

Statement of Bryan Smith
Senior Vice President, Complex Investigations, Financial Industry Regulatory Authority
Before the Subcommittee on Capital Markets
of the Committee on Financial Services
U.S. House of Representatives
April 15, 2026

Chairman Wagner, Ranking Member Sherman and Members of the Committee:

Thank you for the opportunity to appear today to discuss the Financial Industry Regulatory Authority's (FINRA) role and ongoing efforts to combat financial fraud and exploitation across capital markets. We appreciate the work of Chairman Wagner and Ranking Member Sherman to call attention to the rising fraud threat facing investors and the firms that serve them. Informed by my prior career with the FBI, I am glad to be able to lend my perspective as FINRA's head of complex investigations regarding the nature of fraud threats; FINRA's role in the ecosystem required to address fraud; and how technology and partnerships might help us do more – and move more quickly – to protect market participants from the individual investor to the large financial institution.

FINRA's mission is investor protection and market integrity. As a not-for-profit, self-regulatory organization (SRO), FINRA supports the Securities and Exchange Commission (SEC) in overseeing our broker-dealer member firms, comprising most broker-dealers doing business in the United States. FINRA regulates approximately 3,300 member firms with almost 149,000 offices and approximately 634,000 individual registered persons associated with those firms. As a national securities association registered with the SEC, FINRA's activities are subject to ongoing and extensive SEC examination and oversight, with multiple SEC inspections and reviews of FINRA's operations every year, including enforcement operations.¹

FINRA regulates its member firms and their associated persons in accordance with the Securities Exchange Act of 1934 (Exchange Act) and related rules adopted by the SEC. Our comprehensive regulatory program is designed to complement the SEC's broader oversight of broker-dealers and the securities markets more generally and includes – at no cost to taxpayers – writing rules, examining for and enforcing compliance with FINRA rules and federal securities laws, registering broker-dealer personnel and offering them education and training. FINRA also performs cross-market surveillance for equities, options and fixed-income markets to identify manipulation and other misconduct by monitoring billions of daily market events and leveraging innovative technology.

FINRA also provides critical market and regulatory services to members and the wider marketplace, including trade reporting and credentialing platforms. And, FINRA offers education

¹ We are examined regularly by the SEC's Technology Controls Program, Broker-Dealer Exchange Program, and the FINRA and Securities Industry Oversight Program office, whose primary responsibility is oversight of FINRA.

to the public, including through the FINRA Investor Education Foundation®, which supports investor research such as the U.S. National Financial Capability Study, an ongoing study benchmarking indicators of financial capability among investors.²

FINRA operates within a broader network of regulators, law enforcement authorities, and private parties who must collaborate closely to prevent, deter, and address fraud. While fraud can be found in all areas of the financial system, FINRA’s authority is generally limited to member firms and their associated persons. FINRA does not regulate other persons who solicit or handle customer money or assets but are not its members, which may include unregulated U.S. and non-U.S. persons and entities, issuers, investment advisers, investment companies, banks, insurance companies, futures commission merchants, and most providers of crypto assets and related services. Where we identify potential fraud involving persons outside our jurisdiction, we make appropriate referrals to other regulators and law enforcement authorities.

My testimony today will focus on the magnitude of the threat landscape for broker-dealer firms and investors from bad actors outside of the industry, and the unique role that FINRA plays as an SRO working in partnership with other groups to prevent, deter, and address fraud.

Investors and Broker-Dealer Firms Face an Increasing Fraud Threat

Investors, firms and markets are facing financial fraud threats that are unprecedented in scale and sophistication. Most U.S. adults report receiving scam messages on a daily or weekly basis, and over 40% of adults report that a scam email, text or call led them to give away personal information.³ The Federal Trade Commission (FTC) recently reported that customers suffered a staggering \$15.9 billion⁴ in losses in fraud in 2025, a 35.5% increase from 2024.⁵ The FTC further noted that the reports it receives may not capture a substantial portion of criminal activity.⁶ In 2024, the agency estimated that actual losses from fraud could be as high as \$195.9 billion due to underreporting (compared to \$12 billion reported).⁷ The fraud losses reported to the Federal Bureau of Investigation (FBI)’s Internet Crime Complaint Center involve cyber-enabled criminal activity broadly (including fraud outside of the financial services sector), and amount to a

² See Empowering Seniors through Financial Literacy: Tools to Protect Savings, Prevent Fraud, and Promote Independence: U.S. Senate Special Committee on Aging, 116th Cong. (2026) (Testimony of Christine Kieffer).

³ Financial Security Program, United We Stand: A National Strategy to Prevent Scams, pg. 7 (https://static1.squarespace.com/static/671a80aa4a84f2359ce4d360/t/690e1fe9c5c80642162575a5/1762533353206/FraudTFReport_Digital_Final+%282%29.pdf).

⁴ Federal Trade Commission, Prepared Statement of the Federal Trade Commission on The Rising Scam Economy: Modernizing Federal Approaches to Protect Americans from Foreign Fraudsters, before the United States Congress Joint Economic Committee (March 25, 2026), pg. 2 (https://www.ftc.gov/system/files/ftc_gov/pdf/ftc-testimony-jec-hearing-on-the-rising-scam-economy.pdf).

⁵ Consumer losses reported to the FTC have increased year-over-year for the past six years and have risen 430% since 2020. The aggregate totals are also immense. In 2025, victims reported \$15.9 billion in fraud losses to the FTC.

⁶ Prepared Statement of the FTC on The Rising Scam Economy, pg. 2 (https://www.ftc.gov/system/files/ftc_gov/pdf/ftc-testimony-jec-hearing-on-the-rising-scam-economy.pdf).

