Proof

The Fiduciary Intelligence Hub

Q2 2026 Market Analysis of Retirement Provider Vulnerability

Contents

Proof

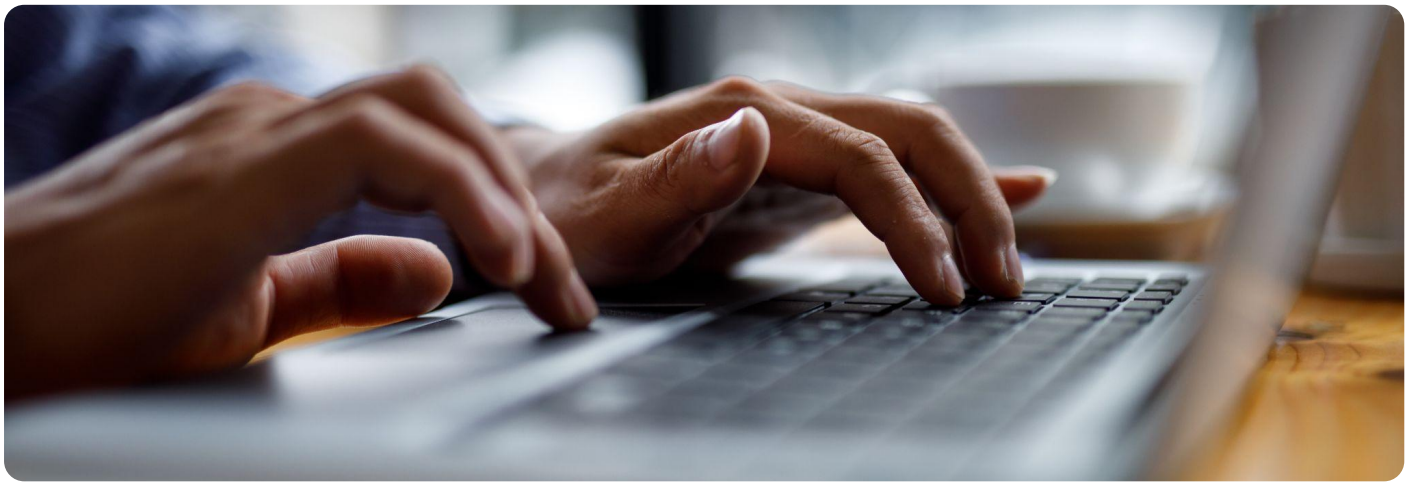
The Breaking Point

Financial crime has entered a high-velocity, industrialized era.

The retirement and pension sector faces systemic instability as attacks transition from bespoke, high-value targets to an industrialized era of financial crime. This shift is defined by the deployment of high-volume, automated botnets capable of conducting thousands of concurrent, low-value probes against institutional money-out workflows[1].

While previous cycles involved threat actors targeting high-net-worth individuals through labor-intensive social engineering, the math has changed. By Q2 2026, agentic artificial intelligence has permanently altered the cost-benefit analysis for criminals. Fraud is now executed at a scale and velocity that legacy defensive infrastructures were never designed to handle.

The Breaking Point



Criminals use micro-targeting to evade internal alert thresholds.

The most prominent evidence of this tactical shift is the micro-targeting of disbursements at specific values designed to evade internal alert floors. Fraudulent requests are increasingly clustering at the $79,700 mark.

This specific figure is a calculated response to the $80,000 manual review threshold common among Tier 1 retirement providers.

By requesting funds just below this ceiling, automated systems extract assets without triggering the enhanced due diligence or manual oversight required for larger distributions.

This "industrialized probing" leverages computational endurance (the ability of AI agents to persist indefinitely until a vulnerability is found) to bypass static rules that rely on human intervention.

The Regulatory Catalyst

Introducing The FIFC: FINRA'S Real-Time Threat Intelligence Hub

On March 31, 2026, the Financial Industry Regulatory Authority (FINRA) launched the Financial Intelligence Fusion Center (FIFC), which is a regulator-led intelligence hub providing a centralized portal for real-time threat intelligence sharing.

The launch of the FIFC is a direct response to the escalating computational endurance race between adversarial AI and legacy defense systems.

