FINRA Members Require Real-Time Deepfake Detection to Protect Investors and Comply with Modernized Fraud Prevention Standards

Jennifer Piorko Mitchell
Office of the Corporate Secretary
FINRA
1700 K Street, NW
Washington, DC 20006-1506

Re: Regulatory Notice 25-07

FINRA Members Face Direct Impact from AI-Enhanced Fraud

In 2024, FINRA imposed a $1.1 million fine against SoFi Securities for fraud prevention failures that enabled criminals to create 800 fraudulent accounts using stolen identities. The attackers transferred $8.6 million from customer accounts without authorization, withdrawing $2.5 million before detection. **FINRA determined that SoFi's "largely automated process for customer identity verification was vulnerable to fraud"** due to inadequate systems.

This enforcement action demonstrates how **FINRA members remain exposed to even relatively basic fraud schemes that AI and deepfake technology now makes exponentially more sophisticated, scalable, and profitable**. The same vulnerabilities that enabled SoFi's exploitation now allow threat actors to deploy AI-generated deepfakes for real-time impersonation attacks targeting broker-dealers, investment advisors, and funding portals. For FINRA members and their clients, these attacks are more common, more costly, and more difficult to avoid than conventional fraud efforts.

Generative AI-enabled fraud losses in the US financial sector could reach approximately $25 billion by 2027.[1] As FINRA acknowledges in its 2025 Annual Regulatory Oversight Report, fraudsters increasingly deploy **"deepfake media to impersonate well-known finance personalities"** and create **"synthetic IDs, deepfake media to establish new fraudulent brokerage accounts."**

A Critical Security Gap in Member Operations

[1] Deloitte Center for Financial Services, "Deepfake banking and AI fraud risk," May 28, 2024.

Current regulatory frameworks inadequately address the threat that deepfakes pose across FINRA member operations:

- **Customer Identity Verification:** AI-generated deepfakes enable identity theft by bypassing biometric evaluation or liveness checks for clients
- **Investment Advisor Impersonation:** Criminals use AI-generated content to impersonate registered representatives or “trusted contacts” in client communications
- **Executive Communication Authentication:** Deepfake impersonations authorize fraudulent transactions through audio or video calls to member firms or their clients
- **Account Takeover Prevention:** Deepfake impersonations enable sophisticated social engineering attacks to compel clients to share personal information or provide real-time feedback to circumvent multi-factor authentication

One in five FINRA members reports difficulty identifying customers despite implementing global KYC protocols, while **42 percent of fraud occurs during customer onboarding**—precisely where deepfake technology proves most effective.

Response to FINRA's Request for Comments

Section G.1: How have technological advances helped or hindered members' ability to fight fraud under FINRA rules, guidance and processes? What additional modifications or changes should FINRA consider to further address changes in fraud practices created by these advances?

Technological advances have created a dual impact on member fraud prevention capabilities. While automated identity verification systems have improved efficiency, they have simultaneously created new vulnerabilities that sophisticated fraudsters exploit. The SoFi Securities case demonstrates how largely automated processes, while cost-effective, can be exploited by criminals using stolen identities to create hundreds of fraudulent accounts.

Deepfake technology represents the next evolution of this threat, transforming static identity theft into dynamic, real-time impersonation attacks. Current FINRA guidance does not adequately address AI-generated content in communications, leaving members uncertain about acceptable detection and prevention measures.

FINRA should explicitly recognize real-time deepfake detection as a reasonable and necessary component of member fraud prevention programs, providing guidance that encourages deployment of automated detection systems analyzing voice, video, and image content during client interactions and internal communications. Incident response teams need deepfake detection capabilities to properly identify, track, and investigate deepfake-fueled intrusions.

FINRA should also modify its existing rules and guidance where it is insufficient to address the threat of deepfake technology:

Rule 3110 (Supervision) — This rule governing supervision activities assumes supervisors can independently authenticate communications and detect "red flags" in risk assessment, regulation, and process supervision. Deepfakes render these assumptions invalid by enabling perfect impersonation of clients across video and phone calls. Section 3110 should be amended to require supervisory procedures that address AI-generated content detection in communication reviews, establishing deepfake detection as a reasonable supervisory control for digital and phone communications.

Rule 2165 (Financial Exploitation of Specified Adults) — This rule's "reasonable belief" standard is gravely complicated by the possibility of genuine-seeming deepfakes that can impersonate trusted contacts designated under Rule 4512, family members, or specified adults themselves. FINRA should amend Section 2165 to recognize that deepfake impersonation attempts constitute financial exploitation, and require enhanced verification procedures when trusted contacts make unusual requests through digital channels.