⁷ *Id.*

staggering leap, rising from \$4.2 billion in 2020, and steadily increasing post-COVID to \$10.3 billion in 2022, \$16.6 billion in 2024, and \$20.9 billion in 2025.⁸

This growth in fraud is a result of a combination of factors, including a global economy which has exponentially increased opportunities for adversaries to attack, an interconnected world where threat actors can impact individuals and firms continents away, and technology advancements such as encrypted communications and cryptocurrency which enable greater privacy, speed and efficiency in commerce but can also be used by bad actors to obfuscate their activity. These actors have also “professionalized” and organized under a “crime-as-a-service” business model in which these criminal organizations build networks of individuals with specialized “best in class” skills they can deploy against individual and company defenses to try to stay ahead of law enforcement. They have developed a highly adaptable criminal ecosystem which they leverage for a variety of cyber and financial crime schemes at a speed and scale which we have not seen before.

Technology Accelerates and Complicates Fraud

Technological advances have enabled a global economy which operates at greater efficiency and speed than during the pre-digital age. Yet those same advances are also being leveraged by threat actors. The affordable and easy access to encrypted communications channels means they can communicate with investors, and each other, without detection, while developments in digital asset technology enable them to transfer funds without the involvement of a regulated intermediary that could perform identity verification or monitor transactions, as well as allowing bad actors to instantaneously transfer and launder funds with a minimal paper trail. They leverage technical infrastructure such as Virtual Private Networks (VPNs), hosting providers, telecommunication systems, and social media entities to facilitate portions of their criminal scheme. For law enforcement agencies and regulators, determining which entity has jurisdiction over a particular incident may be difficult, and it can be impossible for any one entity to have a complete picture of the fraudulent scheme. To reconstruct these transactions not only requires significant technical expertise but often months or years of investigation.

While broker-dealer firms are tapping generative AI (GenAI) as a tool to fight fraud (as discussed further below), GenAI also allows criminals to rapidly scale these complex attacks, accomplishing in minutes what previously required extensive teams and substantial resources.⁹ Moreover, GenAI helps bad actors make their attacks more sophisticated, efficient, scalable and profitable. As an example, Microsoft reported last year that AI-generated phishing e-mails

⁸ Appendix A includes measures of cyber-focused fraud losses released this month by the FBI through its annual *Internet Crime Report from the Internet Crime Complaint Center*, available at https://www.ic3.gov/AnnualReport/Reports/2025_IC3Report.pdf.

⁹ Microsoft, Microsoft Digital Defense Report 2025, pg. 52-55 (<https://cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/microsoft/msc/documents/presentations/CSR/Microsoft-Digital-Defense-Report-2025.pdf#page=1>).

achieved a 54% click-through rate compared to 12% for standard phishing.¹⁰ Criminals may use AI-generated deepfakes to impersonate well-known finance personalities in social media advertisements, enticing investors to participate in fraudulent “investment clubs” hosted on encrypted messaging applications.¹¹ Once there, victims are persuaded to purchase shares of low-volume and thinly-traded securities.¹² Similarly, “imposter schemes” use GenAI to help bad actors impersonate legitimate brokerage firms or regulators (including the SEC and FINRA, and FINRA’s member firms), relying on existing confidence in these entities to manipulate investors.¹³ FINRA has also observed bad actors using GenAI as a force multiplier. Criminals without technical expertise can leverage AI to develop malicious tools they would otherwise lack the skills to create.¹⁴ Bad actors with existing knowledge can also create more sophisticated forms of malware, such as “polymorphic malware” which continuously changes its identifiable features to avoid detection by security products.¹⁵ Some observers estimate that GenAI-driven fraud could result in \$23 billion in losses by 2030.¹⁶

Bad Actors Increasingly Act Internationally

The nature of threats for investors has changed radically in recent years. Bad actors are now more dispersed yet organized – and specialized – whereas once they were more often local and disorganized. The modern threat landscape is dominated by international actors who use technology to exploit jurisdictional gaps across countries and regulators and evade prosecution, resulting in worldwide fraud losses estimated in 2024 at \$1.03 trillion.¹⁷ The fraudsters often

¹⁰ *Id.* at pg. 37. The company also estimates GenAI could make phishing 50 times more profitable by allowing bad actors to reach thousands of targets at minimal cost.

¹¹ KPMG, Deepfake Threats to Companies (<https://kpmg.com/xx/en/our-insights/risk-and-regulation/deepfake-threats.html>); FINRA, “Cybersecurity and Cyber-Enabled Fraud,” 2026 FINRA Annual Regulatory Oversight Report (<https://www.finra.org/rules-guidance/guidance/reports/2026-finra-annual-regulatory-oversight-report/cybersecurity>).

¹² FINRA, Investor Alert: Social Media “Investment Group” Imposter Scams Continue to Rise (<https://www.finra.org/investors/insights/investment-group-imposter-scams>).

¹³ FINRA, Investor Alert: Be Alert to Signs of Imposter Investment Scams (<https://www.finra.org/investors/insights/be-alert-signs-imposter-investment-scams>); FINRA, Cybersecurity Alert – Ongoing Phishing Campaign Impersonating FINRA Employees (<https://www.finra.org/rules-guidance/guidance/cybersecurity-alert-ongoing-phishing-campaign-impersonating-finra-employees>); Securities and Exchange Commission, SEC Impersonators May Lure Investors Into Scams Through Social Media or Text Messages – Investor Alert (<https://www.investor.gov/introduction-investing/general-resources/news-alerts/alerts-bulletins/investor-alerts/sec-impersonators-may-lure-investors-scams-through-social-media-or-text-messages-investor-alert>).

¹⁴ FINRA, “Cybersecurity and Cyber-Enabled Fraud,” 2026 FINRA Annual Regulatory Oversight Report (<https://www.finra.org/rules-guidance/guidance/reports/2026-finra-annual-regulatory-oversight-report/cybersecurity>).

