2022

The Obligations and Regulatory Challenges of Online Broker-Dealers and Trading Platforms

Christine Lazaro
St. John's University School of Law

Teresa J. Verges

THE OBLIGATIONS AND REGULATORY CHALLENGES OF ONLINE BROKER-DEALERS AND TRADING PLATFORMS

Christine Lazaro and Teresa J. Verges[1]

Investing has been evolving for decades. On "Mayday" in 1975, the SEC abolished fixed commissions, changing the face of the brokerage industry.[2] A few months later, Charles Schwab opened its first offices, and discount brokerages were born.[3] By the mid-1980s, there were over 600 discount brokers operating.[4] By 1990, discount brokerage firms captured just under than 10% of the market, although Charles Schwab captured 40% of the discount brokerage market.[5] Throughout the 1990s, new firms entered the market, including E*Trade and AmeriTrade.[6] Online trading became more prevalent;

---

1. Christine Lazaro is a Professor of Clinical Legal Education and the Director of the Securities Arbitration Clinic at St. John's University School of Law. Teresa J. Verges is Associate Professor of Clinical Legal Education and Director of the Investor Rights Clinic at the University of Miami School of Law. The authors wish to thank Nicolas T. Geraci ('22 University of Miami School of Law) and Aron Kaplan ('23, St. John's University School of Law) for their research for and contributions to this article.

2. *See* Jason Zweig, *Lessons of May Day 1975 Ring True Today: The Intelligent Investor*, WALL ST. J. (Apr. 30, 2015), https://www.wsj.com/articles/lessons-of-may-day-1975-ring-true-today-the-intelligent-investor-1430450405.

3. *See id.*

4. *See* Stephen Mihm, *The Death of Brokerage Fees Was 50 Years in the Making*, BLOOMBERGOPINION (Jan. 3, 2020), https://www.bloombergquint.com/view/how-nyse-went-from-quasi-cartel-to-zero-fee-stock-trading.

5. *See* Richard D. Hylton, *All About: Discount Brokers; Now Fewer Firms Are Chasing Small Investors Discount Brokers*, N.Y. TIMES (June 17, 1990), https://www.nytimes.com/1990/06/17/business/all-about-discount-brokers-now-fewer-firms-are-chasing-small-investors-discount.html.

6. *See* Bob Pisani, *Man Vs. Machine: How Stock Trading Got So Complex*, CNBC (Sept. 13, 2010), https://www.cnbc.com/2010/09/13/man-vs-machine-how-stock-trading-got-so-complex.html.

by 1999 25% of all trades occurred online.[7] The term "day trader" entered our vocabulary.[8] Commissions declined, until they reached zero.[9]

Investors now have more choices than ever when deciding how and with whom to invest. In addition to the large full service brokerage firms, there are independent broker-dealers, discount brokers, and online platforms and apps. Across the models, the level of service varies, as does the minimum amount needed to open an account and the ease with which an account can be opened.

Both new and experienced investors responded to these new trading models and reduced barriers to entry. 2020 witnessed a surge in new retail brokerage accounts opened on online platforms.[10] One research analyst at JMP Securities estimates that more than 10 million new online brokerage accounts were opened in 2020.[11] According to a joint study conducted by the FINRA Investor Education Foundation and NORC at the University of Chicago, 66% of survey respondents who opened a new account in 2020 were new investors, who had not previously owned a taxable investment account.[12] The FINRA/NORC study found that the new investors were younger, had lower incomes, and were more racially diverse, compared to the other groups measured, specifically experienced investors that also opened online brokerage accounts in 2020, or "holdover" account owners who owned a brokerage account but did not open a new account in 2020.[13] The FINRA/NORC study attributed the surge in new retail investors to the

---

7. *See* Arthur Levitt, Chair, Sec. Exch. Comm'n, Remarks to the National Press Club, Plain Talk About On-Line Investing (May 4, 1999), http://3197d6d14b5f19f2f440-5e13d29c4c016cf96cbbfd197c579b45.r81.cf1.rackcdn.com/collection/papers/1990/1999_0429_LevittDraftT.pdf.

8. *See* Pisani, *supra* note 6.

9. *See* Mihm, *supra* note 4.

10. *See* FINRA INVESTOR EDUCATION FOUNDATION AND NORC REPORT, INVESTING 2020: NEW ACCOUNTS AND THE PEOPLE WHO OPENED THEM, at 1 (Feb. 2021) (hereinafter, "FINRA/NORC Study"), https://www.finrafoundation.org/sites/finrafoundation/files/investing-2020-new-accounts-and-the-people-who-opened-them_1_0.pdf.

