BROKERAGE FIRMS AND SCAMS

ABSTRACT

ADAM GANA, MICHAEL C. BIXBY, AND BENJAMIN P. EDWARDS*

Often supported by artificial intelligence, transnational criminal organizations now steal billions of dollars from Americans each year with increasingly inventive scams and frauds.. These thefts currently fuel human trafficking, terrorism, forced criminality, sexual exploitation, and undermine the rule of law across southeast Asia and other regions around the globe. By failing to protect their customers and respond to red flags for fraud, financial exploitation, or scams, brokerage firms now allow their customers to be victimized and supply these organizations with the capital necessary to expand operations, driving rampant human trafficking and criminality overseas. Regulatory and policy inaction has failed to spur brokerage firms to become more vigilant protectors and meet the current challenge. This essay argues that regulators and policymakers must take more aggressive steps to ensure that brokerage firms comply with existing obligations and amend existing rules to clarify expectations that key intermediaries respond to suspicious activities. More effective fraud interdiction efforts are necessary to protect investors and deprive criminal organizations of the capital they use to victimize others.

* Adam Gana is the managing partner of Gana Weinstein LLP and the president of the Public Investors Advocate Bar Association (PIABA). Michael C. Bixby is the founder and managing attorney of Bixby Law PLLC and the incoming president of PIABA. Benjamin Edwards is a Professor of Law at the William S. Boyd School of Law at the University of Nevada, Las Vegas and the incoming vice-president of PIABA. Thanks to Jennifer Shaw and Joe Wojciechowski for their efforts in helping us make this paper a reality.

Table of Contents

I. Introduction and Background

Regulators and policymakers have largely failed to mobilize and combat industrial-scale fraud operations. This lassitude has allowed scam operations to metastasize, leaving investors with substantial losses and fueling explosive growth in criminal networks. In the absence of effective regulatory leadership, burned investors now seek recoveries in arbitration. Instead of leaving investors to fight alone after being victimized, government and industry regulators must act to make securities accounts harder targets for scammers to hit.

Successful scams now steal astounding sums. For example, an arbitration panel recently ordered Morgan Stanley to pay $843,000 in damages to Marjorie Kessler, a septuagenarian investor.[1] After talking to scammers, Kessler became convinced that "her identity had been stolen and she needed to convert her assets to cash, gold and cryptocurrency that would be deposited into a U.S. Treasury account for safe keeping."[2] While running the fraud, scammers obtained "gold bullion bars worth more than $1.6 million" from Ms. Kessler's funds.[3]

Critically, Morgan Stanley did not steal Ms. Kessler's funds—an unknown scammer did. Morgan Stanley argued that it should not have been held liable as "Ms. Kessler made misstatements to her financial advisor about the purpose of the transfers and authorized them to be sent to a third-party bank account held in her name."[4]

Yet this does not mean that Morgan Stanley was blameless in the matter. The claim alleged that Morgan Stanley missed "glaring red flags and obvious warning signs of financial exploitation" and facilitated the "withdrawal of $2.09 million in funds from a line of credit and the liquidation of assets from a life insurance trust during a nine-day period."[5] The claim also alleged that Kessler had asked her advisor to keep the withdrawals "'secret' and not to disclose them to her son, who had been directly involved in every major decision in his mother's investment accounts during the prior

---

[1] Karmen Alexander, *Morgan Stanley Ordered to Pay $843,000 in Elder Fraud Case*, ADVISOR HUB, Feb. 12, 2025, https://www.advisorhub.com/morgan-stanley-ordered-to-pay-843000-in-elder-fraud-case/.
[2] *Id.*
[3] Bruce Kelly, *Morgan Stanley loses $843,000 investor claim stemming from 'gold bar' scam*, INVESTMENT NEWS, Feb. 11, 2025, https://www.investmentnews.com/alternatives/morgan-stanley-loses-843000-investor-claim-stemming-from-gold-bar-scam/259274.
[4] *Id.*
[5] *Id.*

six years."[6] Effective schemes, like the one that victimized Ms. Kessler, often isolate targets and prevent them from talking to others about the true reasons for their withdrawals.[7] When trusted advice firms like Morgan Stanley fail to respond to red flags, they leave their customers as soft targets, ripe for scammers to exploit.

There are many people like Marjorie Kessler across America. Data from the Federal Trade Commission (FTC) indicates that Americans lost at least $10 billion to fraud in 2023.[8] Of that figure, investment scams generated over $4.6 billion in losses with imposter scams taking in at least another $2.7 billion.[9] In reality, these figures likely dramatically underreport the true scale of the losses because many victims do not report their losses to the FTC.