Historically, firms operated in isolation and treated fraud as an internal operational risk. The FIFC formalizes the transition to a collective defense posture, acknowledging that modern attacks rarely target a single institution in isolation.

The Regulatory Catalyst

Complementing the FIFC is FINRA Regulatory Notice 26-02, which proposes critical amendments to Rules 4512 and 2165 to protect senior and vulnerable investors from financial exploitation[2]. A

key proposal includes extending the maximum hold period for suspicious disbursements from 55 business days to 145 business days.

This extension is necessary because AI-driven frauds often require significant time to investigate, escalate, and remediate.

Furthermore, the industry is moving toward adopting the term "emergency contact" in place of "trusted contact person" to increase participant comfort with account-level protection measures.

The Business Case For Modernization

To quantify the risk and opportunity cost associated with legacy processes, this analysis examines the metrics of two industry leaders: a Top 5 U.S. Retirement Provider managing $1.5 trillion in assets and a Top 10 Global Actuarial and Retirement Firm that recently transitioned to automated high-stakes workflows[2].

For institutions of this scale, manual, paper-based workflows represent a critical security vulnerability. Before implementing modernized identity attestation, these institutions faced manual "wet signature" error (NIGO) rates of 33%[5]. Updated March 2026 data indicates that manual form processing and mailing costs have risen to $34.70 per form, driven by persistent inflation and increased labor costs.

Additionally, spousal consent requirements impact approximately 20% of withdrawal requests, which is roughly 168,000 transactions annually for a Top 5 provider, creating significant operational friction[7].

Proof Implementation Results

The implementation of Proof's multi-signal identity infrastructure has fundamentally reset these operational benchmarks. Since late January, a Top 10 global firm utilizing the platform has secured over $4.2 billion in transactions and eliminated more than 2,500 processing days[4].

By achieving a 70% digital adoption rate, these institutions have realized a projected ROI of $7.5 million in annual recurring net savings[7].

Metric	Legacy State	Proof State	Impact
NIGO Error Rate	33%	<1%	97% reduction in rework
Cost Per Form	$34.70	Optimized digital overhead	Substantial overhead reduction
Time to Detect	18 days	Real-time	Near-instant threat mitigation
Fraud Loss Rate	12.5 bps	<1 bps	>90% loss reduction

<1%

NIGO error rate

Real-time

Threat mitigation

<1bps

Fraud loss rate

The "Money Out" Identity Gap

The "Money Out" phase remains the primary point of failure for identity verification. Vulnerabilities in 401(k) rollovers and hardship withdrawals have intensified following SECURE 2.0 Act self-certification provisions. While intended to streamline access, these provisions have inadvertently caused a 6% surge in account leakage. Fraudsters exploit the reduced evidentiary requirements to initiate illegitimate withdrawals under the guise of financial hardship[1].

Simultaneously, the industry is observing a 40% increase in video injection attacks targeting participant distributions[11]. These attacks represent an escalation of deepfake technology, where an unauthorized party injects an AI-generated video stream into a live identity verification interview.

These tools can simulate micro-expressions and lip-syncing, making it difficult for human agents to distinguish between a legitimate participant and a high-resolution deepfake. This surge highlights the inadequacy of visual-only "Know Your Customer" (KYC) protocols[13].

Calibrated Strategic Metrics (2022–2026)

Metric	2022 (Actual)	2024 (Actual)	2025 (Year End)	2026 (Projected)
Incident Volume	~900/yr	4,200/yr	8,800/yr	12,600/yr
Average Disbursement	~$182k	$124k	$92k	$79.7k
Average Account Target	~$348k	$265k	$210k	$168k
Time To Detect (ATO)	18 days	9.5 days	5 days	2.5 days

Trends

Industrialized probing: High-volume automation

Micro targeting: Evading $80k alert floors

Mid-market saturation: Bulk asset targeting

Real-time convergence: Driven by the FIFC

The Technical Solution

Address the identity gap through multi-signal attestation.

The Proof platform secures the "money out" identity gap by moving beyond binary document checks. The platform employs a multi-signal attestation model evaluating risk across identity, device, network, and behavioral vectors[15].