11. *See* Susan Tompor, *Why New Investors Bought Stock During the COVID-19 Pandemic*, DET. FREE PRESS (Feb. 5, 2021), https://www.freep.com/story/money/personal-finance/susan-tompor/2021/02/05/how-invest-stock-market/4360276001/.

12. *See* FINRA/NORC Study, *supra* note 11 at 2.

13. *See id.*

reduction in barriers to entry for retail investing, including no-minimum and low-minimum accounts and low or zero trading commissions.[14]

In addition to lowering the barriers to the markets, the online platforms have changed how investors interface with firms and the markets. They offer a number of different design features, commonly described as "gamification." These may include games when an investor opens an account; animations, including confetti when a milestone is reached; social networking tools; prizes or rewards for activity streaks; points, badges, and leaderboards; lists of popular stocks; free stocks for referring additional customers; and push notifications.[15]

However, regulators are concerned that many new investors, prompted by gamification, have engaged in high-risk trading strategies without an appreciation of the risks. Noting the surge in online trading, including options trading, in its 2021 exam report FINRA identified emerging "digital communications risks" associated with digital platforms and mobile apps that have interactive and "game-like" features, which could mislead investors about the risks of certain trading strategies, such as options trading.[16] FINRA also recently announced that it will seek public comment on gamification

---

14. *See id.* at 7-8. Another reason for the surge of new investors was the market volatility related to the COVID-19 pandemic, prompting new investors to take advantage of market dips. *See id.* at 1, 8. COVID-19 relief stimulus checks also contributed to the spike in online brokerage accounts opened by younger, new investors. *See* Jessica Menton, *Stimulus Check: Young Investors Use $1,400 COVID-19 Relief Payments to Join Stock Market Boom*, USA TODAY (Mar. 17, 2021), https://www.usatoday.com/story/money/2021/03/17/stimulus-check-young-investors-covid-relief-payments-stock-market/4693988001/.

15. *See* Robert W. Cook, President and Chief Executive Officer, FINRA, Statement Before the Financial Services Committee U.S. House of Representatives (May 6, 2021), https://www.finra.org/media-center/speeches-testimony/statement-financial-services-committee-us-house-representatives; *see also* Annie Massa and Tracy Alloway, *Robinhood's Role in the 'Gamification' of Investing*, BLOOMBERG WEALTH (Dec. 19, 2020), https://www.bloomberg.com/news/articles/2020-12-19/robinhood-s-role-in-the-gamification-of-investing-quicktake; Robinhood Financial, LLC, Docket No. E-2020-0047 (Mass. Off. of the Sec'y of the Commonwealth Sec. Div. Dec. 16, 2020), https://www.sec.state.ma.us/sct/current/sctrobinhood/MSD-Robinhood-Financial-LLC-Complaint-E-2020-0047.pdf.

16. *See* FINRA, 2021 REPORT ON FINRA'S EXAMINATION AND RISK MONITORING PROGRAM, at 22 (Feb. 2021) (hereinafter "2021 FINRA Report)", https://www.finra.org/rules-guidance/guidance/reports/2021-finras-examination-and-risk-monitoring-program.

practices utilized by these platforms, with a view towards potential new rulemaking.[17] SEC Chairman Gensler also expressed concern about the "gamification" of trading apps with features that "encourage investors to trade more," and indicated that these new models may require new rules.[18]

The concerns raised today about online trading echo concerns raised by then-SEC Chairman Arthur Levitt in 1999.[19] Chairman Levitt recognized that a firm's obligations do not change even though their platforms have changed:

> The laws regulating our markets are a product of the New Deal era. To me, their concepts are as immutable as the Constitution. They have weathered challenge after challenge, decade after decade, and are every bit as relevant and effective today as they were the day they were written. Companies offering their shares -- whether off a website or through a prospectus -- still have to disclose what they are selling and why. Brokers -- whether traditional or on-line -- still have the same obligations to their customers. And fraud -- whether perpetrated over the Internet, on the phone, or in-person -- is still fraud.[20]

Chairman Levitt raised concerns about the influx of new and inexperienced investors trading inconsistently with their goals and risk tolerances.[21] He recognized that as firms grow, their ability to provide effective customer service must keep pace.[22] He emphasized that firms have an obligation of best execution, regardless of how the trade has been placed.[23] He also raised concerns about the clarity of communications, and the accuracy of advertising.[24] These same concerns are echoed today by FINRA, the SEC and the state regulators.