Remarkably effective modern scams differ from the con-artistry of yesteryear because technology now grants scammers global reach. Ubiquitous smart phones allow scammers to communicate with almost anyone at any time and can make it appear that they are communicating from within the United States based on spoofed phone numbers. Generative artificial intelligence technology supports operations at scale and in multiple languages.[10] The United Nations Office on Drug and Crime (UNODC) reports that cyber-fraud operations have now reached "industrial proportions."[11] These criminal networks now engage in massive human trafficking and forced labor operations to operate at scale.[12] To handle all of

---

6 *Id.*

7 Minnesota Attorney General's Office, How to Spot a Scam, https://www.ag.state.mn.us/consumer/publications/howtospotascam.asp#:~:text=Scam%20artists%20may%20ask%20consumers,situation%20and%20get%20their%20opinion: (last visited May 28, 2025) ("Scam artists may ask consumers not to tell anyone about the situation so that the consumer doesn't get advice from someone who might detect the scam").

8 FTC, As Nationwide Fraud Losses Top $10 Billion in 2023, FTC Steps Up Efforts to Protect the Public (Feb. 9, 2024), https://www.ftc.gov/news-events/news/press-releases/2024/02/nationwide-fraud-losses-top-10-billion-2023-ftc-steps-efforts-protect-public.

9 *Id.*

10 Matt Burgess & Lily Hay Newman, *Pig Butchering Scams Are Going High Tech*, WIRED (Oct. 12, 2024), https://www.wired.com/story/pig-butchering-scams-go-high-tech/.

11 UNODC, TRANSNATIONAL ORGANIZED CRIME AND THE CONVERGENCE OF CYBER-ENABLED FRAUD, UNDERGROUND BANKING AND TECHNOLOGICAL INNOVATION IN SOUTHEAST ASIA: A SHIFTING THREAT LANDSCAPE 5 (Oct. 2024), https://www.unodc.org/roseap/uploads/documents/Publications/2024/TOC_Convergence_Report_2024.pdf.

12 Targeting one ringleader personally, the United States Department of the Treasury's Office of Foreign Assets Control (OFAC) recently sanctioned Cambodian businessman Ly Yong Phat and his business entities for "serious human rights abuse related to the treatment of trafficked workers subjected to forced labor in online scam centers." U.S. Dep't Treasury, *Treasury Sanctions Cambodian Tycoon and Businesses Linked to Human Trafficking and*

the cash swindled from victims, transnational criminal networks have even developed their own financial services to launder "massive volumes of state-backed fiat and cryptocurrencies."[13]

Facing industrialized and professionalized scam operations, Americans need a more robust institutional and legal response to quell the outflow of assets and present a harder target.[14] This essay argues that the critical institutional custodians holding American assets must protect client assets more effectively. Although our observations apply to many financial services firms, we focus our analysis here on brokerage firms—the entities with custody of American securities holdings. By becoming more vigilant about scam and fraud risks, brokerage firms may reduce investor losses now pumping lifeblood into transnational criminal organizations.

Brokerage firms sit in a unique position and enjoy fraud-fighting advantages. Brokerages understand market realities better than their clients. They receive constant updates about current scams and frauds from regulators and victimized clients. This broader view of market developments positions them to identify potential scams and alert their clients, other industry members, and the government to criminal activity.[15]

Brokerage firms also play a critical custodial role for America's securities and retirement savings—meaning that many investment frauds will necessarily need a brokerage firm to relinquish custody and transfer client assets elsewhere. Brokerage firms act as the gatekeepers, determining who gains access to investor funds and under what conditions, making their supervisory responsibilities critical to maintaining the integrity of the financial markets. Brokerage firms also maintain sophisticated compliance tools and systems that generate alerts and flag suspicious or potentially fraudulent activity. Thus, brokerage firm vigilance and responsiveness to

Forced Labor in Furtherance of Cyber and Virtual Currency Scams (Sept. 12, 2024), https://home.treasury.gov/news/press-releases/jy2576.

[13] UNODC, CASINOS, MONEY LAUNDERING, UNDERGROUND BANKING, AND TRANSNATIONAL ORGANIZED CRIME IN EAST AND SOUTHEAST ASIA: A HIDDEN AND ACCELERATING THREAT i (Jan. 2024), https://www.unodc.org/roseap/uploads/documents/Publications/2024/Casino_Underground_Banking_Report_2024.pdf.

[14] *See* Dan Shaw, *Schwab, crypto, alleged fraud and an elderly couple's $18.5M loss* (Oct. 24, 2024), https://www.financial-planning.com/news/suit-schwab-did-nothing-to-stop-18-5m-crypto-scam (quoting Hugh Berkson explaining that the "tools the scammers use are continuing to improve with terrifying consequences").

[15] *See* e.g., U.S. Treasury Financial Crimes Enforcement Network, Advisory on Elder Abuse, FinCEN Advisory, FIN-2022-A002 (June 15, 2022), available at https://www.fincen.gov/sites/default/files/advisory/2022-06-15/FinCEN%20Advisory%20Elder%20Financial%20Exploitation%20FINAL%20508.pdf (detailing red flags for fraud).

react to red flags and suspicious transactions may determine whether a scam succeeds or fails.

