CARDOZO LAW

BENJAMIN N. CARDOZO SCHOOL OF LAW – YESHIVA UNIVERSITY

Elizabeth Goldman, *Director*
Securities Arbitration Clinic
Clinical Professor of Law

(646)592-6496
esgoldma@yu.edu

Attn: Ms. Jennifer Piorko Mitchell
Office of the Corporate Secretary
Financial Industry Regulatory Authority (FINRA)

Re: Regulatory Notice 26-02 - Comment on Proposed Rule

The Securities Arbitration Clinic at Cardozo Law School (the "Cardozo Clinic"), a pro bono legal services clinic serving lower income retail investors, respectfully submits this comment ("Comment") in response to the Financial Industry Regulatory Authority's ("FINRA") proposal in Regulatory Notice 26-02 (the "Notice") to amend Rules 4512 and 2165 and to introduce new Rule 2166. The proposed rule would permit member firms to place a temporary five-business-day delay when the firm has a reasonable belief that fraud has occurred, is occurring, or is likely to occur. Drawing on the Clinic's experience representing retail investors harmed by fraud, this Comment offers several recommendations intended to clarify the operational standards governing the proposed amendments and new rule while preserving investor autonomy.

In our clinical practice, many of our clients are elderly or very young, have limited income, and have limited familiarity with financial products and markets. Some also face language barriers or other challenges that increase their vulnerability to fraud. We regularly encounter victims whose losses represent their entire retirement savings accumulated over decades, or funds necessary to meet basic living expenses. From this vantage point, we have seen firsthand the devastating financial and emotional consequences that fraud can impose on individual investors and their families.

The Rapid Growth of Fraud Targeting Retail Investors

Investment fraud targeting retail investors has reached unprecedented levels. The FBI's Internet Crime Complaint Center reported $16.6 billion in fraud-related losses in 2024, a 33% increase from the prior year and more than four times the $3.5 billion reported in 2019.[1] Investment fraud

[1] FEDERAL BUREAU OF INVESTIGATION, INTERNET CRIME COMPLAINT CENTER (IC3) 2024 INTERNET CRIME REPORT 3 (2025), https://www.ic3.gov/Media/PDF/AnnualReport/2024_IC3Report.pdf [hereinafter IC3 2024 REPORT] (reporting $16.6 billion in total fraud-related losses in 2024); FEDERAL BUREAU OF INVESTIGATION, INTERNET CRIME COMPLAINT CENTER (IC3) 2019 INTERNET CRIME REPORT 3 (2020), https://www.ic3.gov/Media/PDF/AnnualReport/2019_IC3Report.pdf [hereinafter IC3 2019 REPORT] (reporting approximately $3.5 billion in losses in 2019). These figures reflect reported losses and likely understate the total magnitude of fraud, as many incidents go unreported.

alone has increased dramatically, rising from approximately $222 million in losses in 2019 to $6.57 billion in 2024, making it the largest category of reported fraud loss in the United States.[2]

These schemes share a common feature: they target individuals directly by persuading victims to transfer funds, disclose sensitive information, or grant access to financial accounts. While technological safeguards and corporate compliance measures have reduced certain forms of enterprise-level fraud, schemes that exploit individual investors have expanded rapidly. Fraud affecting retail investors also spans age groups. Younger adults report fraud victimization at rates comparable to or higher than older adults, although older victims tend to suffer significantly larger financial losses.[3]

Distinguishing Between Actor-Concealed Fraud and Induced Fraud

Operationally, fraud manifests in two materially distinct forms: Actor-Concealed Fraud and Induced Fraud. Actor-Concealed Fraud typically involves compromised sign-in credentials, impersonation, identity theft, and fraudulent ACATS transfer instructions. In these cases, the fraudulent actor is concealed from both the firm and the customer, and the warning signs often appear as technical or transactional anomalies. By contrast, Induced Fraud involves deception that leads customers to "authorize" transactions. Common examples include impersonation scams where someone pretends to be a legitimate representative of the member firm, friendship or romance scams, cryptocurrency transfer schemes, or urgent liquidation requests. Although the customer appears to "authorize" the transaction, that authorization is corrupted by deception.