---

17. *See* Sarah E. Aberg, Shane J. Killeen, *Game On: FINRA Hints at Upcoming Gamification Sweep*, The Nat'l L. Rev. (June 1, 2021), https://www.natlawreview.com/article/game-finra-hints-upcoming-gamification-sweep.

18. Gary Gensler, Chair, Sec. Exch. Comm'n, Statement Before the House Committee on Financial Services, at 2 (May 6, 2021), https://financialservices.house.gov/uploadedfiles/hhrg-117-ba00-wstate-genslerg-20210506.pdf.

19. *See* Levitt, *supra* note 7.

20. *Id.*

21. *See id.*

22. *See id.*

23. *See id.*

24. *See id.*

Regulators may ultimately promulgate new rules to address unique features of these platforms or amend existing rules to address new technology and communication practices. However, as noted by Chairman Levitt, brokerage firms offering self-directed trading services through digital platforms are still subject to existing rules and standards applicable all broker-dealers. This article reviews these primary regulatory obligations.

I. DUTIES OF BROKER-DEALERS OPERATING ONLINE PLATFORMS AND TRADING APPS TO RETAIL CUSTOMERS

Digital trading platforms and mobile apps provide investors with the ability to open a brokerage account (often within minutes) and trade securities from the comfort of their homes. The platforms provide investors with the ability to trade securities for their own accounts, without the guidance or investment recommendations of an individual broker or investment adviser representative. While online broker-dealer platforms may look different from traditional broker-dealers, however, these firms still have many of the same basic obligations to their customers.

As described below, all brokerage firms have ongoing obligations in connection with approving, opening, and maintaining customer accounts, conducting appropriate due diligence in connection with certain trading approvals, and complying with "know your customer" and anti-money laundering regulations. Firms are also prohibited from making false or misleading statements to investors and are subject to rules governing communications to retail investors, some of which may be deemed an "investment recommendation" and therefore, subject to the SEC's Regulation Best Interest or FINRA's suitability rule. All firms are also required to implement written policies and procedures to safeguard confidential customer information, funds and assets. The very technology used by digital trading platforms requires these firms to adopt strong cybersecurity protections for their customers.

A. Opening Customer Accounts, Due Diligence and Suitability Assessments

(i) Opening and Maintenance of Accounts and Customer Identification Program

Regardless of its business model, FINRA rules require all firms to obtain, maintain and regularly update specific customer information in connection with the opening and maintenance of a customer account.

FINRA Rule 2090 requires firms to "use reasonable diligence, in regard to the opening and maintenance of every account, to know (and retain) the essential facts concerning every customer and concerning the authority of each person acting on behalf of such customer."[25] The "essential facts" necessary to comply with the know your customer obligation are those required to: "(a) effectively service the customer's account, (b) act in accordance with any special handling instructions for the account, (c) understand the authority of each person acting on behalf of the customer, and (d) comply with applicable laws, regulations, and rules."[26]

The "know your customer" obligation arises at the beginning of the firm's relationship with the customer and extends throughout that relationship.[27] This makes sense, as customers' profiles, financial status, investment objectives, risk tolerance and other essential information can and will change over time. Moreover, the "know your customer" obligation does not depend on whether the broker or the firm has made a recommendation.

---

25. FINRA, Rule 2090, Know Your Customer (2012). Rule 2090 is modeled after former NYSE Rule 405(1); Rule 2090 and Rule 2111 became effective on October 7, 2011. FINRA REGUL. NOTICE 11-02, SEC APPROVES CONSOLIDATED FINRA RULES GOVERNING KNOW-YOUR-CUSTOMER AND SUITABILITY OBLIGATIONS (Oct. 7, 2011), https://www.finra.org/rules-guidance/notices/11-02.

26. FINRA, Rule 2090.01, Essential Facts (2012).

27. *See* FINRA, REGUL. NOTICE 11-02, *supra* note 25; *see also Obligations to Your Customers*, FINRA (explaining the first step in serving the customer is to "know your customer" and ensure that the facts obtained are accurate and updated), (available at https://www.finra.org/registration-exams-ce/manage-your-career/obligations-your-customers) (last accessed Mar. 19, 2022). Firms typically comply with the maintenance requirement by sending periodic letters or notices to customers (either annually or upon a change in the account) reflecting the information they have for the customer and shifting the burden on the customer to contact the firm if any information is correct.

