Comment Letter on FINRA Regulatory Notice 26-02

Investor Protection Enhancements for Senior and Vulnerable Investors

Submitted by: Chad Hicks & Philip Loeffel

Introduction and Acknowledgment of Collaborative Engagement

We appreciate the opportunity to comment on FINRA Regulatory Notice 26-02 issued by the Financial Industry Regulatory Authority (FINRA). This notice reflects repeated, substantive, and meaningful collaboration between FINRA and industry participants, including direct engagement with our organization.

Through ongoing dialogue, data-driven discussions, and practical feedback grounded in real-world fraud and exploitation scenarios, FINRA demonstrated a clear commitment to incorporating firm-level experience into its regulatory approach. Regulatory Notice 26-02 represents a thoughtful and responsive outcome of that process and a meaningful advancement in modernizing investor protection frameworks.

Importantly, the direction of this proposal and similar signals across the regulatory landscape, reflects a shared understanding between regulators and industry participants that **enhancing protective and supervisory controls to mitigate illicit activity will, at times, introduce friction into the customer experience. While this may reduce transactional speed or convenience in certain instances, the overarching objective is to protect customers from increasingly sophisticated fraud schemes and financial exploitation**. We believe this mutual recognition of the protection-versus-friction dynamic is both necessary and appropriate in the current threat environment.

I. Terminology Update – Rule 4512

We strongly support FINRA's proposal to permit the use of the term "emergency contact" as an alternative to "trusted contact" under Rule 4512.

During prior engagement with FINRA, our Senior and Vulnerable Investor (SVI) Designated Principal raised this issue based on consistent customer confusion observed across the industry. Specifically:

- Customers frequently misinterpret the term “trusted contact” to mean the individual has authority to access or transact in their accounts, which is not the case.
- This misunderstanding has caused hesitation among customers particularly seniors resulting in lower designation rates and reduced effectiveness of the rule.
- The term “emergency contact” aligns with widely understood consumer terminology and clearly communicates the limited, communication-only purpose of the role.

This proposal reflects FINRA’s responsiveness to operational realities and customer behavior patterns. While updating terminology may appear modest, clarity in communication is foundational to effective supervisory frameworks.

More broadly, this change exemplifies the evolving regulatory posture: firms are being asked to strengthen protective controls while simultaneously maintaining customer trust and comprehension. Clear terminology reduces unnecessary friction and confusion, helping balance enhanced supervisory safeguards with an accessible customer experience.

We believe this amendment will materially improve customer understanding, increase participation rates, and enhance the protective intent of Rule 4512 without imposing additional operational burden.

II. Reporting to Federal Agencies – Request for Clarification

We support FINRA’s proposal to expand reporting options to include federal agencies when firms reasonably suspect financial exploitation or fraud. However, we respectfully request additional clarity to promote consistent implementation across member firms.

During collaborative discussions, our SVI Designated Principal noted:

- The term “federal agencies” is currently undefined and subject to broad interpretation.
- In practice, firms understand the proposal to primarily reference the Federal Bureau of Investigation Internet Crime Complaint Center (IC3) and the Financial Crimes Enforcement Network (FinCEN).
- The absence of specificity may create uncertainty, inconsistent reporting practices, and potential examination risk due to differing interpretations.

Recommendation

FINRA should provide either:

- A non-exhaustive list of recognized federal agencies appropriate for reporting; or
- Clear criteria defining what constitutes an acceptable federal reporting destination.

Clarification will promote uniform supervisory practices and improve regulatory outcomes.

As regulatory expectations increasingly encourage proactive reporting and law enforcement coordination, firms recognize that additional reporting obligations may require expanded internal controls and documentation. This evolution may slow certain processes or introduce additional procedural steps. However, the industry broadly understands and increasingly shares with regulators that these measures are necessary tradeoffs to better detect and prevent illicit conduct before losses become irreversible.

III. Temporary Hold Extensions – Rule 2165

We generally support FINRA's proposal to allow extended temporary holds when there is a reasonable belief of financial exploitation. This flexibility reflects the complex and evolving nature of modern fraud investigations.