¹⁵ *Id.*

¹⁶ Jill Gregorie, Satish Lalchand, Val Srinivas, Using Biometrics to Fight Back Against Rising Synthetic Identity Fraud (<https://www.deloitte.com/us/en/insights/industry/financial-services/financial-institutions-synthetic-identity-fraud.html>).

¹⁷ Global Anti-Scam Alliance, Global State of Scams Report (<https://gasa.org/knowledge-base/blog/global-state-of-scams-report-2024-1-trillion-stolen-in-12-months-gasa-feedzai>); Federal Bureau of Investigation, IC3 Annual Report (2024), pg. 16.

originate from or transit through countries that either lack the infrastructure to combat financial fraud or have limited or no frameworks for collaboration with U.S. law enforcement or regulatory agencies.

The complexity of these international schemes and the unclear jurisdiction make it difficult for victims to understand how, or to whom, they should report attacks by bad actors. A recent report found that three-quarters of victims who lost money to scams or online attacks never filed a report with law enforcement, citing confusing procedures, shame and hopelessness as reasons not to seek help from authorities.¹⁸ Federal and local regulators offer multiple reporting platforms for fraud and often use inconsistent terminology. This fragmentation of data may inhibit the ability of well-intentioned investigators to perceive and respond to significant changes in the fraud landscape.

Potential Harm from Fraud is Growing

Technology based schemes, domestic and abroad, take many forms – and the threats evolve. Individual investors, and broker-dealer firms, must be wary of a wide variety of fraud threats, from ransomware to account takeovers, listed in Appendix B.

The stakes of successfully avoiding rampant fraud are high for investors. Even smaller losses can be life changing when seniors stand to lose a lifetime of savings – the very savings that make them targets. FINRA Foundation research has found that senior investors may be particularly vulnerable to fraud, given they may have medical, social, and behavioral risk factors that make them more vulnerable to financial exploitation.¹⁹ According to the FBI's 2025 [Internet Crime Report](#), seniors 60 and older reported \$7.748 billion in losses from internet crimes that year alone—up 59% from 2024.²⁰

The stakes are high for broker-dealers as well, as broker-dealer firms are themselves targets of fraud in account takeover and other schemes, leading to reputational risks, loss of investor trust

¹⁸ Financial Security Program, United We Stand: A National Strategy to Prevent Scams, pg. 7 (https://static1.squarespace.com/static/671a80aa4a84f2359ce4d360/t/690e1fe9c5c80642162575a5/1762533353206/FraudTFReport_Digital_Final+%282%29.pdf).

¹⁹ For example, see DeLiema, M., Gao, S., Brannock, D., & Langton, L. (2025). The effects of risky behaviors and social factors on the frequency of fraud victimization among known victims. *Innovation in Aging*, 9(2), igae111. <https://academic.oup.com/innovateage/article/9/2/igae111/7934543>; Yu, L., Mottola, G., Kieffer, C. N., Lee, J., Kapadia, M., Han, S. D., Wroblewski, K., Bennett, D. A., & Boyle, P. A. (2023). Vulnerability of older adults to government impersonation scams. *JAMA Network Open*, 6(9), e2335319. <https://jamanetwork.com/journals/jamanetworkopen/fullarticle/2809785>; Yu, L., Mottola, G., Bennett, D. A., & Boyle, P. A. (2021). Adverse impacts of declining financial and health literacy in old age. *The American Journal of Geriatric Psychiatry*, 29(11), 1129-1139. <https://www.sciencedirect.com/science/article/abs/pii/S1064748121002098?via%3Dihub>

²⁰ Federal Bureau of Investigation, Internet Crime Report (2025) pg. 44 (https://www.ic3.gov/AnnualReport/Reports/2025_IC3Report.pdf).

and increased costs. In the FBI's Internet Crime Report, investment fraud had the highest loss figure for the third year in a row at \$8.648 billion.²¹

In the face of this elaborate, technology-fueled threat environment, we also have opportunities for interventions that powerfully leverage technology, and the opportunity to work with an ecosystem of law enforcement, regulators, companies, educators and others to prevent and address fraud. And, as detailed later, FINRA provides rules that help broker-dealers prevent losses – such as permitting broker-dealers to place temporary holds on accounts under specified circumstances.

The Unique Role of Self-Regulation in Fighting Fraud

FINRA has a long history of protecting investors and ensuring market integrity, with a well-developed set of programs, tools, and partnerships to fight fraud. But as the nature of the threat has evolved, leveraging more sophisticated technology and transnational networks, so too must FINRA. FINRA has sought to build on its strengths as an SRO to help fight fraud, leveraging expertise and insights from our member firms, sharing intelligence across the industry, deploying practical tools for use by our member firms, and cultivating public-private partnerships with law enforcement agencies and other regulators.

Our commitment to continuous improvement in the face of the changing risk landscape is embodied in FINRA Forward, the initiative we launched last year to advance our mission through rule modernization, empowering member firm compliance, and combating cybersecurity and fraud risks.²² Central to this program is a recognition that supporting effective compliance up front can often better protect investors and markets than addressing problems after the fact. This focus on prevention is especially important for financial fraud, where the proliferation of new, more sophisticated threat actors demands proactive, cooperative measures to stay one step ahead.²³

FINRA Enables Unique Risk and Threat Information-Sharing to Member Firms

FINRA has always shared risk and threat mitigation information with its member firms. But we have taken that to the next level with the launch of the Financial Intelligence Fusion Center (FIFC).²⁴ The FIFC is a secure, centralized portal available to all FINRA member firms designed to

²¹ *Id.*

²² Robert Cook, News Blog: New FINRA Initiatives to Support Members, Markets and the Investors They Serve (April 21, 2025) (<https://www.finra.org/media-center/blog/new-finra-initiatives-support-members-markets-and-investors-they-serve>).