At least some (but certainly not all) of the essential facts necessary to comply with the "know your customer" rule are captured through the firm's compliance with FINRA Rule 4512, which sets forth the minimum information firms must obtain, maintain and update for every customer account.[28] For retail investor customer accounts, the firm must obtain the customer's name, residential address, tax identification or social security number, the customer's occupation and name of employer, determine whether the customer is of legal age to open a brokerage account, and if the customer is a corporation, partnership or other legal entity, obtain the names of any persons authorized to trade in the account.[29] The firm should also identify for each account the associated person(s), if any, responsible for the account and the scope of each associated person's responsibility,[30] and the name of a "trusted contact" (unless the customer refused to provide one).[31]

Regardless of business model, a firm's supervisory system must include written procedures for the review and approval of customer accounts in compliance with the firm's regulatory obligations.[32] Rule 4512 requires that

---

28. *See* FINRA, Rule 4512, Customer Accout Information (2019).

29. *See* FINRA, Rule 4512(a) (2019). In 2001, the SEC amended its books and records regulations to add, among other things, a new customer account record rule requiring firms to obtain similar information, but expanded the required information to include investment objectives, annual income and net worth (excluding value of primary home). 17 C.F.R. § 240.17a-3(a)(17) (2021) (eff. May 2, 2003). The SEC adopted the new customer account rule in order to provide SRO and state regulators access to the types of records they would need to determine the firm's compliance with the suitability rule. SEC. EXCH. COMM'N, REL. NO. 34-44992, BOOKS AND RECORDS REQUIREMENTS FOR BROKER AND DEALERS UNDER THE SECURITIES EXCHANGE ACT OF 1934 (Nov. 2, 2001), https://www.sec.gov/rules/final/34-44992.htm. However, the SEC exempted brokers and dealers who are not required to comply with the suitability rule. 17 C.F.R. § 240.17a-3(a)(17)(i)(D) (2021) ("this section will not be applicable to an account for which, within the last 36 months, the member, broker or dealer has not been required to make a suitability determination under the federal securities laws or under the requirements of a self-regulatory organization of which it is a member").

30. *See* FINRA, Rule 4512(a)(C) (2019).

31. *See* FINRA, Rule 4512.06, Trusted Contact Person (2019). The firm must maintain and preserve this information for a period of at least six years after the date the information is obtained or updated. *See* FINRA, Rule 4512.01, Customer Account Retention Periods (2019).

32. Under FINRA Rule 3110, Supervision, a firm's supervisory system must include written procedures to supervise the types of business in which a firm engages and its

the firm maintain a record of the signature of the supervisory principal "denoting that the account has been accepted in accordance with the member's policies and procedures for acceptance of accounts."[33]

The account approval and maintenance processes are increasingly automated, especially in the context of self-directed broker trading platforms. Retail investors, particularly younger and new investors, more frequently choose to invest through self-directed discount trading platforms and apps.[34] Investors can complete an application online or through an app, directly providing their customer information to the trading platform, and obtain trading approval in minutes.[35]

The ease with which new customer accounts can be opened and approved through automated processes, however, underscores the importance of firms developing and implementing a written Customer Identification Program in compliance with the Bank Secrecy Act ("BSA").[36] The BSA requires firms to monitor for, detect and report suspicious activity conducted or attempted to the U.S. Treasury's Financial Crimes Enforcement Network ("FinCEN").[37] A

---

associated persons that are reasonably designed to achieve compliance with applicable securities laws, regulations and FINRA Rules. *See* FINRA, Rule 3110(b)(1), Supervision (2022). These rules include requirements for the opening and maintenance of every customer account.

33. FINRA, Rule 4512(a)(1)(D) (2019).

34. *See* FINRA/NORC Study, *supra* note 10, at 1.

35. *See, e.g.* Letter of Acceptance, Waiver, and Consent, FINRA Dep't of Enforcement v. Robinhood Financial, LLC, Docket No. 2020066971201 (June 30, 2021) at 17, https://www.finra.org/sites/default/files/2021-06/robinhood-financial-awc-063021.pdf (hereinafter "Robinhood 2021 AWC") (account approval "nearly instantaneously").

36. 31 U.S.C. § 5311 *et seq.* (2021). The BSA's implementing regulations require that firms "establish, document, and maintain a written Customer Identification Program . . . appropriate for [the firm's] size and business" and that the program contain "procedures for verifying the identity of each customer to the extent reasonable and practicable." 31 C.F.R. § 1023.220(a)(1) and (a)(2) (2021).