Brokerage firms also have existing transaction and account monitoring compliance systems in place. These tools are already used to track identification information like what IP address is contacting an account and what device and operating system is being used to connect to an account. Firms also monitor for suspicious transactions that are outside of the character and listed investment objectives for an account on an automated basis. Thus, since the compliance apparatus is already in place to monitor for suspicious contacts and transactions, it would not require a Herculean effort to use that same apparatus more effectively to protect investors from these sorts of frauds.

Consider another recent arbitration involving TD Ameritrade. Willard Holgate, a Texas octogenarian, lost $460,000 after scammers convinced him that he needed to wire his retirement savings overseas.[16] An arbitration panel found TD Ameritrade liable for $97,200 in compensatory damages after his counsel argued that red flags showed up on Holgate's conversations with TD Ameritrade that the brokerage firm should have responded to.[17]

Even though Holgate recovered a substantial amount, his victory does not mean that future victims will be able to effectively use his case or Kessler's to hold financial intermediaries accountable.[18] Although TD Ameritrade was found liable, the arbitration award does not necessarily create precedent or provide controlling law for future cases.[19] Functionally, industry-wide arbitration means that newer problems—such as how financial services firms should respond to the rise of industrial-scale scam operations remains insulated from meaningful judicial review. Courts simply lack opportunities to update existing precedent to address new problems.[20]

This precedent gap exists in large part because FINRA, the industry self-regulator for brokerage firms, provides an arbitration forum for claims against its members.[21] As nearly all FINRA members include pre-dispute arbitration clauses in their account opening documents, courts only rarely

---

[16] Dan Shaw, *TD Ameritrade to pay $100K for not stopping elder fraud* (Oct. 21, 2024), https://www.financial-planning.com/news/elder-fraud-case-lands-tdameritrade-100k-fine.
[17] *Id.*
[18] *See* Benjamin P. Edwards, *Arbitration's Dark Shadow*, 18 NEV. L.J. 427, 434 (2018) (explaining that arbitration awards do not create precedent and how industry-wide arbitration stalls the development of common law).
[19] *Id.*
[20] *Id.*
[21] *Id.*

opine on substantive law. This absence of meaningful judicial involvement means that industry regulators must become more proactive.

Considering this dynamic, this Essay argues that regulators and policymakers must take more aggressive action to clarify brokerage firms' obligations and increase the likelihood that key intermediaries will respond to suspicious activities. This essay opens in Part II and reviews the current scam epidemic. Part III reviews brokerage authority and obligation to protect clients from exploitation. Part IV discusses possible regulatory responses to improve brokerage firm responsiveness.

II. THE TRANSNATIONAL SCAM LANDSCAPE

The volume of scams targeting Americans has risen dramatically in recent years. This part highlights the rising problem and explains how fraud and scam revenue now drives human trafficking, money laundering, and other crimes. As explained below, many scams and frauds operate with some link to cryptocurrency transactions.

A. The Rising Scam and Fraud Problem

Fraud and scam losses have risen dramatically in recent years. The most recent figures from the FTC reveal that Americans reported losses of more than $12.5 billion to fraud in 2024.[22] *This is a 25% increase over the prior year.*[23]

Other federal agencies also report substantial increases. The Federal Bureau of Investigation's Internet Crime Complaint Center released its own figures for 2024, finding that there were $16.6 billion in losses over the year—a new record.[24] Losses have escalated dramatically over time with Americans suffering approximately $4 billion in losses in 2020, $6 billion in 2021, $10 billion in 2022, and $12 billion in 2023.[25]

An incorrect perception often exists that scams only impact Americans who are incapacitated or vulnerable, such as elderly individuals

---

[22] FTC, *New FTC Data Show a Big Jump in Reported Losses to Fraud to $12.5 Billion in 2024*, 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 (last visited May 28, 2025).
[23] *Id.*
[24] FBI, Internet Crime Report 2024, 3 https://www.ic3.gov/AnnualReport/Reports/2024_IC3Report.pdf (last visited May 28, 2025).
[25] *Id.* at 7.

with dementia or Alzheimer's.[26] Data suggests, however, that scams impact a wide swath of the American public. A recent report finds that more than 40% of American adults (over 110 million people) "have had money stolen to due to fraud or sensitive information obtained and used fraudulently."[27] Another recent survey suggests over one-third of U.S. Adults have faced a financial scam or fraud in the past year.[28] Simply put, scams can affect anyone and in certain circumstances younger victims may be even more prone to victimization.[29]

Losses from scams and frauds are not evenly distributed across the population. Persons over the age of 60 lost substantially more than other demographic groups.[30] Older Americans likely suffer greater losses because they have accumulated more wealth that can be stolen and because they are more likely to experience cognitive decline, making them more vulnerable to scams and frauds.

Quantifying the true scope and scale of the fraud and scam problem remains extraordinarily difficult. Although the FTC has found that investment scams cost Americans over $4 billion annually, that figure likely understates the harm.[31] The AARP, recently found that American adults over the age of sixty likely lose over $28 billion annually to elder financial exploitation.[32] Of that figure, over $8 billion was stolen by strangers.[33] Notably, the AARP figures do not include any estimates for losses suffered by persons under the age of sixty.