Member firms would benefit from additional guidance regarding:

- Documentation expectations for each hold extension;
- Customer notification frequency and content;
- How firms should demonstrate continued reasonable belief over extended timeframes.

Clear supervisory guardrails will allow firms to balance investor protection with customer autonomy and ensure predictable examination outcomes.

We recognize that extended holds may create customer dissatisfaction or perceived inconvenience. However, regulatory signals across the financial services ecosystem increasingly reflect a shared understanding: preventing financial exploitation may require slowing transactions when credible red flags arise. The temporary introduction of friction is preferable to the permanent loss of customer assets.

IV. Proposed Rule 2166 – Temporary Delays for Suspected Fraud

A. Strong Support for Proposed Rule 2166

We view proposed Rule 2166 as a valuable and timely tool for preventing fraud, particularly given the rise of real-time payment scams affecting investors of all ages.

The Federal Bureau of Investigation's 2024 Internet Crime Report documented losses exceeding $16.6 billion to fraud, with individuals over age 60 accounting for at least $4.8 billion of those losses. The Global Anti-Scam Alliance has reported that rapid real-time payment fraud has resulted in over $1 trillion in global losses.

Modern fraud schemes exploit the speed and finality of instant payment systems. Authorized push payment fraud, account takeover schemes, business email compromise, and AI-enhanced social engineering including deepfakes and voice cloning have materially altered the risk landscape.

In this context, the proposed five-business-day "speed bump" framework represents a necessary recalibration of the balance between transaction efficiency and customer protection. Regulatory and supervisory bodies globally are signaling that instantaneous movement of funds without intervention controls is incompatible with effective fraud mitigation.

The industry increasingly recognizes that enhancing pre-disbursement controls may slow certain legitimate transactions. However, this friction is aligned with the overarching goal of safeguarding customers and preserving trust in financial markets.

B. Recommendations for Effective and Consistent Implementation

1. Clarify the Standard for Reasonable Suspicion

We recommend FINRA provide actionable guidance on the standard for establishing a "reasonable belief of fraud" sufficient to invoke a delay.

Drawing from international regulatory frameworks, including guidance from the Financial Conduct Authority, FINRA could provide a non-exhaustive framework incorporating:

Behavioral Indicators

- Signs of distress, confusion, or third-party coaching
- Inconsistent or implausible explanations
- Emotional urgency inconsistent with transaction history

Transactional Indicators

- Significant deviations from historical account patterns
- Multiple rapid disbursement requests
- Payment methods commonly associated with fraud typologies

Technology-Enhanced Detection

- Alerts from validated fraud monitoring systems
- Machine learning anomaly detection
- Device or location anomalies

Providing such guardrails reinforces the shared understanding that protective intervention is appropriate when risk indicators converge even if that intervention temporarily alters the customer experience.

---

2. Affirm Good-Faith Use and Safe Harbor Protections

Firms need assurance that reasonable, good-faith use of Rule 2166 will not create enforcement exposure.

We recommend FINRA explicitly affirm that:

- Good-faith invocation of delay authority even if fraud is ultimately not confirmed will not result in enforcement action.
- Reasonable judgment exercised by trained personnel will be respected.
- The absence of confirmed fraud does not retroactively invalidate a documented, reasonable belief.

Without such clarity, firms may hesitate to apply protective controls due to fear of second-guessing. Regulatory alignment around good-faith intervention is essential to encourage appropriate use of delay authority.

As regulators continue signaling that proactive fraud interdiction is expected, firms must be empowered to introduce friction when necessary without punitive hindsight analysis.

---

3. Harmonization With Existing Obligations

FINRA should clarify interactions with:

- Regulation T and customer account agreement timing provisions;
- Customer notification best practices;
- Suspicious Activity Report (SAR) considerations involving FinCEN;
- Expanded federal reporting mechanisms referenced in the Notice.