37. *See* 31 C.F.R. § 1023.320 (2021). Title 31 U.S.C. § 5318(g) authorizes the Treasury Department to issue suspicious activity reporting requirements for broker-dealers. The Treasury Department issued the implementing regulation, 31 C.F.R. § 103.19(a)(1) (2021), in July 2002, providing that with respect to any transaction after December 30, 2002, "[e]very broker or dealer in securities within the United States . . . shall file with [the Financial Crimes Enforcement Network (FinCEN)] . . . a report of any suspicious transaction relevant to a possible violation of law or regulation." FinCEN issued 31 C.F.R. § 1023.320 (2021) (the SAR Rule) (effective Jan. 3, 2011)

failure to file suspicious activity reports with FinCEN constitutes a violation of FINRA Rules 3310 and 2010.[38]

FINRA Rule 3310 requires firms "to develop and implement a written anti-money laundering program reasonably designed to achieve and monitor the member's compliance with the requirements of the [BSA]."[39] At a minimum, the firm's anti-money laundering ("AML") program must: (a) implement policies, procedures and internal controls that can reasonably detect and cause reporting of suspicious transactions; (b) provide for annual testing of the procedures; (c) designate and identify to FINRA by name, title and contact information the personnel responsible for implementing and monitoring the day-to-day operations and controls of the program; and (d) include risk-based procedures for ongoing customer due diligence, including understanding the nature and purpose of customer relationships for the purpose of developing customer risk profiles.[40]

---

amending BSA regulations, requiring a broker-dealer to make SARs and supporting documentation available to any SRO that examines the broker-dealer for compliance with the requirements of the SAR Rule upon the request of the SEC. *See* FINRA, REGUL. NOTICE 12-08, SEC REQUESTS BROKER-DEALERS MAKE SARS AND SAR INFORMATION AVAILABLE TO FINRA (Jan. 2012), https://www.finra.org/rules-guidance/notices/12-08.

38. *See, e.g.,* Letter of Acceptance, Waiver, and Consent, FINRA Dep't of Enforcement v. Precision Securities, LLC, Docket No. 2020067467601 (July 19, 2021) (firm operated a trading platform used primarily by day- and swing-traders; however, firm did not reasonably design AML program to monitor and report suspicious activity in light of the firm's business model, including suspicious trading from China-based accounts for trading in excess of $200 million; FINRA fined firm $350,000); Letter of Acceptance, Waiver, and Consent, FINRA Dep't of Enforcement v. ITG, Inc., Docket No. 2017054643601 (Mar. 3, 2021) (firm failed to establish and implement AML policies and procedures reasonably designed to detect and cause the reporting of suspicious low-priced securities trading; firm failed to investigate numerous red flags in connection with trading of at least 30 low-priced securities, including a potential pump and dump scheme; firm censured and fined $450,000).

39. FINRA Rule 3310, Anti-Money Laundering Compliance Program (2018).

40. *See id.* NASD Notice to Members 02-21 was issued shortly after the NASD filed Rule 3310's predecessor rule, promulgated in response to the passage of the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (PATRIOT Act), Pub. L. No. 107-56, 115 Stat. 272 (2001). Title III of the PATRIOT Act, referred to as the International Money Laundering Abatement and Anti-Terrorist Financing Act of 2001 (Money Laundering Abatement Act), imposes obligations on broker/dealers under new anti-

FINRA has reminded firms about their obligations to implement AML programs to monitor and report suspicious activity. In Regulatory Notice 17-40, FINRA informed firms about additional customer due diligence requirements imposed by FinCEN, specifically, that firms identify and verify the identity of the beneficial owners of all legal entity customers at the time a new account is opened, subject to certain exclusions and exemptions.[41] FINRA has also brought enforcement actions against online trading platforms for failure to establish a Customer Identification program tailored to the firm's business model,[42] and failure to adapt its AML program to its growth sufficient to surveil suspicious money movements and investigate suspicious activity.[43]

Most recently, FINRA warned about the heightened risk for fraud during the COVID-19 Pandemic in Regulatory Notice 20-13, which stated that that

---

money laundering (AML) provisions and amendments to the existing Bank Secrecy Act (BSA) requirements. 31 U.S.C. §§ 5311 *et seq.* (2021).