Plus, the integration of Visa's global transaction intelligence (Q4 2025) has significantly enhanced the Proof risk model. By leveraging network-level visibility across Visa Direct and Risk Insights, the platform correlates signals invisible to a single institution[17]:

- **Device fingerprinting:** Identifying unique hardware signatures to detect if the same device is accessing multiple unrelated accounts[19].
- **Email age:** Analyzing the history of the associated email. Requests from accounts created less than 24 hours ago are automatically escalated[15].
- **Location correlation:** Comparing IP locations against historical data and piercing VPN or proxy masking[15].

Bridging the Literacy Gap with Explainable AI (XAI)

A significant challenge is the cybersecurity literacy gap, where approximately 1 in 4 business leaders lack the technical familiarity to interpret complex AI-driven fraud attempts.

Proof's Explainable AI (XAI) interface translates sophisticated risk scores into clear insights, such as "Unusual IP location following recent password reset"[15].

This transparency empowers staff to make informed decisions without deep forensic training, reducing the likelihood of human error[22].

Calculate your ROI

Talk to Proof

Proof Performance Data

630%

Outperformance over traditional industry benchmarks for fraud detection at a high risk threshold[15]

13x

Proof Defend Risk Engine efficiency compared to an industry-leading passive-signal fraud model[15]

6x

Amount of fraud Proof can identify compared to benchmarks at equivalent intervention rates[15].

<1 bps

Fraud loss reduction for institutions fully integrated into Proof's multi-signal model[24]

Proof

Sources

Sources Cited

1. FINRA Regulatory Notice 26-02:(https://www.finra.org/rules-guidance/notices/26-02).
2. Alloy's 2026 State of Fraud Report:(https://www.alloy.com/reports/fraud-report-2026).
3. EP Wealth Advisors Security Incident Report: Cyberattack Notice (February 2, 2026).
4. SECURE 2.0 Act Analysis: 401(k) Asset Leakage and record-rates.
5. Visa Q4 2025 Strategic Partnership:(https://thepaypers.com/fraud-and-fincrime/news/proof-joins-forces-with-visa-for-secure-digital-payments).
6. Hiya State of the Call 2026 Report:(https://www.morningstar.com/news/business-wire/20260301082723/state-of-the-call-2026-ai-deepfake-voice-calls-hit-1-in-4-americans-as-consumers-say-scammers-beating-mobile-network-operators-2-to-1).
7. Bureau of Labor Statistics: Employer Costs for Employee Compensation (March 2026).
8. FINRA Financial Intelligence Fusion Center (FIFC):(https://www.finra.org/media-center/newsreleases/2026/finra-launches-financial-intelligence-fusion-center-combat).
9. Proof Performance Data:(https://www.proof.com/blog/multi-signal-fraud-detection-benchmarks).

Works Cited

1. Financial Fraud on the Rise: 2025 Data Reveals Growing Threats to Consumers and Businesses - Meredith Village Savings Bank, accessed April 6, 2026, https://www.mvsb.com/2025/12/05/financial-fraud-on-the-rise-2025-data-reveals-growing-threats-to-consumers-and-businesses/

