digital wallet flows such as Apple Pay® and Google Pay™ that would otherwise blend into typical activity. By aligning VRM policies with healthcare-specific behavior, HealthEquity strengthened card-present and eCommerce decisions while sharpening detection accuracy with minimal false positives.

Complementary scoring from Visa Advanced Authorization (VAA) and Visa Account Attack Intelligence (VAAI) further enhanced precision, triangulated risk signals using velocity, context, and healthcare merchant profiles. **Together, these components**

shortened detection, identified precise interventions and elevated HealthEquity's fraud performance to one of the strongest footprints in the health benefits sector without impacting the account holder experience. [10]

Key outcomes[9] included:

- **Card Fraud performance improved to roughly 1.1 bps**, placing HealthEquity in the *top percentile* and best-in-class of comparable healthcare portfolios.[10]
- **~31% increase in early-stage fraud-event detection**, driven by earlier visibility into enumeration and bot-driven testing behaviors, allowing HealthEquity to intervene before attacks escalated.
- **False-positive ratios improved below 5:1**, reducing friction and unnecessary declines for legitimate healthcare transactions.
- **Meaningful fraud-loss and chargeback avoidance**, as earlier interdiction prevented downstream fraud events and reduced reimbursement and dispute volume across both digital and card-present channels.
- **Interchange revenue protection through sustained higher authorization rates** [10] ensuring account holders' urgent healthcare transactions were approved rather than mistakenly declined.
- **Improved operational efficiency**, with clean case queues and few manual reviews as more fraud was accurately identified and stopped automatically before reaching investigations.

These results demonstrate how combining Visa's global scale with HealthEquity's healthcare benefits-specific operating model delivers both strong protection and smooth account holder experience.

Customer perspective

"Safeguarding our account holders' trust – protecting their identity, their accounts, and their healthcare dollars – is foundational to HealthEquity's mission. Visa's intelligence expanded our visibility into emerging threats and enabled earlier, more precise interventions. Together, we've built one of the most advanced fraud defense programs in healthcare benefits, one that reduces losses, preserves legitimate access, and helps account holders save, spend and invest with confidence."
- Ajit Gaddam, SVP, Head of Fraud and Financial Crimes, HealthEquity

This statement reflects the opinion of the speaker and is not a guarantee of outcomes.

HealthEquity® VISA

Conclusion

Fraud in healthcare payments is evolving rapidly, but so is the opportunity to build a more secure, frictionless future for account holders. By uniting HealthEquity's deep subject matter expertise with Visa's network scale intelligence, a fraud prevention framework that delivers earlier detection, strong protection and superior account holder experience was established.

As the digital experience continues to grow, HealthEquity remains committed to advancing solutions that safeguard the healthcare dollar, ensuring account holders can trust their funds are protected.

Sources

[1] National Health Care Anti-Fraud Association

[2] KFF Health System Tracker, Health Spending Growth

[3] Medical Economics, Digital Transformation in Healthcare Payments

[4] Office of the Inspector General, National Healthcare Fraud Takedown

[5] Patient Protect, Healthcare Breach Statistics 2025

[6] Insurance Information Institute, Identity theft and cybercrime

[7] Group IB, The dark side of automation and rise of the AI agent

[8] Devenir Mid-Year 2025 Report

[9] HealthEquity Quarterly Reports 2025

[10] Visa Issuer Report, October 2025

[11] Visa Fact Sheet, September 2025

HealthEquity

VISA

Standard disclosure

Case studies, comparisons, statistics, research, and recommendations are provided "AS IS" and are intended for informational purposes only and should not be relied upon for operational, marketing, legal, technical, tax, financial or other advice. Visa neither makes any warranty or representation as to the completeness or accuracy of the information within this document, nor assumes any liability or responsibility that may result from reliance on such information. Client results are provided by the client; Visa has not independently verified such data.