Successful scams require assets and funds to move from the victim's control and to the scammer. In many cases, this means that the scam will

---

[26] Christina Ianzito, 4 in 10 Americans Have Lost Money to Fraud, AARP Survey Finds , AARP, April 21, 2025, https://www.aarp.org/money/scams-fraud/fraud-awareness-survey-2025.html (last visited June 17, 2025).
[27] *Id.*
[28] Katie Kelton, *Survey: More than 1 in 3 Americans have faced a financial scam or fraud in the past year*, BANKRATE, Mar. 3, 2025, https://www.bankrate.com/credit-cards/news/financial-fraud-survey/ (last visited June 17, 2025).
[29] FTC, Who experiences scams? A story for all ages, Dec. 8, 2022, https://www.ftc.gov/news-events/data-visualizations/data-spotlight/2022/12/who-experiences-scams-story-all-ages (last visited June 17, 2025).
[30] *Id.* at 8.
[31] FTC, As Nationwide Fraud Losses Top $10 Billion in 2023, FTC Steps Up Efforts to Protect the Public (Feb. 9, 2024), https://www.ftc.gov/news-events/news/press-releases/2024/02/nationwide-fraud-losses-top-10-billion-2023-ftc-steps-efforts-protect-public.
[32] AARP, *AARP Report Finds $28.3 Billion a Year is Stolen from U.S. Adults Over 60* (June 15, 2023), https://press.aarp.org/2023-06-15-AARP-Report-Finds-28-Billion-a-Year-is-Stolen-from-US-Adults-Over-60 .
[33] *Id.*

require the victim to purchase cryptocurrencies or initiate some wire transfer.[34] Cryptocurrency transactions occur outside the traditional banking system and offer scammers a preferred means to exfiltrate assets efficiently.[35]

Cryptocurrency transactions now play a central role in scams and frauds. The FBI found that in 2024 $9.3 billion in losses involved cryptocurrencies.[36] This marks a 66% increase from the prior year.[37] Now, cryptocurrencies provide a common nexus for many different types of scams including investment fraud, romance scams, government impersonation scams and others.[38]

B. Many Scammers Are Victims Themselves

The growing and extraordinarily profitable tide of scam operations requires a substantial labor force. The United Nations Office on Drugs and Crime has issued reports detailing how transnational criminal syndicates now trick victims into "online job compounds" where they may be forced to engage in criminal acts, namely scams.[39] These organized criminal groups meet labor "needs by trafficking young, educated, media savvy . . . people from Asia (and beyond) into the various scam compounds . . . where they could be confined and made to carry out the scams."[40] These criminal groups specifically target "university graduates who are fluent in multiple languages . . ., have skills in Information Technology (IT), . . . social media, and some working knowledge of cryptocurrency."[41] To convince victims to travel to a place where they will be under a criminal group's physical control, these

[34] FBI, *supra* note 24, at 17.
[35] *See* Selam Gebrekidan & Joy Dong, *The Scammer's Manual: How to Launder Money and Get Away With It,* N.Y. TIMES, Mar. 23, 2025, at A1, https://www.nytimes.com/2025/03/23/world/asia/cambodia-money-laundering-huione.html (last visited May 28, 2025) (detailing how money laundering operations use cryptocurrencies).
[36] FBI, *supra* note 24, at 35.
[37] *Id.*
[38] *Id.* at 38.
[39] UNITED NATIONS OFFICE ON DRUGS AND CRIME, INFLECTION POINT: GLOBAL IMPLICATIONS OF SCAM CENTRES, UNDERGROUND BANKING AND ILLICIT ONLINE MARKETPLACES IN SOUTHEAST ASIA 32 (April 2025), https://www.unodc.org/roseap/uploads/documents/Publications/2025/Inflection_Point_2025.pdf (last visited May 28, 2025).
[40] UNITED NATIONS OFFICE ON DRUGS AND CRIME, CASINOS, CYBER FRAUD, AND TRAFFICKING IN PERSONS FOR FORCED CRIMINALITY IN SOUTHEAST ASIA 7 (September 2023), https://www.unodc.org/roseap/uploads/documents/Publications/2023/TiP_for_FC_Policy_Report.pdf (last visited May 28, 2025).
[41] *Id.* at 8.

criminal networks often conduct "up to four seemingly legitimate online interviews to secure the 'job.'"[42]

The United Nations explains that trafficking victims endure similar ordeals. On arriving at a casino compound under the false belief that they will begin a new and legitimate career, they learn that they "will not be working in the role that they were promised but, rather, that they are to conduct criminal activities, particularly online scams and fraud."[43] Once in the compound, victims are generally "confined to the scam compound" and made to work.[44] Victims that that do not meet their "sales quotas" by scamming enough people often experience violence, frequently electrocutions or beatings.[45]