²³ *Id.*

²⁴ FINRA, News Release: FINRA Launches Financial Intelligence Fusion Center to Combat Cybersecurity and Fraud Threats (<https://www.finra.org/media-center/newsreleases/2026/finra-launches-financial-intelligence-fusion-center-combat>).

proactively collect, analyze and disseminate timely, actionable threat intelligence to member firms.²⁵

The FIFC relies on internal and external information sources, aggregating intelligence from FINRA, member firms, regulators, technology companies and law enforcement to better understand threats facing the broker-dealer industry.²⁶ This bi-directional intelligence sharing platform takes advantage of the respective capabilities of firms and FINRA. Firms bring unique "in the moment" insight into the threats they are seeing; FINRA brings the ability to combine this information with a broader industry wide view, giving context for the firm's individual reports. Member firms can then better respond to threats while FINRA can better identify new schemes or tactics to disseminate as intelligence to the industry.²⁷ FINRA can also improve that intelligence with information from internal FINRA sources, other regulators, technology companies and law enforcement, among other sources.²⁸ This information is also shared with our Investor Education group so these insights can help both firms and investors protect against fraud.

In a short time, the FIFC has already had a meaningful impact. On the day of the FIFC's launch, three firms shared intelligence about a fraudulent e-mail purporting to be from various regulators, including FINRA and the SEC, asking firms for a call to discuss regulatory issues. Within two hours, FIFC teams published a Cybersecurity Alert about these e-mails to the over 700 individual FIFC users who signed up on launch day. Without the FIFC, it may have taken a few days to receive the complaints, recognize the connection, and issue an alert. With this real-time platform, the time between the threat actor emailing the first firm to the dissemination of the Alert to all member firms was three hours. To date, we know of no firms who were victimized by this particular scam.

FINRA Provides Hands-On Cybersecurity and Fraud Training for Member Firms

FINRA augments intelligence-sharing initiatives like FIFC with hands-on training for member firms, like our Cyber Workshops and Tabletop Exercises (TTXs). These immersive, scenario-driven sessions are designed to help our member firms strengthen their ability to identify, respond to and recover from cyber-threats by simulating real-world incidents.²⁹ FINRA has held TTXs across the country on a range of topics, including incident management, GenAI-powered social engineering and trading platform issues.

²⁵ See <https://fifc.finra.org/>.

²⁶ FINRA FIFC News Release (<https://www.finra.org/media-center/newsreleases/2026/finra-launches-financial-intelligence-fusion-center-combat>).

²⁷ *Id.*; See <https://fifc.finra.org/>.

²⁸ *Id.*

²⁹ See FINRA, Cyber Workshops & Tabletop Exercises: Prepare for Potential Cybersecurity Events (https://www.finra.org/sites/default/files/2025-07/Cyber_Workshops_and_Tabletop_Exercises.pdf); see also, FINRA, Combating the Adversarial Use of GenAI (<https://www.finra.org/events-training/on-demand-education/combating-adversarial-genai-use>).

FINRA Provides Critical Resources to Member Firms with Third Party Vendor Risks

Of the sixteen critical infrastructure sectors, whose assets, systems and network are considered vital to the U.S. under Presidential Policy Directive 21, the financial services industry is the most reliant upon third party entities in support of their operations. Yet not all firms possess the same knowledge and expertise on the cybersecurity risks from these third parties. FINRA has devoted significant resources to these vendor-related risks, with a Cyber & Operational Resilience (CORE) team focused on sharing actionable risk intelligence with member firms.³⁰ CORE analyzes information from member firms, open-source intelligence, dark web monitoring and other resources to detect breaches and vulnerabilities that can affect our members. The CORE team then delivers actionable intelligence to the impacted firms directly with tailored intelligence about a threat impacting the firm and specific suggestions for mitigating the potential harm.

FINRA Shares Threat Mitigation Tactics with Member Firms

Beyond our non-public CORE alerts, FINRA also publishes actionable information for firms about other risks that may affect their customers and operations, as well as suggested mitigation tactics. Certain publications, like FINRA's public Cyber Alerts, are aimed at raising broader awareness among member firms about emerging risks and mitigation strategies.³¹ Others, like FINRA's Threat Intelligence Products (TIPs), are designed to provide actionable intelligence to FINRA member firms and are kept private to prevent bad actors from seeing sensitive information and changing their tactics.³² When FINRA detected an increase in complaints about imposter sites impersonating FINRA member firms and their personnel, we sent our member firms a TIP and created a "takedown tool-kit," which is currently available on our website, that provides step-by-step instructions for firms to identify, view and take down these sites.³³ In addition to these resources, FINRA continues to search for fake sites, resulting in nearly 500 takedowns of fraudulent sites in the last year.

Certain TIPs to member firms outline the specifics on the adversarial use of GenAI and how it can be leveraged in fraudulent schemes and attacks. Our efforts have focused on specific threat activities and how GenAI is leveraged in the context of known fraud activities such as investment fraud scams, new account fraud, and ransomware, among others. This approach provides firms with specifics so they can review their processes and technical alerts to better detect and identify new GenAI-driven variations on these existing schemes.

³⁰ See FINRA, Cyber & Operational Resilience (CORE) (https://www.finra.org/sites/default/files/2025-07/FINRA_CORE.pdf).

³¹ See e.g., FINRA, Cybersecurity Alert, Ongoing Phishing Campaign Impersonating FINRA Employees (<https://www.finra.org/rules-guidance/guidance/cybersecurity-alert-ongoing-phishing-campaign-20260123>);

³² FINRA, Threat Intelligence Product: Protecting Vulnerable Adult and Senior Investors (<https://www.finra.org/rules-guidance/key-topics/senior-investors/tip-protecting-vulnerable-adult-senior-investors>).