Works cited

2. Regulatory Notice 26-02 | FINRA.org, accessed April 6, 2026, https://www.finra.org/rules-guidance/notices/26-02
3. EP Wealth Advisors Data Breach Investigation - Strauss Borrelli PLLC, accessed April 6, 2026, https://straussborrelli.com/2026/03/09/ep-wealth-advisors-data-breach-investigation/
4. presentation PDF - OREGON PUBLIC EMPLOYEES RETIREMENT SYSTEM BOARD MEETING AGENDA, accessed April 6, 2026, https://www.oregon.gov/pers/Documents/Board-Meetings/2025/12-05-2025-PERS-Board-Meeting-Packet.pdf
5. KP&F - KPERS, accessed April 6, 2026, https://www.kspers.gov/pdf/kpfemployersmanual.pdf
6. RETIREMENT HANDBOOK - Contra Costa Water District, accessed April 6, 2026, https://www.ccwater.com/DocumentCenter/View/5020/Retirement-Handbook?bidId=
7. Q4 2025 Earnings Call Transcript, accessed April 6, 2026, https://s206.q4cdn.com/265218871/files/doc_earnings/2025/q4/transcript/Q425-Earnings-Transcript.pdf
8. Visa Direct Blog | Tap, Send, Done: How Payments Became Real-Time, accessed April 6, 2026, https://corporate.visa.com/en/products/visa-direct/blog/tap-send-done-how-payments-became-real-time.html
9. FINRA Launches Financial Intelligence Fusion Center to Combat ..., accessed April 6, 2026, https://www.finra.org/media-center/newsreleases/2026/finra-launches-financial-intelligence-fusion-center-combat
10. Financial fraud: Emerging threats and the future of prevention - Convera, accessed April 6, 2026, https://convera.com/blog/compliance/financial-fraud-emerging-threats-and-the-future-of-prevention/
11. Profiles of the REGTECH100, the world's most innovative RegTech companies that every leader in the regulatory industry needs t - FinTech Global, accessed April 6, 2026, https://fintech.global/regtech100/wp-content/uploads/2025/12/RegTech100-Report-2026-2.pdf
12. The Implications of Sharing Personal Data - Experian Insights, accessed April 6, 2026, https://www.experian.com/blogs/insights/implications-sharing-personal-data/

Works cited

13. Fraud in BPO Hiring: Rising Stakes for 2025 - Journeyfront, accessed April 6, 2026, https://www.journeyfront.com/blog/fraud-is-infiltrating-bpo-hiring-and-the-stakes-have-never-been-higher
14. Pew Reveals What Americans Know About Cybersecurity - Experian Insights, accessed April 6, 2026, https://www.experian.com/blogs/insights/pew-reveals-what-americans-know-about-cybersecurity/
15. How Proof's Layered Intelligence Model Outperforms Passive Fraud Detection 600 - 1,300% With Minimal Friction, accessed April 6, 2026, https://www.proof.com/blog/multi-signal-fraud-detection-benchmarks
16. Financial Intelligence Fusion Center (FIFC) - FINRA, accessed April 6, 2026, https://www.finra.org/filing-reporting/fifc
17. March 9, 2026 Mr. James Wrona Vice President & Associate General Counsel Office of General Counsel Financial Industry Regulatory Authority, accessed April 6, 2026, https://www.finra.org/sites/default/files/NoticeComment/PIABA%20Comment%20FINRA%2026-02.pdf
18. FINRA Forward In Action | FINRA.org, accessed April 6, 2026, https://www.finra.org/about/finra-forward/see-more
19. GNNs: Modernizing fraud prevention in financial services - Thoughtworks, accessed April 6, 2026, https://www.thoughtworks.com/en-us/insights/articles/graph-neural-networks-in-fraud-prevention
20. Online Gambling Fraud: What is It & How to Prevent It - SEON, accessed April 6, 2026, https://seon.io/resources/online-gambling-fraud/
21. Merchant acquiring for international e commerce how to reduce the risk of termination, accessed April 6, 2026, https://coredo.eu/merchant-acquiring-for-international-e-commerce-how-to-reduce-the-risk-of-termination/
22. How to Spot a Fake Job Applicant Before It's Too Late - Sardine, accessed April 6, 2026, https://www.sardine.ai/blog/fake-job-applicant
23. 2026 Group Remuneration Policy and Report - UniCredit, accessed April 6, 2026, https://www.unicreditgroup.eu/content/dam/unicreditgroup-eu/documents/en/governance/compensation/group-compensation-policy/2026/2026_Group_Remuneration_Policy_and_Report.pdf
24. Protecting digital payments from timely threats | Visa, accessed April 6, 2026, https://corporate.visa.com/en/sites/visa-perspectives/security-trust/security-at-network-scale.html

Proof SM

About Us

Proof provides the high-assurance digital identity infrastructure for the internet's most important transactions. As a digital identity issuer, Proof verifies who is behind a critical action and ensures every interaction is continuously secured through our Identity Authorization Network. Our platform empowers organizations to authorize high-stakes actions and preserve verifiable records that are both defensible and authentic. To date, Proof has secured over $640B in transactions across critical workflows including account recovery, financial approvals, and the Notarize Network, the world's largest on-demand notary platform. Learn more at proof.com.