Low performance may result in other control methods. Victims may be "sold" to a different scam compound and told that they must pay off "debt" incurred by their purchase.[46] These "artificial debts act as a means of psychological control of victims, in which victims retain hope that they can repay the debt and eventually be freed."[47] Women who fail to meet "sales quotas" are "threatened with being sold to brothels and other locations for sexual exploitation."[48]

Southeast Asia now hosts a substantial number of scam compounds in Cambodia, Myanmar, Lao PDR, the Philippines, Malaysia, and elsewhere[49] At present, these scam compounds operate at scale with dormitory bedrooms, "scammer training manuals," and enforcers "hired to control trafficking victims."[50] The operations earn criminal groups "billions of US dollars, with profits rivaling the GDP of some countries in the region."[51] Even a relatively small group of controlled victims can produce enormous profits. A group of ten Turkish victims generated $400,000 a week for their captors.[52]

Successful scams lead to more scams and human trafficking. The criminal groups use funds secured from their victims to expand their

---

[42] *Id.* at 12.
[43] *Id.* at 8.
[44] *Id.* at 13.
[45] *Id.* at 14.
[46] *Id.*
[47] *Id.*
[48] *Id.*
[49] *Id.* at 15-19 (detailing compound locations).
[50] *Id.* at 7.
[51] *Id.* at 20.
[52] *Id.*

operations, undermine the rule of law, and evade enforcement.[53] Recent reports indicate that the scam compounds have grown so dramatically that the entire region now faces an inflection point, "leaving criminal groups free to pick, choose, and move jurisdictions, operations, and value as needed, with the resulting situation rapidly outpacing the capacity of governments to contain it."[54]

At present, the United Nations Office on Drugs and Crime recommends that nations strengthen their regulatory frameworks to prevent losses and effectively enforce their laws.[55] It specifically recommends supervisory reforms "for monitoring high-risk financial service providers, particularly those operating through digital platforms."[56] In the United States, this means that brokerage firms and other financial service providers must become more effective at stopping asset losses from scams and frauds.

III. EXISTING ANTI-EXPLOITATION RESPONSIBILITY AND AUTHORITY

Today, brokerage firms and their registered representatives stand as front-line guardians for American savings. Exfiltrating substantial client assets from brokerage accounts requires brokerage firms to affirmatively release client assets. Their employees generally maintain personal relationships and regular contact with account holders, leaving them well-positioned to know when a clients' behavior appears odd. Because of their keystone position, sophistication, and market insights, brokerage firms enjoy unique opportunities to prevent frauds. A report co-sponsored from the FINRA Foundation, a non-profit affiliated with FINRA, acknowledged that for preventing scam victimization "[s]ome of the most effective intervention points could be at the locations where the financial transactions occur."[57] This part briefly reviews brokerage obligations to understand their client's situation, obtain trusted contact information, and authority to act when a client is over the age of 65 or otherwise appears "unable to protect their own interests."[58]

---

[53] *Id.*
[54] UNDOC, INFLECTION POINT, *supra* note 39, at 3-4.
[55] *Id.* at 12.
[56] *Id.*
[57] James Langton, *Why protecting repeat fraud victims is no easy task*, INVESTMENT EXECUTIVE, Mar. 4, 2021, https://www.investmentexecutive.com/news/from-the-regulators/why-protecting-repeat-fraud-victims-is-no-easy-task-research/ (last visited June 18, 2025)
[58] FINRA Rule 2165(a)(1).

A. Extensive Brokerage Visibility into Client Situations

Brokerage firms providing personalized investment advice to clients have existing obligations to develop a thorough understanding of their clients' financial situation. The Financial Industry Regulatory Authority (FINRA), serves as the primary regulator for brokerage firms.[59] Its rules impose an ongoing obligation on brokers to know their customers.[60] It requires brokers to use reasonable diligence to understand the "essential facts concerning every customer and concerning the authority of each person acting on behalf of such customer."[61] Functionally, this means that brokers must know information essential to "effectively service the customer's account."[62]

Although brokerage firm personnel will not know everything about their clients, providing personalized financial advice requires them to have a solid understanding of a client's situation. This places them in a unique position to identify and respond to red flags or signs of potential fraud such as when a client's behavior changes in a concerning way.

B. Trusted Contact Information

In addition to having an understanding about the customer's essential situation, FINRA rules mandate that brokerage firms use reasonable diligence to identify trusted contacts for their clients. This means that they must collect the "name of and contact information for a trusted contact person age 18 or older who may be contacted about the customer's account."[63] A FINRA Regulatory Notice explains that brokerage firms must notify customers that the brokerage may use the information to "contact a trusted contact person to address possible financial exploitation of the customer."[64]

FINRA instituted the trusted contact requirement in 2018 as part of an effort to limit the financial exploitation of senior investors.[65] A FINRA Regulatory Notice explains that the trusted contact is "intended to be a

---

[59] *See* Benjamin P. Edwards, *Fiduciary Duty and Investment Advice: Will A Uniform Fiduciary Duty Make A Material Difference?*, 14 J. Bus. & Sec. L. 105, 111 (2014) (explaining that FINRA is the primary regulator for brokerage firms).