³³ FINRA, Imposter Website Takedown Toolkit (<https://www.finra.org/sites/default/files/2026-01/takedown-toolkit.pdf>).

FINRA Shares Emerging Practices on Leveraging GenAI to Help with Fraud Detection and Mitigation

While GenAI in the wrong hands poses a significant challenge for investors targeted by fraud, there is also the potential for great benefits. FINRA is working to share emerging practices of those firms that are developing GenAI-driven fraud detection and mitigation strategies.³⁴ Potential use cases include agentic AI software programs that autonomously identify and analyze data to execute routine fraud detection workflows with faster escalation protocols, and AI systems that autonomously monitor alerts or trading activity to identify potential market manipulation, insider trading, and other prohibited practices utilizing adaptive technology with varying levels of human oversight. By facilitating information sharing and developing a common terminology around firms' use of GenAI, we believe we can help our member firms develop a pathway to gaining an advantage in addressing and preventing fraud using the latest tools and techniques.

FINRA Gives Member Firms Tools to Protect Seniors and Vulnerable Adults

FINRA has adopted rules for broker-dealers that are designed to help to protect senior investors and other vulnerable adults, including rules regarding the establishment of trusted contacts on accounts and temporary holds on securities transactions and disbursements of funds or securities where exploitation is suspected.³⁵ This rule on temporary holds was the first uniform national standard for placing temporary holds to address suspected financial exploitations. FINRA is soliciting feedback on further rule changes to provide greater flexibility under these rules and a new "speed bump" to help alert all customers of suspected fraud.³⁶ FINRA also works with the National Adult Protective Services Association and protective services offices across the country to provide education on fraud trends and the role that FINRA rules can play in halting suspected financial exploitation.

Bringing Government and Industry Together to Fight Fraud

FINRA's working relationships go well beyond its connections with member firms. The ability of regulators and private companies to address sophisticated fraud schemes relies upon the success of relationships with state and local law enforcement, federal regulators, private companies and international groups to share information and respond. Accordingly, FINRA maintains strong collaborative relationships with domestic regulators and agencies, such as the FBI, CFTC, SEC, exchanges, banking regulators and law enforcement agencies, along with foreign regulators in countries that have robust enforcement programs.

³⁴ See <https://www.finra.org/media-center/blog/observations-on-ai-agents>.

³⁵ See <https://www.finra.org/rules-guidance/rulebooks/finra-rules/2165>.

³⁶ See <https://www.finra.org/rules-guidance/notices/26-02>.

On the international front, FINRA works through ten formalized memoranda of understanding with agencies based around the world,³⁷ exchanging information on emerging trends, risks, and potentially fraudulent activity. These discussions help FINRA better understand how global fraud schemes and tactics are evolving. FINRA makes referrals to foreign regulators in matters where there is potential misconduct in the foreign jurisdiction or foreign investor harm, but where FINRA or U.S. authorities may not have jurisdiction or a significant interest. Similarly, we receive referrals and regulatory intelligence from foreign regulators that may inform our risk assessments and investigations.

Domestically, FINRA maintains robust coordination with state regulators through frequent communication and collaborative initiatives to combat fraud, protect investors and support market integrity. FINRA and state regulator subject matter experts are often featured at each other's trainings and events. In just one of many examples, last year FINRA staff presented on topics including scams that impact senior investors and how artificial intelligence may be used to detect and prevent financial fraud.

FINRA also partners with private companies beyond its membership base. For example, FINRA collaborated with Microsoft's Digital Crimes Unit (DCU) in their effort to take legal action against the ONNX Store (ONNX), a "Phishing-as-a-Service" (PhaaS) targeting Microsoft 365 accounts at FINRA member firms.³⁸ ONNX used an advanced social engineering attack known as "quishing," where a bad actor emails PDFs embedded with QR codes that redirect victims to malicious websites.³⁹ FINRA had separately received intelligence about this threat and published an alert for our members.⁴⁰ The DCU found FINRA's alert and collaborated with us in a legal action that led to the seizure of 256 fraudulent websites associated with ONNX, significantly disrupting ONNX's criminal capabilities.⁴¹ The outcome in the ONNX matter demonstrates the results that can be achieved through collaborative intelligence sharing and coordinated responses.

Educating Investors to Fight Fraud

FINRA has long provided investor education and fraud trend alerts directly to investors, and offers resources detailing how investors can take steps to safeguard their investments and

³⁷ See e.g., FINRA, Memorandum of Understanding with United Kingdom Financial Services Authority (Sept. 15, 2010) (<https://www.finra.org/sites/default/files/industry/p122102.pdf>).

³⁸ Steven Masada, Targeting the Cybercrimes Supply Chain (<https://blogs.microsoft.com/on-the-issues/2024/11/21/targeting-the-cybercrime-supply-chain/>); FINRA, Cyber Alert: ONNX Store Purportedly Targeting Firms in Quishing Attacks (<https://www.finra.org/rules-guidance/guidance/cybersecurity-alert-onnx-store-purportedly-targeting-firms-quishing-attacks>).

³⁹ *Id.*

⁴⁰ FINRA, Cyber Alert: ONNX Store Purportedly Targeting Firms in Quishing Attacks (<https://www.finra.org/rules-guidance/guidance/cybersecurity-alert-onnx-store-purportedly-targeting-firms-quishing-attacks>).

⁴¹ Masada, Targeting the Cybercrimes Supply Chain (<https://blogs.microsoft.com/on-the-issues/2024/11/21/targeting-the-cybercrime-supply-chain/>).

identities from fraud threats.⁴² Among other tools, Social media is widely used by investors and FINRA has collaborated with numerous industry regulators and organizations on targeted social media campaigns focused on increasing awareness of specific scams or on adding a trusted contact to investment accounts. FINRA has also trained social media companies to identify channels for fraudulent investor schemes, equipping those companies to better detect and prevent fraud.