These two forms of fraud present different detection challenges. Actor-Concealed Fraud often manifests through technical anomalies detectable through automated monitoring, whereas Induced Fraud frequently appears as customer-authorized activity influenced by deception characterized by behavioral and other contextual warning signs. Recognizing both forms within the Rule 2166 framework will help ensure that firms do not limit intervention only to traditional unauthorized account activity.

Member Firms are uniquely positioned to protect investors from Actor-Concealed Fraud because they can monitor suspicious activity through investor trading patterns, device identification and authorization, and other transactional indicators that may signal suspicious activity.

---

[2] IC3 2019 REPORT, *supra* note 1, at 20 (reporting approximately $222 million in investment fraud losses in 2019); IC3 2024 REPORT, *supra* note 1, at 10, 19 (reporting approximately $6.57 billion in investment fraud losses in 2024). Investment fraud is now the single largest category of reported fraud loss in the United States. *See New FTC Data Show a Big Jump in Reported Losses to Fraud to $12.5 Billion in 2024*, FED. TRADE COMM'N (Mar. 10, 2025) https://www.ftc.gov/news-events/news/press-releases/2025/03/new-ftc-data-show-big-jump-reported-losses-fraud-125-billion-2024.

[3] FEDERAL TRADE COMMISSION, CONSUMER SENTINEL NETWORK DATA BOOK 2024 4–5, 13 (2025) https://www.ftc.gov/system/files/ftc_gov/pdf/csn-annual-data-book-2024.pdf (reporting that individuals aged 20–29 were more likely to report fraud victimization than individuals aged 70–79 in 2024). *See also* IC3 2024 REPORT, *supra* note 1, at 8, 27–33 (reporting that adults aged sixty and older reported approximately $4.9 billion in fraud losses in 2024 and experience significantly higher median losses than younger victims).

For example, in one case, a young investor's brokerage account was compromised by a series of unauthorized transactions. Although the trades were executed from an unauthorized device, sent to unverified accounts and were inconsistent from the investor's prior history, the brokerage firm failed to intervene until he lost a significant portion of the value in his account. One of the transfers was made at 3 a.m. Had the firm placed a hold on these transactions and communicated with the client to determine whether he had authorized the erratic activity, the losses would have been wholly preventable.

Victims of Induced Fraud can similarly benefit from heightened incentives for fraud detection, client communication, and comprehensive investigations.

In another case, a 78-year-old retiree from Brooklyn was targeted in an online investment scam. A fraudster contacted her through WhatsApp in her native language, made a personal connection to her, and persuaded her to invest through what appeared to be a legitimate online trading platform. Through repeated assurances and manufactured urgency, the fraudster induced her to authorize multiple transfers. At first, she transferred funds from her savings. A few months in, she transferred money out of her brokerage account while her broker was on vacation. She transferred over $155,000 – all her retirement savings and the funds she had spent decades saving to support a daughter with disabilities. By the time her licensed broker and her other daughter discovered the fraud, the money was already gone. Had they been able to discuss the transactions and show her how to check if the investment account that she was transferring her money to was legitimate, this fraud likely would not have occurred.

Another retiree was defrauded by a customer support impersonator of a member firm's exclusively online brokerage services platform. After being locked out of his brokerage account, he searched online for the firm's customer support number. He called the phone number listed on the top of the search result, which had the broker-dealer's logo and a direct link to its parent company's stock price. When asked if the agent could take control of his device to fix the problem, the retiree responded yes. Within minutes, the fraudulent agent convinced the retiree to transfer two quick $5,000 transfers in succession to a purported "Gold Account" within the firm, claiming doing so would allow him to obtain significant benefits associated with his account. After a few minutes, the customer grew suspicious and tried to contact the member firm to stop the transfer but was unable to reach a live person. The member firm failed to contact the customer for weeks. By the time the retiree was able to reach anyone, the money was gone. Notably, this customer had never transferred funds out of his account before, and the transfers were to unverified accounts. These transfers amounted to a significant portion of this retiree's retirement savings and have caused great emotional turmoil and financial hardship. Even a short delay on this transfer, or any kind of check-in notifying him that his money was being transferred out of his account would have likely prevented this unfortunate event from happening.