[60] FINRA Rule 2090. Know Your Customer, https://www.finra.org/rules-guidance/rulebooks/finra-rules/2090.

[61] *Id.*

[62] *Id.*

[63] FINRA Rule 4512(a)(1)(f). Customer Account Information, https://www.finra.org/rules-guidance/rulebooks/finra-rules/4512.

[64] FINRA Regulatory Notice 17-11 Financial Exploitation of Seniors (Mar. 2017), https://www.finra.org/sites/default/files/Regulatory-Notice-17-11.pdf.

[65] *Id.*

resource for the member in administering the customer's account, protecting assets and responding to possible financial exploitation."[66]

C. Explicit Authority to Freeze Transactions

In 2016, the North American Securities Administrators Association (NASAA) adopted the Senior Model Act (the "Model Act").[67] It has since been broadly adopted by the states.[68] The Model Act aims to address and prevent the financial exploitation of seniors by requiring brokerage employees to report financial exploitation and notify their state securities regulators.[69] The Model Act also creates a safe harbor for brokerage firms to delay disbursements and freeze transactions for fifteen days or longer to resolve issues.[70]

Yet the Model Act does not cover all individuals. Its protective terms apply to persons "age 65 or older and those adults who would be subject to the provisions of a state's adult protective services statute."[71] Functionally, this means that high-functioning persons over the age of 65 enjoy clearer protection than even lower-functioning persons under the age of 65.

FINRA amended its rules in 2018 to accommodate widespread Model Act adoption and create a consistent baseline across the country by adopting Rule 2165.[72] It takes a similar approach to the Model Act and applies to natural persons over the age of 65 and any "natural person age 18 and older who the member reasonably believes has a mental or physical impairment that renders the individual unable to protect his or her own interests."[73] Supplementary guidance explains that brokerages do not need to conduct a medical assessment, and may simply rely on "the facts and circumstances observed in the member's business relationship with the natural person" when deciding if they are unable to protect their own interests.[74]

At present, FINRA guidance does not clearly sketch the boundaries of a "mental or physical impairment that renders the individual unable to

---

[66] *Id.*
[67] *See* North American Securities Administrators Association, NASAA Senior Model Act, https://www.nasaa.org/industry-resources/senior-issues/model-act-to-protect-vulnerable-adults-from-financial-exploitation/ (last visited May 26, 2025).
[68] *Id.*
[69] *Id.*
[70] *Id.*
[71] *Id.*
[72] FINRA Rule 2165, https://www.finra.org/rules-guidance/rulebooks/finra-rules/2165 (last visited May 28, 2025).
[73] *Id.* at (a)(1).
[74] *Id.* at Supplementary Material .03.

protect their own interests."[75] As FINRA members channel customer claims into FINRA arbitration, courts have not been able to construe the provision. This vagueness leaves brokerage firms and investors fumbling.

Many different impairments may make an individual unable to protect their own interests. Cognitive decline may be difficult to identify and assess and it may fluctuate over time.[76] Persons may bristle at the mere suggestion that they may be experiencing cognitive decline.[77] A person seeking to withdraw funds at the request of a scammer likely lacks a meaningful ability to protect their own interests. Scams succeed because scammers exploit some vulnerability to cause a victim to believe a false reality.

To encourage its Members to err on the side of freezing suspicious transactions, FINRA's guidance makes clear that it also provides its Member firms with a safe harbor from other FINRA rules to allow them to stop transactions they would otherwise facilitate and initiate an "internal review of the facts and circumstances" to determine how to proceed.[78] Although this safe harbor should create a bias toward action, the industry has failed to meet the escalating scam threat.

D. Mandatory Training and Supervision Around Exploitation

FINRA's rules do more than merely authorize firms to act, they affirmatively require firms to train their personnel and escalate in response to problems. FINRA Rule 2165 requires its member firms to "establish and maintain written supervisory procedures . . . including, but not limited to, procedures related to the identification, escalation and reporting of matters related to the financial exploitation of Specified Adults."[79]

Although brokerage firm policies and procedures are not ordinarily publicly available documents, these policies and procedures must do more than merely pay lip service to compliance. In guidance on effective practices, FINRA highlighted escalation processes, training programs and "ongoing, regular reminders that included spotting and responding to red flags of financial exploitation, diminished capacity or cognitive impairment in their clients."[80]

---

[75] *Id.* at (a)(1)(B).
[76] *See* Sharona Hoffman, *Cognitive Decline and the Workplace*, 57 WAKE FOREST L. REV. 115, 120 (2022) (discussing cognitive decline).
[77] *Id.*
[78] FINRA Rule 2165 (b)(1)(C).
[79] FINRA Rule 2165(c)(1).
[80] FINRA, Protecting Senior Investors 2015–2020, 14, https://www.finra.org/sites/default/files/2020-04/protecting-senior-investors-2015-2020.pdf.