41. *See* FINRA, REGUL. NOTICE 17-40, FINRA PROVIDES GUIDANCE TO FIRMS REGARDING ANTI-MONEY LAUNDERING PROGRAM REQUIREMENTS UNDER FINRA RULE 3310 FOLLOWING ADOPTION OF FINCEN'S FINAL RULE TO ENHANCE CUSTOMER DUE DILIGENCE REQUIREMENTS FOR FINANCIAL INSTITUTIONS (Nov. 2017), https://www.finra.org/rules-guidance/notices/17-40. FINRA again reminded firms about their obligations to monitor and report suspicious activity, providing a series of red flags that would alert firms to issues involving: (i) customer due diligence and interactions with customers; (ii) deposits in securities; (iii) red flags in securities trading; (iv) red flags in money movement; (v) red flags in insurance products; and (vi) various other potential red flags associated with the account or account activity. *See* FINRA, REGUL. NOTICE 19-18, ANTI-MONEY LAUNDERING (AML) PROGRAM (May 2019), https://www.finra.org/rules-guidance/notices/19-18.

42. *See, e.g.,* Letter of Acceptance, Waiver, and Consent, FINRA Dep't of Enforcement v. Score Priority Corp., Docket No. 2020067466901 (Apr. 14, 2021) (FINRA imposed $250,000 fine and censure against online, self-directed broker-dealer that failed to develop and implement an AML program reasonably expected to detect and report suspicious activity from transactions and money movements in domestic and foreign-based retail accounts; firm also failed to establish a Customer Identification Program tailored to the firm's business and a due diligence program reasonably designed to detect money-laundering activities).

43. *See, e.g.,* Letter of Acceptance, Waiver, and Consent, FINRA Dep't of Enforcement v. Interactive Brokers LLC, Docket No. 2015047770301 (Aug. 10, 2020) (assessing $15 million fine and censure against Interactive Brokers, finding that the firm failed to reasonably design its AML program to match its significant growth, and that its existing AML program was deficient because it failed to surveil thousands of suspicious money movements in the hundreds of millions of dollars, and the firm failed to investigate potentially suspicious activity).

firms reported an increase in newly-opened fraudulent accounts, with fraudsters targeting online account platforms, particularly "firms that recently started offering such services."[44] FINRA warned that fraudsters were using stolen or synthetic identities to establish fraudulent accounts to divert congressional stimulus funds, unemployment payments or engage in automated clearing house (ACH) fraud.[45] For firms that opened accounts through electronic means, FINRA stressed the importance of a strong Customer Identification Program (in the opening and ongoing monitoring of customer accounts), which utilized *both* documentary and non-documentary (i.e., independent verification of customer information) methods of verifying customer identity, limited automated approval of multiple accounts opened by the same customer, and used other verification procedures for bank accounts and transfers.[46]

FINRA's 2021 enforcement action against Robinhood Financial included charges against the firm for its failure to establish and implement a reasonably designed Customer Identification Program.[47] According to the FINRA AWC, the firm approved more than 5.5 million new customer accounts between June 2016 to November 2018, relying primarily on a customer identification process that was "largely automated" and suffered from "multiple flaws."[48] Among other things, Robinhood did not have any employees whose primary job responsibilities related to the Customer Identification Program, as required by FINRA Rule 3310, Anti-Money Laundering Compliance Program, and had

---

44. FINRA, REGUL. NOTICE 20-13, HEIGHTENED THREAT OF FRAUD AND SCAMS, FINRA REMINDS FIRMS TO BEWARE OF FRAUD DURING THE CORONAVIRUS (COVID-19) PANDEMIC (May 5, 2020), https://www.finra.org/rules-guidance/notices/20-13; *see also* FINRA, REGUL. NOTICE 19-18, *supra* note 41 (providing a comprehensive list of "money laundering red flags" that is not exhaustive or all-inclusive).

45. FINRA, REGUL. NOTICE 20-13, *supra* note 44.

46. *See id.* at 2-3. In addition to fraudulently opened accounts, Regulatory Notice 20-13 identified three additional scams which increased during the pandemic, including firm imposter scams (where fraudsters impersonate firms and associated persons in communicating with customers); IT Help Desk scams (fraudsters posing as persons associated with the firm to obtain new sign-on credentials from the firm's IT desk); and business email compromise schemes (fraudsters posing as manager or executive requesting payment for an invoice or other expense). *See id.*

47. *See* Robinhood 2021 AWC, *supra* note 35, at 26.

48. *See id*. at 26-27.

just one principal responsible for more than half of the new accounts.[49] The firm's automated system approved accounts even after its clearing firm flagged an account as needing "further review" due to the presence of a "fraud victim warning."[50]

Moreover, FINRA found that Robinhood ignored its own written procedures for the verification of these accounts. For example, although the clearing firm recommended thorough verification of flagged accounts, Robinhood *overrode* those alerts to approve the accounts anyway without any additional verification.[51] As a result of these failures, FINRA found that Robinhood had violated FINRA Rules 3310, Anti-Money Laundering Compliance Program and 2010, Standards of Commercial Honor and Principles of Trade.[52]

Brokerage firms' obligations to conduct customer due diligence, obtain and maintain updated customer information, and implement strong supervisory systems to monitor against fraudulent activity is also central to firms' obligations to protect customer information and assets, as discussed below.