These cases illustrate the devastating financial and emotional harm that fraud can cause and underscore the importance of providing member firms with tools that allow them to intervene before funds are irrevocably transferred and lost.

The proposals in the Notice represent an important step in modernizing FINRA's regulatory framework to address the rapidly evolving threat of fraud and financial exploitation affecting retail investors. The Notice recognizes that technological developments, including artificial intelligence-enabled deception and increasingly sophisticated impersonation schemes, have dramatically expanded the scale and complexity of fraud targeting investors of all ages.

The Cardozo Clinic supports FINRA's effort to provide member firms with additional tools to detect and interrupt fraudulent activity before investors suffer irreversible losses.

However, the effectiveness of the proposed framework will depend heavily on the clarity of the operational guidance provided to member firms. In our experience representing retail investors who have been harmed by fraud, the absence of clear standards frequently results in inconsistent firm responses to suspicious activity and uncertainty regarding when intervention is appropriate.

This Comment therefore offers several recommendations designed to strengthen the Notice's proposals while preserving the balance between investor protection and customer autonomy that FINRA has emphasized.

Specifically, this Comment addresses three areas of the Notice's proposal:

First, the proposed Speed Bump under Rule 2166 and the operational meaning of the "reasonable belief of fraud" standard.

Second, the proposed amendments to Rule 4512 concerning trusted contacts and the alternative terminology of "emergency contact."

Third, the proposed extension of the maximum temporary hold period under Rule 2165 from 55 business days to 145 business days.

Proposed Rule 2166 and the Temporary Delay Framework – Speed Bump

Proposed Rule 2166 would permit member firms to place a temporary delay of up to five business days on a disbursement or securities transaction when the firm has a reasonable belief that fraud has occurred, is occurring, has been attempted, or will be attempted. The Cardozo Clinic supports the introduction of this mechanism. Many modern fraud schemes, particularly Actor-Concealed transfers, impersonation, relationship manipulation, or fraudulent investment schemes, depend on creating urgency and isolating victims from outside perspectives. A short delay can disrupt these tactics by providing time for firms to communicate with customers, verify authorization, and present information about potential fraud schemes.

In all of the cases cited above, the Speed Bump would have at least mitigated and likely would have prevented the fraud from occurring in the first place.

At the same time, the proposed Speed Bump appropriately limits the scope of the intervention, balancing investor protection with customer autonomy. For the rule to function effectively across business models and firm sizes, however, additional clarification regarding the "reasonable belief of fraud" standards would improve consistency and encourage firms to use the safe harbor.

The Regulatory Context and the Need for Rule 2166

Proposed Rule 2166 extends a safe-harbor framework to all adult customers by permitting the Speed Bump where a member firm reasonably believes fraud has occurred, is occurring, has been attempted, or will be attempted. We strongly support this approach for three reasons:

1. Fraud increasingly targets younger and middle-aged investors;
2. Emotional manipulation and urgency tactics impair judgment irrespective of age;
3. Short intervention windows can disrupt fraud momentum before funds leave the system.

The Speed Bump appropriately reflects the limited investigative role available outside the Specified Adult context and preserves customer autonomy by limiting the delay period. The principal area requiring refinement is definitional clarity.

Clarifying "Reasonable Belief of Fraud"

A. The Current Definition

Proposed Rule 2166 defines "fraud" as a deceptive scheme perpetrated by a third party that results in a request for a disbursement or securities transaction based on false or misleading information.

While broad, the rule does not specify what constitutes sufficient indicia to form a "reasonable belief." Firms have limited their scope of fraudulent activity on customer accounts that are eligible for reimbursement.[4] We suggest strengthening the definition of fraud (and/or supplying examples) to provide firms with a clearer guideline as to account activity and transactions that should constitute a reasonable belief of fraud.