In some instances, these rules have protected seniors from exploitation. A FINRA review highlights a series of victories, including temporary holds that stopped thefts from lottery scams, romance scams, and a scam where an investor sought to withdraw funds to purportedly aid the United States Central Intelligence Agency.[81]

Although not in the senior exploitation context, FINRA has also sought discipline when brokerage firms fail to implement effective policies and procedures and allow scams to dissipate client assets. In 2020, FINRA censured and fined Lincoln Investment for failures around supervising funds transmittals that allowed an imposter to steal customer funds.[82] As part of the settlement, Lincoln Investment adopted continuing training on "social engineering red flags and email-related scams."[83]

E. Escalating in Response to Red Flags

Effective programs will train brokerage personnel to react to red flags indicating possible scams of financial exploitation. Acting together, the U.S. Securities and Exchange Commission, FINRA and NASAA, have released training materials detailing some red flags that should trigger escalation for scams and frauds.[84] Those include: (1) "Uncharacteristic and repeated cash withdrawals or wire transfers;" (2) "Appearing with new and unknown associates, friends, or relatives; (3) Uncharacteristic nervousness or anxiety when visiting the office or conducting telephonic transactions; (4) Lacking knowledge about his, her, or their financial status; (5) Having difficulty speaking directly with the client or customer without interference by others; (6) Unexplained or unusual excitement about an unexplained or 'too good to be true' windfall; (7) "[R]eluctance to discuss details;" (8) Sudden changes to financial documents such as powers of attorney, account beneficiaries, wills, or trusts; (9) Large, atypical withdrawals or closing of accounts without regard to penalties; and (10) Frequent password reset requests or new online account access requests.[85]

The regulators' training materials explain that once red flags emerge, brokerage personnel should "immediately escalate" within the firm and

---

[81] *Id.*
[82] FINANCIAL INDUSTRY REGULATORY AUTHORITYLETTER OF ACCEPTANCE, WAIVER AND CONSENT, NO. 2018056408401, Dec. 10, 2020.
[83] *Id.* at 8.
[84] SEC, NASAA, & FINRA, Addressing and Reporting Financial Exploitation of Senior and Vulnerable Adult Investors (June 2023), https://www.finra.org/sites/default/files/2023-05/NASAA-SEC-FINRA-Training-Senior-Investor-Protection-June2023.pdf (last visited May 28, 2025).
[85] *Id.* at 13.

involve "supervision, compliance, or legal as soon as you see red flags."[86] and launch an internal investigation if appropriate.[87] It also advises that the brokerage discuss potential adverse consequences with the investor and consider notifying a trusted contact person.[88]

From a scam intervention perspective, identifying and escalating in response to red flags remains critical. Brokerage personnel will generally not be aware of the full situation or the alternative reality the scammer has created for the client. Operating at the scammer's direction, the client will likely provide the brokerage with a pretextual rationale for withdrawing or transferring assets away. As these stories will generally be inconsistent with the client's established preferences and generate substantial problems, the stories rarely make sense in context.

Consider Marjorie Kessler's situation again.[89] She made repeated requests for funds while making misstatements about the "purpose of the transfers."[90] Even if the initial request might have appeared plausible, the subsequent requests shortly after the first may have appeared more suspect. Although FINRA arbitration awards do not explain a panel's reasoning, counsel for Ms. Kessler took the view that the panel gave Morgan Stanley the benefit of the doubt on the first transaction, but could not on the subsequent requests.[91]

F. Anti-Money Laundering

In addition to all of the foregoing, brokerage firms also operate under an obligation to report and prevent money laundering.[92] This requires firms to create and implement policies and procedures designed to comply with the Bank Secrecy Act.[93] In many instances, a person acting at the behest of a scammer will behave in ways that also generate red flags for potential money laundering. For example, FINRA instructs that when a "customer appears to be acting as an agent for an undisclosed principal, but is reluctant to provide information" as a red flag for possible money laundering.[94] Other red flags include: (1) "transactions that lack business sense or an apparent investment

---

[86] *Id.* at 17.
[87] *Id.*
[88] *Id.*
[89] *See* Kelly, *supra* note 3.
[90] *Id.*
[91] *Id.*
[92] FINRA Rule 3310.
[93] *Id.*
[94] FINRA, ANTI-MONEY LAUNDERING (AML) PROGRAM, FINRA PROVIDES GUIDANCE TO FIRMS REGARDING SUSPICIOUS ACTIVITY MONITORING AND REPORTING OBLIGATIONS, Notice to Members 19-18, at 4, https://www.finra.org/sites/default/files/2019-05/Regulatory-Notice-19-18.pdf (last visited May 30, 2025).

strategy, or are inconsistent with the customer's stated business strategy;" (2) "transactions that show a sudden change inconsistent with normal activities of the customer;" and (3) when a "customer does not exhibit a concern with the cost of the transaction or fees (e.g., surrender fees, or higher than necessary commissions)."[95]

These identified red flags for money laundering already require brokerage firms to escalate and respond. Firms that rise to the challenge may discover their client being exploited by some scam while time remains to prevent substantial losses.