Clear harmonization guidance will ensure that enhanced supervisory controls are implemented consistently and transparently.

V. Training, Technology, and Industry Coordination

Training

FINRA should provide guidance on minimum training elements, including:

- Recognition of evolving fraud typologies;
- Customer vulnerability indicators;
- Documentation best practices;
- Communication techniques that balance protective intent with customer autonomy.

Technology Integration

Modern fraud detection increasingly relies on real-time analytics and machine learning. FINRA should clarify that:

- Technology generated alerts may support reasonable belief determinations when appropriately validated;
- Firms are not required to adopt specific technologies but should implement controls appropriate to their risk profile;
- Human review remains essential.

Cross-Industry Data Sharing

Fraud prevention requires coordination. While infrastructure initiatives may fall outside FINRA's direct authority, FINRA can encourage responsible intelligence sharing consistent with privacy and competitive considerations.

Conclusion

Regulatory Notice 26-02 reflects FINRA's responsiveness to industry experience and its commitment to collaborative rulemaking. We commend FINRA's engagement with our SVI Designated Principal, brokerage compliance, and platform governance teams throughout this process.

Across the proposals we discussed terminology updates, expanded reporting, extended holds, and temporary payment delays a consistent regulatory signal is evident: enhanced protective and supervisory controls are necessary to combat increasingly sophisticated illicit activity. The industry broadly recognizes that strengthening these controls may introduce additional review steps, documentation requirements, and transaction delays that affect customer convenience. However, this measured friction serves the broader objective of protecting customers, preserving assets, and maintaining trust in financial markets.

With the clarifications outlined above, we believe the proposed amendments will significantly enhance investor protection, promote consistent implementation across firms, and strengthen the industry's ability to combat financial exploitation and fraud.

We appreciate FINRA's consideration of these comments and remain available to provide additional input as the rulemaking process continues.

Submitted by:
Chad Hicks, Certified Fraud Examiner (CRD Number on File)

Philip Loeffel, Certified Chief Information Security Officer (Certification Number on File)

About the Authors:

Chad Hicks is a Certified Fraud Examiner (CFE) and Regulatory, Fraud, Legal & Product Consulting Specialist at Robinhood, where he serves as a frontline leader in the firm's engagement with the Securities and Exchange Commission (SEC) and FINRA on financial crimes investigation, investor protection, and regulatory compliance. With over a decade of progressive experience spanning fraud detection, incident response, platform governance, and risk operations, Hicks possesses an end-to-end understanding of the customer fraud lifecycle from initial detection through legal and regulatory resolution. Thus, enabling him to design and implement enterprise-wide controls that strengthen every layer of the protective framework. He co-leads Robinhood's Veterans Employee Resource Group and brings a mission-driven discipline forged as a United States Marine with global operational experience. His direct, ongoing coordination with federal regulators on reporting, senior and vulnerable investor protections, and emerging fraud typologies, including authorized push payment fraud, AI-enhanced social engineering, and account takeover schemes and provides the operational authority and regulatory credibility underpinning the recommendations in this comment letter. Hicks holds a CRD number on file with FINRA and studied at American University in Bosnia and Herzegovina.

Philip Loeffel is the Founder and CEO of Mind Mesh AI, a software technology executive with over 20 years of experience building and scaling enterprise software companies across fintech, defense, and AI sectors. He holds current certifications as a Chief Information Security Officer (CISO) and Certified Ethical Hacker (CEH), along with a FINRA Securities Industry Essentials (SIE) credential—giving him a rare intersection of software engineering depth, cybersecurity authority, and securities industry regulatory awareness. Philip's career spans founding and leading defense contractor Riptide Software through over $100M in awarded contracts, writing mission-critical code for NASA and government programs, and currently advising government agencies and financial institutions on secure AI transformation. His expertise in AI-enhanced fraud detection, software engineering, and the cybersecurity implications of autonomous AI agents directly informs the technology integration and detection framework recommendations

outlined in this comment letter. Philip holds a B.S. in Computer Engineering and an M.S. in Computer Science.