Absent additional guidance, firms may face operational uncertainty regarding what constitutes a reasonable belief regarding fraud. Firms may be unsure whether the firm must speak directly to the customer to establish the belief, whether algorithmic alerts are sufficient, and/or whether familiarity with a customer's historical behavior is necessary to justify intervention. Providing

[4] *See e.g.*, *How We Help Protect You*, CHASE, https://www.chase.com/digital/resources/privacy-security/security/how-we-protect-you ("You won't be held responsible for unauthorized charges made with your credit card." "We'll reimburse you for [] unauthorized transactions."); SELECTED TERMS AND CONDITIONS FOR WELLS FARGO CONSUMER DEBIT AND ATM CARDS, WELLS FARGO 6 (2025) ("With Zero Liability protection, you'll have no liability for Card transactions that you did not make or authorize."). Additionally, Wells Fargo stipulates an investigation process under their Zero Liability protection guarantee that the protection "does not apply if [they] determine, based on substantial evidence, that [the customer] [was] fraudulent or negligent in the handling of [their] Card or Account[.]" *Id.*

interpretive guidance identifying objective, non-exclusive indicators of fraudulent activity would improve consistency and reduce hesitation among firms that might otherwise refrain from acting due to perceived liability risk.

In the Cardozo Clinic's experience, firms often hesitate to intervene in cases involving Induced Fraud because they view those transactions as customer-authorized and therefore outside the scope of reimbursement obligations. Indeed, they often state so explicitly. For example, one member firm states in its Security Guarantee that it "won't offer any reimbursement to customers who have fallen victim to a scam, if a fraud investigation determines that the customer" authorized any transactions.[5] Because of these disclaimers, firms treat such transactions as matters of customer responsibility rather than fraud events requiring intervention. This Comment is directed at the need for intervention. Member firms' reluctance to intervene can allow fraudulent schemes to proceed unchecked even when warning signs are present.

We have seen a number of instances where there is an indication that Induced Fraud may be occurring, and member firms can take basic precautions that can help prevent it. Member firms could implement short, clear confirmation prompts that are modeled on safeguards used by peer-to-peer payment apps such as Zelle or Venmo. While broker-dealers operate under a different regulatory framework than payment platforms, similar confirmation prompts could provide effective consumer protection tools. Venmo asks users to confirm the recipient's identity and prompts them to verify the last four digits of the recipient's phone number to ensure the funds are transferred to the correct recipient. Zelle functions similarly by asking users to add the recipient as a contact first by entering their email address or phone number. Suggestions for pop-up messages prompted by transfers, for example, that are being made for the first time, or to unverified accounts could include: "Are you sure you would like to send this payment out of your account? Make sure you know and trust the recipient before sending. Scammers often ask for urgent transfers," and "Before completing this transfer, please confirm you know the recipient and are not being asked to move funds urgently. If you are unsure, please pause and contact a firm representative."

Proposed Objective Trigger Framework

To promote consistency and prevent arbitrary application, we recommend that FINRA provide non-exclusive examples of circumstances that support a reasonable belief of fraud. We suggest a structured but non-mandatory trigger framework. A rebuttable presumptive basis for invoking Rule 2166 could include:

a. A first-time transfer to a newly linked external account or unrecognized recipient; or
b. A transfer exceeding a defined percentage of account value or a customer-set threshold.

[5] *Security Guarantee*, ROBINHOOD, https://robinhood.com/us/en/support/articles/security-guarantee/ (last visited Mar. 6, 2026).

This approach targets high-risk transaction types, preserves autonomy through customizable thresholds, and aligns with existing Anti-Money Laundering ("AML") and fraud-prevention best practices. Many firms already employ similar monitoring tools for AML compliance and fraud detection. Leveraging these existing systems to identify high-risk disbursement patterns may therefore allow firms to implement Rule 2166 with a relatively limited additional operational burden.

Supplementary Risk Indicators

Drawing on FINRA's prior fraud guidance referenced in Regulatory Notice 23-06, the following non-exhaustive indicators could support a reasonable belief:

1. Velocity Indicators

a. Rapid liquidation of long-held positions;
b. Immediate outbound transfer following asset arrival;
c. High-frequency movements are inconsistent with prior activity.

2. Identity and Access Anomalies

a. Recently changed contact information;
b. Newly linked bank account;
c. IP address or geolocation discrepancies;
c. Device fingerprint inconsistencies.

3. Transfer Irregularities

a. Repeated rejected or corrected transfer instructions;
b. Serial submission of incomplete transfer requests;
c. Account title discrepancies.