IV. Policy Responses

As the United Nations has recommended, nations must strengthen their regulatory frameworks to prevent losses and combat the rise of transnational criminal organization.[96] In the domestic context, American brokerages must mount more effective responses in the current environment. The trafficking victims compelled to scam Americans today remain highly motivated to avoid beatings, electrocution, or sexual exploitation. In contrast, American brokerage and other financial services employees often fail to alert to obvious red flags for scams or exploitation. This part offers a range of responses to reduce the scale and severity of American losses. Critically, stopping these scams also reduces the incentive to conduct human trafficking and compel forced criminality.

A. FINRA Enforcement Priorities

Each year FINRA releases a report on its regulatory oversight. In January of 2025, FINRA identified a series of findings around senior investors and their trusted contact persons.[97] It identified brokerage firm failures to obtain trusted contact information, failures to conduct any documented training for personnel around these issues, and failures to conduct any documented internal reviews.[98] It recommended, among other things, additional training "for both front office and back office staff, on **common financial and investment scams** and the warning signs of potential (1) fraud or exploitation perpetrated on the customer or (2) diminished capacity."[99]

---

[95] *Id.* at 10-11.
[96] UNDOC, Inflection Point, *supra* note 39, at 3-4.
[97] FINRA, 2025 FINRA Annual Regulatory Oversight Report 28 (January 2025), https://www.finra.org/sites/default/files/2025-01/2025-annual-regulatory-oversight-report.pdf (last visited May 30, 2025).
[98] *Id.*
[99] *Id.* at 29 (emphasis in original).

Despite this stated focus on these issues, we have not been able to identify a single FINRA enforcement action against a member firm related to its failure to comply with FINRA Rule 2165—the provision governing Financial Exploitation of Specified Adults.[100] Similarly, FINRA does not appear to have taken any actions against a Member firm for failing to make reasonable efforts to collect and maintain trusted contact information for customers.[101]

FINRA's enforcement actions send a signal to brokerage firms about their responsibilities and potential exposure for failures in this context. Devoting resources to enforcement actions on these issues would send a strong signal that brokerage firms must become more diligent and vigilant around these issues.

B. State Enforcement Actions and Inquiries

Although FINRA serves as the primary regulator for brokerage firms, state securities regulators also possess jurisdiction over brokerage firms and license their operations. Bringing enforcement actions against brokerages for failures to prevent the dissipation of client assets under anti-fraud powers may present unique challenges because brokerage personnel generally have no intention to facilitate fraud. Rather, their laxity allows highly motivated scammers to exploit Americans.

In this context, state regulators should consider more aggressive action. Brokerage firms that present themselves to the investing public as diligent stewards while failing to take action when it matters should face some enforcement action or inquiry. Ultimately, the goal of enforcement actions must be to change behavior across the industry and make brokerages respond more effectively to red flags.

C. Regulatory Guidance

Both FINRA, the SEC, and state regulators may drive behavioral change by releasing guidance stressing the need for brokerages to respond to the current crisis. As customer disputes will almost always be resolved in arbitration, regulatory guidance on firm responsibilities plays an outsize role in shaping behavior and liability.

---

[100] FINRA maintains a searchable database for disciplinary actions. Although our review found the number 2165, we could not locate a single instance of FIRNA bringing an enforcement action against a firm for failing to comply with Rule 2165. *See* FINRA, FINRA Disciplinary Actions Online, https://www.finra.org/rules-guidance/oversight-enforcement/finra-disciplinary-actions-online (last visited May 30, 2025).

[101] *Id.*

Releasing public guidance on firm obligations serves two purposes. First, it clearly tells brokerage firms what they should be doing and what their policies and procedures should, at minimum, include. Second, these documents provide key evidence in arbitration hearings about the relevant standard of care for brokerages managing American securities holdings.

For example, regulators should release guidance making clear that individuals under the influence of a scammer have a "mental impairment" making them unable to protect their own interests.[102] At present, brokerage firms may attempt to limit their responsibility only to persons with advanced and readily apparent dementia, allowing them to argue they should escape liability for facilitating transactions even when their personnel believe the investor may be the victim of a scam.

D. Legislative or Rulemaking Action

Legislative action or additional rulemaking may also be used to drive change. While brokerage firms have substantial obligations at present, much of the existing regulatory structure focuses on a customer's age with persons over the age of 65 receiving more protection than persons under the age of 65. Relatively modest revisions would clarify obligations and change brokerage firm behavior to better protect American investors. Rules that clearly require brokerage firms to act in response to threats and prohibit them from processing transactions when they know or should know that such transactions are fraudulent could provide brokerage firms the incentive to prioritize fraud prevention.

V. CONCLUSION

Ultimately, American investors are now under attack from transnational criminal groups. Failures to protect investor assets provide resources to support widespread criminality, human trafficking, and a host of other problems. Brokerage firms serve as key institutional custodians and must become more effective at preventing the dissipation of investor assets.

[102] *See* FINRA Rule 2165.