Rule 4512 (Customer Account Information) — Obligations to obtain and verify authentic contact information are undermined by the possibility for deepfakes to impersonate clients and request changes to critical information for contact or verification purposes. FINRA should establish clear authentication protocols for communications with trusted contacts and clients, particularly for account information changes.

Rule 3310 (Anti-Money Laundering) — Given the prevalence of identity verification and customer identification to AML guidelines set out in Rule 3310, FINRA should specifically require reasonable technological measures to detect AI-generated synthetic media during the verification process.

Section G.5: Are there other tools (including rules, guidance or technology solutions) that FINRA can provide to members to further facilitate protection of senior and vulnerable investors from fraud and other types of financial exploitation?

Senior and vulnerable investors face heightened risk from AI-powered impersonation schemes that exploit their trust in familiar voices and faces. Deepfake technology enables criminals to impersonate family members, trusted advisors, or financial professionals with unprecedented accuracy.

Key risks for vulnerable investors are heightened by AI technology, especially in the case of AI impersonation schemes wherein criminals deepfake the investor to authorize fraudulent transactions, or deepfake trusted contacts to undermine Rule 2165 protections. FINRA members should implement real-time deepfake detection within their own communication platforms as well as providing guidance for clients to protect themselves outside of communication with their firms.

FINRA should clarify that automated deepfake detection constitutes an acceptable technology solution for enhanced investor protection, particularly for members serving senior and vulnerable populations. Clear guidance would enable firms to deploy real-time

detection capabilities without regulatory uncertainty, providing immediate alerts when AI-generated impersonations attempt to exploit vulnerable clients.

Section E.3: What are members' recordkeeping challenges regarding AI-generated communications and how do these challenges vary based on the type of AI-generated communication?

Members face uncertainty about recordkeeping obligations when using AI tools, including when deploying AI-powered fraud detection systems. Current guidance does not specify whether automated deepfake detection logs, threat analysis reports, and intervention records satisfy regulatory documentation requirements.

FINRA should specify that automated deepfake detection logs and intervention records constitute appropriate compliance documentation, enabling firms to demonstrate proactive fraud prevention measures while maintaining necessary audit trails. This clarity would eliminate regulatory uncertainty that may hinder deployment of advanced detection technologies.

Real-Time AI Detection to Address Compliance Gaps

Reality Defender's proven deepfake detection platform directly addresses the compliance vulnerabilities identified across FINRA's regulatory framework. Our technology enables members to maintain compliance with existing rules while protecting against AI-driven fraud in real time:

Compliance Enhancement: Real-time analysis of communications during supervisory reviews enables detection of AI-generated content in correspondence and internal communications, ensuring supervisors can reliably identify "red flags" and authenticate executive or sensitive communications requiring oversight.

Protection Reinforcement: Automated detection when contacting trusted contacts under financial exploitation procedures ensures members can verify authentic responses and prevent deepfake impersonation from undermining temporary hold decisions.

Identity Verification Support: Advanced authentication capabilities for customer and trusted contact communications protect account information integrity, especially during verification processes for account changes or emergency contacts.

AML Program Integration: Sophisticated identity verification enhancement detects AI-generated synthetic media during customer identification programs and ongoing monitoring, strengthening compliance with Customer Due Diligence requirements.

Implementation Recommendations

Immediate Regulatory Actions:

- Amend existing rule guidance to explicitly recognize deepfake detection as reasonable social engineering and fraud prevention technology
- Establish recordkeeping standards for AI-generated content detection logs and intervention records
- Create regulatory safe harbor for good-faith implementation of deepfake detection systems

Member Implementation Support:

- Develop technical standards for deepfake detection integration with existing compliance systems
- Establish suspicious activity reporting protocols for confirmed deepfake incidents affecting member operations
- Create information-sharing frameworks enabling members to report and defend against emerging deepfake attack patterns

Protecting Market Integrity Through Technological Adaptation

The SoFi case demonstrates that existing fraud prevention vulnerabilities become exponentially more dangerous when combined with AI capabilities. **FINRA's modernization initiative provides the essential opportunity to strengthen existing rules against deepfake threats while enabling members to deploy necessary detection technologies.**

Reality Defender's platform transforms regulatory compliance from reactive fraud detection to proactive threat prevention, enabling FINRA members to maintain investor protection standards in an era of AI-powered deception.

Sincerely,

Ben Colman
Co-Founder and CEO
Reality Defender

About Reality Defender: Reality Defender secures critical communication channels against deepfake impersonations, enabling financial institutions to operate with confidence. Our patented real-time multimodal detection technology integrates seamlessly with existing systems to protect assets and preserve trust.