4. Communication Pattern Changes

a. Sudden deviation from normal communication method;
b. Unusual grammar or tone;
c. Language emphasizing urgency or secrecy.

Providing illustrative factors would enhance supervisory defensibility without mandating a specific checklist.

Applicability Across Business Models

Member firms operate under a wide range of business models. Some maintain advisor-client relationships while others operate via fully digital platforms.

Online-only firms may lack direct phone contact, historical personal relationships, or in-person verification opportunities. FINRA should clarify that objective transaction-based indicators are sufficient as a basis to protect customers against fraud. AI-driven or algorithmic anomaly detection may support a "reasonable belief" of fraudulent activity, and direct verbal confirmation that a problem has occurred is not a prerequisite.

Absent such clarification, firms without traditional client interaction may underutilize the rule due to perceived evidentiary risk to the detriment of many of their most vulnerable clients.

While there will be some operational costs, including system upgrades, push-notification development, and staff training, we believe these costs will be offset by the losses that fraud would otherwise impose. This includes reputational and economic harm to member firms and a reduction in regulatory fines and customer arbitration exposure.

Operationalizing the Speed Bump

The Speed Bump is intended to function as an educational intervention. Effective implementation should include:

a. Immediate digital notification;
b. Real-time confirmation interface;
c. Neutral screening questions, such as:
    i. "Has anyone instructed you to move funds urgently?"
    ii. "Have you been told to keep this transaction confidential?"
d. Brief educational prompts regarding common fraud schemes.

Research cited in the Notice supports the effectiveness of emotional interruption and targeted awareness. The Notice explains that many scams rely on creating "a false sense of urgency or isolation" to pressure victims into acting quickly before they have time to reconsider the transaction. Recognizing this dynamic, the FBI advises consumers to "Take a Beat" and pause to assess the situation rather than responding immediately to urgent requests. The Notice references research suggesting that emotional stimuli can increase susceptibility to fraud and that awareness of common scam tactics can help reduce financial loss. A structured pause that allows firms to engage customers and highlight indicators of fraud can help disrupt the urgency and pressure that drive many modern scams. Moreover, the Notice emphasizes that the ability to pause gives the customer time to receive education about the specific type of suspected fraud they may be facing. Additionally, this moment of reflection gives customers the opportunity to evaluate the legitimacy of the request. In this way, the Speed Bump functions not only as a delay but as an opportunity for actual fraud awareness, increasing the likelihood that customers will recognize warning signs in the future.

FINRA may wish to consider providing illustrative language for firms to use in push notifications or digital warnings. Such examples could promote clarity and consumer

understanding while still allowing member firms the flexibility to test alternative messaging approaches. The Speed Bump should function as a cooling-off period. Firms should, however, not be prohibited from testing different templates to determine their effectiveness.

Preserving Customer Autonomy and Economic and Competitive Concerns

The Notice emphasizes balancing investor protection and autonomy. To reinforce that balance, customers should be permitted to customize transfer thresholds, and where appropriate, opt-out of additional safeguards above any baseline regulatory triggers. Firms should also be required to document override confirmations.

Additionally, while the Notice acknowledges potential indirect costs, including some possible lost opportunities and customer dissatisfaction, clarifying objective triggers, and allowing customer autonomy will reduce litigation risk, supervisory ambiguity, and uneven competitive impact. Furthermore, fraud prevention itself yields systemic economic benefits by preserving investor capital and reducing reputational harm to member firms.

Trusted Contact and Emergency Contact Framework Under Rule 4512

The Cardozo Clinic strongly supports efforts to promote the trusted contact/emergency contact framework. In most fraud cases that the Cardozo Clinic has encountered, particularly online investment scams and so-called "pig butchering" schemes, contacting a trusted contact would have at least mitigated the fraud and likely would have prevented the fraud from ever occurring.

Many consumers are already familiar with the concept of "emergency contact" from medical settings. Allowing firms to use this terminology therefore may reduce confusion and increase adoption. We therefore support FINRA's proposal in the Notice to allow firms to refer to the trusted contact as an "emergency contact." A limited anecdotal survey of the Cardozo Clinic's client population, however, suggests that many investors would be willing to designate a trusted contact when the purpose of the designation is clearly explained. For the clients surveyed, understanding how the designation could help them was more important than the terminology of the designation.