Elder Americans and other vulnerable adults can be particularly susceptible to fraud, especially where they lack appropriate tools and education. In 2025, FINRA initiated the FINRA CARES (Comprehensive Assistance and Resources for Elder Security) initiative focused on expanding outreach events with member firms, investors, state regulators, and others and enhancing elder fraud related resources and tools for members. These resources include scenario-based workshops to empower member firms to identify and respond to common elder fraud scenarios. In addition, FINRA’s Securities Helpline for Seniors (Senior Helpline) is a toll-free number (844-57-HELPS or 844-574-3577) that has aided senior investors for over 10 years with concerns about their accounts, investments and interactions with firms.⁴³ In its first 10 years, the Senior Helpline assisted in recovering more than \$9.3 million for investors.

Fighting Fraud and Returning Money to Investors

Prevention is a critical part of FINRA’s efforts to address the fraud threat, but FINRA also helps to directly mitigate the realized harm to investors where we can. For example, a senior investor recently called the Helpline about an issue that turned out to be a computer takeover scam. That information led to a member firm putting a stop to a suspicious transaction and returning almost \$250,000 to the investor.

Another example of helping to stop harm came in 2024, when FINRA identified a change in tactics for investment fraud schemes. Fraudsters were leveraging social media “investment clubs” to lure investors into “pump and dump” schemes with millions in losses. FINRA shared that intelligence with firms and engaged with one of the social media companies whose platform was being exploited. The company shut down over 7 million accounts affiliated with fraud and disseminated a [Public Service Announcement](#) on the activity. To keep pace with the response to these actions by fraudsters, FINRA provided additional intelligence TIPS to member firms and additional training of U.S. Department of Justice (DOJ) and FBI staff covering the schemes.

In 2025, bad actors in China posed as U.S.-based investment advisors on social media, lured people into buying stock with promises of huge returns, drove the price up artificially, then dumped their shares and made millions. Meanwhile, investors — some of whom lost nearly

⁴² See e.g., FINRA, Scam Prevention & Assistance Resources (<https://www.finra.org/rules-guidance/key-topics/scam-prevention-assistance-resources>).

⁴³ See <https://www.finra.org/investors/need-help/helpline-seniors>; FINRA, Regulatory Notice 26-02 (<https://www.finra.org/rules-guidance/notices/26-02>).

everything — watched the stock collapse. FINRA’s broader efforts to surveil for these types of schemes and keep member firms informed paid off when a firm contacted FINRA staff directly about unusual and potentially illicit proceeds from this activity. That information was referred by FINRA to the FBI and DOJ investigators who ultimately seized over \$200 million in criminal proceeds and subsequently indicted seven individuals involved in the scheme. The DOJ has since created a remission fund to compensate victims using the funds it seized.⁴⁴ To assist with this effort, FINRA reviewed our complaint system and identified over 200 victims who reported this fraud. FINRA contacted each victim to inform them of the potential recovery of their assets and referred them to the DOJ/FBI victim assistance site.

A few months later, FINRA identified a similar case and referred it to DOJ and FBI, resulting in the seizure of \$70 million in illicit proceeds. And in a separate case, the DOJ announced the creation of the Roger Knox Remission Fund—over \$12 million in forfeited funds—to compensate victims of microcap pump-and-dump schemes carried out by a network of bad actors.⁴⁵ Roger Knox and others were cited in several FINRA referrals to the SEC concerning suspected market manipulation involving numerous microcap issuers.

FINRA also maintains a robust surveillance system that allows us to monitor, on average, a little under a trillion market events each day for potential red flags.⁴⁶ This intelligence, combined with information FINRA receives from dedicated teams that review customer complaints and tips, informs thorough investigations that frequently lead to referrals to other regulators. In 2024, FINRA referred over 1,300 fraud and insider trading cases to the SEC and other federal or state law enforcement agencies for potential prosecution.⁴⁷ It is not unusual that when we make these referrals to the SEC and criminal authorities, they lead to prosecutions and monetary sanctions against bad actors in the markets.

As a recent example, a FINRA investigation and series of referrals contributed to SEC and DOJ cases against two individuals that allegedly ran a years-long securities fraud and money laundering scheme relating to the securities of six publicly traded companies.⁴⁸ The DOJ has

⁴⁴ United States Department of Justice, Press Release: U.S. Department of Justice Announces Compensation Process for Victims of Chinese Liberal Education Holdings Ltd. (CLEU) Investment Fraud Scheme (Feb. 3, 2026) (<https://www.justice.gov/opa/pr/us-department-justice-announces-compensation-process-victims-chinese-liberal-education>).

⁴⁵ United States Department of Justice, Press Release: U.S. Department of Justice Announces Distribution of Over \$15.5 Million to Compensate Victims of Massive Global Securities Fraud Scheme (Mar. 2, 2026) (<https://www.justice.gov/opa/pr/us-department-justice-announces-distribution-over-155-million-compensate-victims-massive>).

⁴⁶ FINRA, FINRA Unscripted: Navigating the 2026 Regulatory Oversight Report: Key Insights from FINRA Leadership (Dec. 9, 2025) 04:41-5:40 (<https://www.finra.org/media-center/finra-unscripted/navigating-the-2026-regulatory-oversight-report-key-insights-from-finra-leadership>).

⁴⁷ FINRA, Annual Financial Report (2024), pg. 5 (<https://www.finra.org/sites/default/files/2025-06/2024-finra-annual-financial-report.pdf>).

⁴⁸ United States Attorney’s Office Southern District of California, Press Release: La Jolla-Based Couple Charged with \$100 Million Fraud (<https://www.justice.gov/usao-sdca/pr/la-jolla-based-couple-charged-100-million-fraud>); Securities and Exchange Commission, Litigation Release: SEC Charges Three Individuals and Corporation for Their Role in Alleged Microcap Stock Fraud (<https://www.sec.gov/enforcement-litigation/litigation-releases/lr-26475>).