(ii) Approving Customer Accounts for Options Trading and Margin

The 2021 Report on FINRA's Examination and Risk Monitoring Program stated that 2020 "witnessed a surge in new retail investors entering the market via online brokers, as well as an increase in certain types of trading, including options," noting the increase in "game-like" features of trading apps and other

---

49. *See id.* at 27.

50. *Id.* The clearing firm flagged accounts as needing further review because, among other reasons, the customer's social security was not issued by the Social Security Administration, the customer's age could not be verified, the customer's address was a storage facility, P.O. Box or cash-checking facility, or the customer's address had been used ten times or more by individuals with different social security numbers. *Id.*

51. *See id.* Robinhood approved 90,000 accounts that had been flagged for potential fraud, without requesting additional identification (such as a driver's license or passport), ignoring its own requirements to obtain other physical verification of customer identities. *See id.*

52. *See id.* In the AWC, FINRA tied Robinhood's violations of its other conduct rules – including Rule 3310 – to Rule 2010 which requires firms maintain a high standards in the conduct of their business. FINRA explained that a violation of Rule 3310 also constitutes a violation of Rule 2010. *See id.*

communications that may encourage investors to engage in higher risk trading.[53] Robert Cook, FINRA's CEO, echoed this concern in his May 6, 2021 statement before the U.S. House of Representatives Financial Services Committee, observing that game-like features on trading Apps "may encourage investor behaviors that impact sound investment decisions."[54] Cook announced that FINRA established a cross-departmental working group to assess how broker-dealers use their trading platforms and mobile apps to influence customer behavior, and determine whether additional rulemaking or guidance is necessary.[55]

To the extent trading platforms and mobile apps are directing or facilitating higher risk trading in the form of options trading, however, these firms are required to approve each customer for a specific level of options trading (and use of margin) based on the customer's profile and experience.

FINRA Rule 2360 requires firms to conduct due diligence in approving a customer's account for options trading, including obtaining the essential facts about the customer, the customer's financial situation and investment objectives, and the customer's *investment experience* and knowledge, including the number of years and type of trading.[56]

FINRA Rule 2360(b)(16)(A)-(D) require a brokerage firm to consider the various levels of options trading (e.g., buying covered calls, uncovered writing), the risks specific to the customer in light of the customer's profile and experience, and "determin[e] whether and *to what extent* to approve the account for options trading."[57] Subsection (16)(B)(ii)(d) further requires a firm to note in the customer's account records the "[n]ature and types of transactions for which" it is approved. A firm cannot accept an options order unless it has provided the customer with an options disclosure document[58] and

53. 2021 FINRA Report, *supra* note 16, at 22.

54. Cook, *supra* note 15.

55. *See id.*

56. FINRA, Rule 2360(b)(16)(B), Diligence in Opening Accounts (2020).

57. *Id.*

58. The specific disclosure document is entitled "Characteristics and Risks of Standardized Options," a 188-page pamphlet available for download on the Options Clearing Corporation website at: https://www.theocc.com/Company-Information /Documents-and-Archives/Options-Disclosure-Document.

the customer's account has been approved for options trading by a registered Options Principal or Limited Principal – General Securities Sales Supervisor.[59]

In 2021, FINRA reminded firms that the obligations to conduct due diligence in connection with options account approvals and margin equally applies to self-directed accounts.[60] FINRA's notice was prompted by the significant increase in the number of customers opening self-directed accounts and trading options.[61] The notice explained that Rule 2360(b)(16) requires a firm to specifically approve (or disapprove) each customer for options trading and the appropriate level of options trading for that customer based upon "detailed customer information, including, among others, the customer's knowledge, investment experience, age, financial situation and investment objectives."[62] This obligation applies regardless of whether the account is self-directed or the options are recommended.[63]

Since option transactions are often required to be traded in a margin account, FINRA's notice reminded firms of margin maintenance requirements under Rule 4210, explaining that firms must also "have procedures to review the limits and types of credit extended to all customers, to review the need for higher margin requirements for individual securities and customers and to formulate their own margin requirements."[64]

Despite due diligence and supervisory approval requirements, customers frequently get "instant" approval for options trading in margin accounts when opening self-directed accounts online or through an app, like Robinhood. This is because online trading firms have largely automated the customer account opening process, which often includes an application to trade options. Firms are nevertheless required to implement supervisory reviews of any automated processes, however, to ensure that they comply with FINRA rules.