We therefore believe that providing clearer explanations of the trusted contact/emergency contact option and how it would work would encourage more people to designate a trusted contact and recommend that FINRA provide further guidance and language for firms to use.

Additionally, we recommend that firms check in on an annual basis to ensure that the named trusted contact is still appropriate. As the requirement currently stands, in accordance with Rule 4512 and 17 C.F.R. § 240.17a-3(a)(17) (2025), member firms are only required to provide customers with a copy of their account records within the first three years and list the individual designated as the customer's trusted contact. Customers must then notify the firm if they wish to make any changes to, among other things, the person designated as their trusted contact. Accordingly, the current system not only allows a designated trusted contact to become outdated

but also increases the likelihood that customers will inadvertently overlook opportunities to update this information. Over time, a trusted contact may become unavailable due to death, incapacity, or changes in personal relationships. Requiring periodic confirmation of the designated contact, such as during annual account updates, would help ensure that the information remains accurate and usable.

Incorporating such confirmation into existing account maintenance processes would impose a minimal operational burden while strengthening the effectiveness of the trusted contact framework.

Extension of the Temporary Hold Under Rule 2165

The Notice proposes extending the maximum temporary hold period under Rule 2165 from 55 business days to 145 business days. This proposal reflects the reality that investigations into financial exploitation frequently require considerable time and may involve coordination across institutions, jurisdictions, and law enforcement agencies.

Adult Protective Services investigations and law enforcement inquiries often extend well beyond the existing hold period. Available data indicates in a meaningful subset of cases, particularly where investigators must obtain financial records or coordinate across institutions and jurisdictions.[6] Extended holds necessarily raise concerns regarding investor autonomy and access to funds. However, these concerns are mitigated by Rule 2165's requirement that firms maintain a continuing reasonable belief of financial exploitation and document the basis for the hold. We believe that the Notice's proposed structured extension framework appropriately balances these concerns by requiring documentation and continued reasonable belief of exploitation.

Conclusion

The Notice's proposal represents an important step toward strengthening investor protection in an environment of rapidly evolving fraud risks. Fraud schemes targeting retail investors have grown dramatically in both scale and sophistication, and member firms are often uniquely positioned to detect suspicious activity before losses become irreversible.

Providing member firms with tools such as temporary transaction delays, expanded temporary hold authority, and a strengthened trusted contact framework has the potential to significantly reduce fraud-related losses while preserving investor autonomy.

---

[6] *See* L. McGee & K. Urban, Admin. Cmty. Living et al., Adult Maltreatment Data Report 2023 36–38 (2023), https://pfs2.acl.gov/strapib/2023_Adult_Maltreatment_Report_8e4fcee5f2.pdf. This report states that the national median duration of Adult Protective Services investigations is 36 days. *Id.* at 37–38 exhibit 5.5. State-level data show substantial variation. For example, Kentucky reported a median investigation duration of 72 days, Vermont 81 days, New Hampshire 90 days, and Washington 113 days. *Id.* Given that the figures provided are medians, these figures indicate that while many investigations conclude within several weeks, many investigations in various jurisdictions may exceed three months.

The effectiveness of the Notice's proposed rules will depend on clear operational guidance regarding the reasonable belief standard, appropriate indicators of fraud risk, and practical implementation of the temporary delay mechanism. Clarifying these elements would promote consistent application across firms while ensuring that the rules achieve their core objective of preventing fraud before losses occur.

The Cardozo Clinic appreciates FINRA's efforts in addressing these issues and welcomes the opportunity to engage with FINRA further as the rulemaking process continues.

Respectfully submitted,

The Cardozo Law School Securities Arbitration Clinic

Prof. Elizabeth Goldman, Director, Clinical Professor of Law

Olenka Ballena, Student Member

Drew Davis, Student Member

Michele Kallo, Student Member

Jacqueline Moshkovich, Student Member

Justin Rhee, Student Member

Casey Rosen, Student Member

Joshua Rosen, Student Member

Chrisann Timbie, Student Member

Benjamin Yasharpour, Student Member