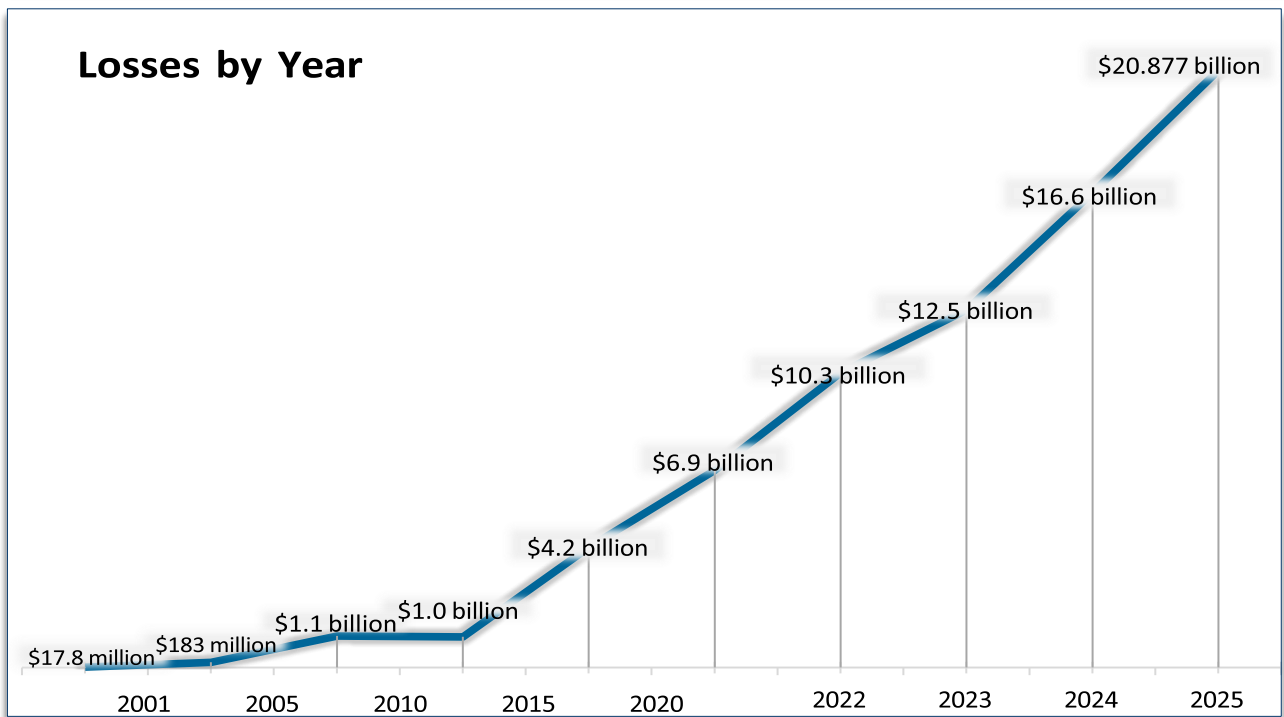
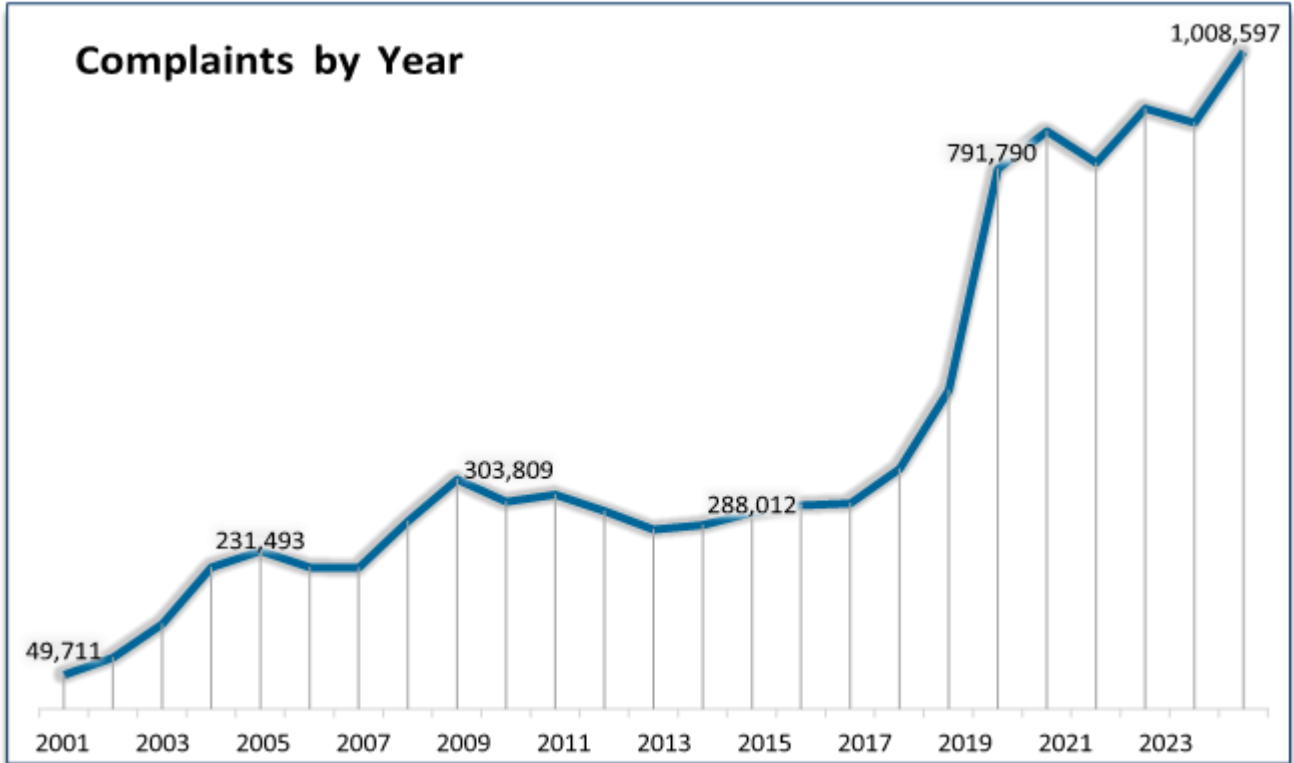
filed a 24-count indictment against the individuals and the SEC has brought a civil fraud case against them, their company and the CEO of one of the companies they allegedly promoted.⁴⁹

These successes and others demonstrate the value of information sharing in a self-regulatory organization and the power of cross-market surveillance, as well as the importance of coordinated efforts with firms, private sector, and law enforcement. This coordination is critical for stopping fraud and getting restitution back to victims. FINRA recognizes that there is always room for improvement; that is why we have worked to create tools like the FIFC that speed connections among firms, regulators, vendors and other sources so that we can leverage our respective expertise and authorities to together detect and defeat fraud.

Conclusion

Investors and broker-dealer firms confront an increasingly complex and evolving threat landscape, with fraud expanding amid rapid technological change and the globalization of fraudulent activity. FINRA fulfills a vital role within the broader ecosystem gathered to address these threats. Drawing on our unique capabilities as a self-regulatory organization, FINRA can: empower member firms through threat intelligence and market data; empower investors through education, fraud alerts, and robust enforcement; empower law enforcement through referrals, tips, and best practices; and empower other private sector participants to better identify and stop fraud. These coordinated efforts slow or even stop bad actors while building resilience among individuals and firms. We welcome the opportunity to continue to serve as a resource to Congress as it seeks to address fraud and protect investors and markets.

⁴⁹ *Id.*



Appendix B – Investor Fraud Landscape

- *Ransomware and Extortion Events*: cyberattacks involving unauthorized access to firm systems, often installing malware to encrypt or access and steal sensitive firm data or customer information. The stolen or encrypted data is held for ransom;
- *Data Breaches*: unauthorized access, acquisition or disclosure of confidential information, such as firm data and customer data, including personally identifiable information (PII);
- *Phishing, Smishing or Quishing*: deceptive social engineering attacks using email, SMS text messages or QR codes to redirect customers to malicious domains for the purposes of gathering their login and other credentials;
- *New Account Fraud*: attacks using falsified customer information or stolen identity information often purchased from criminal sites on the dark web, via a mobile app or internet browser, for the purpose of opening accounts;
- *Account Takeovers*: threat actors using compromised customer login credentials to gain unauthorized access to online accounts;
- *Account Impersonations*: threat actors using stolen customer information in combination with a compromised or spoofed email address to initiate actions, often a third-party wire transfer request, from the customer’s account;
- *Imposter Sites*: attacks leveraging spoofed domains and social media profiles (including those that impersonate financial firms, registered representatives and FINRA staff) to defraud firms and customers;
- *Relationship Investment Scams*: deceptive schemes targeting customers directly through social media or through text messages, establishing trust and then defrauding their victims; and
- *Insider Threats*: incidents involving firm employees who purposely or inadvertently use their access to firms’ systems to cause harm to firms and their customers.
- *GenAI-Enabled Fraud*: threat actors exploiting GenAI’s ease of use and wide range of applications to enhance their cyber-enabled crimes, for example, by:
 - generating fake content (e.g., imposter sites, false identification documents, deepfake audio and video);
 - creating polymorphic malware, which is a type of malicious software that constantly morphs, evolves or changes appearance to avoid detection by security products; and
 - leveraging GenAI models to develop malicious tools, allowing those without technical ability to become sophisticated cybercriminals.
- *Cybercrime-as-a-Service*: criminals with technical expertise selling tools and services—including information stealers, phishing kits and ransomware—to less technical threat actors, allowing them to commit sophisticated cybercrimes.

Bryan Smith Biography

Bryan Smith currently serves as FINRA's Senior Vice President for Complex Investigations & Intelligence as part of the Regulatory Operations-Investigations program. In this role, he oversees FINRA's specialized investigative teams through the Cyber and Analytics group which houses FINRA's Cyber-Enabled Fraud, Cyber Security Group, and the Crypto Asset Investigation teams as well as the Illicit Finance & Fraud group composed of the Anti-Money Laundering Teams (AML), the Anti-Fraud Investigative Team (AFI); the High Risk Representative Group (HRR); and the Vulnerable Adults and Seniors Investigation Team (VAST) as well as being responsible for U.S Law Enforcement Engagement.

Prior to joining FINRA, Bryan spent more than 21 years with the FBI as a Special Agent and most recently was the Section Chief for the FBI's Cyber Criminal Operations, responsible for all of the FBI's investigations and operations against cyber criminal actors and threats. He served as the U.S. lead for the 37-country Counter-Ransomware Initiative, Disruption efforts, Previous FBI leadership assignments included leading the Cyber/White Collar branch of the Cleveland office, the FBI's national money laundering/bank fraud program, and serving as the FBI Detailee to the U.S. Securities and Exchange Commission where he assisted both agencies in insider trading, market manipulation, and investment fraud matters. His experience crosses over financial crimes, cyber, and virtual currency and in 2013 he initiated the FBI's first unit focused on cryptocurrency. A proponent of public private partnerships he initiated several private sector outreach efforts to better leverage the complementary knowledge of both. Prior to the FBI, he worked as a systems and business consultant for Accenture and Deloitte.