One of the charges against Robinhood in FINRA's enforcement action was its failure to establish or maintain a supervisory system to achieve compliance

---

59. *See* FINRA, Rule 2360(b)(16)(A), Approval Required (2020).

60. *See* FINRA, REGUL. NOTICE 21-15, FINRA REMINDS MEMBERS ABOUT OPTIONS ACCOUNT APPROVAL, SUPERVISION AND MARGIN REQUIREMENTS (Apr. 9, 2021), https://www.finra.org/rules-guidance/notices/21-15.

61. *See id.* at 1.

62. *Id.* at 2.

63. *See id.* The notice also referenced requirements under FINRA Rule 2090, Know your Customer, FINRA Rule 4512, Customer Account Information, and FINRA Rule 3310, Anti-Money Laundering (AML) Program. *See id.* at 1-2.

64. *Id.* at 4.

with FINRA Rule 2360(b)(16), because it used an automated system that did not sufficiently implement the due diligence requirements under the rule. The AWC stated that the firm had relied almost entirely on an automated system that used algorithms – known by Robinhood as "option account approval bots" – to review customer responses to eligibility questions and, based on those responses, approve or reject option applications "nearly instantaneously."[65] But the system failed to comply with Rule 2360(b)(16)'s due diligence and approval obligations in several respects:

- The bots considered only the information provided in the immediate customer application, without regard to any prior application or information provided by the customers;[66]
- The bots approved customers for level 3 trading (requiring three years of trading experience) even if the customers were under 21 years old, or had previously represented they had no options experience, or who had previously certified that they did not understand option spreads;[67]
- Robinhood's principals reviewed on a weekly basis less than 0.1% of the accounts to ensure that the bots performed as programmed; moreover, the reviews were limited only to ensuring that the bots functioned as programmed, and not whether the information provided was consistent for that customer or whether options trading was appropriate for that customer in the first place;[68] and
- Robinhood's system approved thousands of accounts where the customer had provided false information, or where the customer had revised risk tolerance information that would have made them ineligible to trade options under the firm's own criteria.[69]

As a result of these failures, FINRA found that Robinhood failed to supervise its system for approving options trading and exercise due diligence in approving customers for options trading, in violation of FINRA Rules 3110, 2360 and 2010.[70]

---

65. Robinhood 2021 AWC, *supra* note 35, at 17.

66. *See id.*

67. *See id.* at 17-18.

68. *See id.* at 18.

69. *See id.* at 18-19.

70. *See id.* at 21.

B. Communications and Investment Recommendations

Brokerage firms have certain obligations when they communicate with the public. The 2200 series of the FINRA rules govern communications and disclosures. FINRA Rule 2210 broadly covers communications with the public. FINRA Rules 2220, 2264, and 2270 cover more specific types of communications relating to options trading, margin trading, and day-trading. As previously noted, these rules apply regardless of the way the firm does business – through brokers, online, or through a mobile app. Firms are obligated to ensure that all communications comply with FINRA rules.

(i) Communicating with the Public

FINRA categorizes communications as Retail, Correspondence, and Institutional.[71] A "retail communication" is "any written (including electronic) communication that is distributed or made available to more than 25 retail investors within any 30 calendar-day period."[72] "Correspondence" is defined as "any written (including electronic) communication that is distributed or made available to 25 or fewer retail investors within any 30 calendar-day period."[73] An "institutional communication" is defined as "any written (including electronic) communication that is distributed or made available only to institutional investors, but does not include a member's internal communications."[74]

How a communication is defined determines the firms' approval and review obligations in connection with the communication. All retail communications must be approved by a principal of the firm either before it is first used or before it is filed with FINRA.[75] Correspondence must be reviewed and supervised as determined by FINRA Rule 3110.[76] Institutional communications must be reviewed by a principal.[77]

---

71. *See* FINRA, Rule 2210, Communications with the Public (2019).

72. FINRA, Rule 2210(a)(5) (2019).

73. FINRA, Rule 2210(a)(2) (2019).

74. FINRA, Rule 2210(a)(3) (2019).

75. *See* FINRA, Rule 2210(b)(1)(A) (2019).

76. *See* FINRA, Rule 2210(b)(2) (2019).

77. *See* FINRA, Rule 2210(b)(3) (2019).

FINRA has also instituted broad content standards for all communications. Communications must be "fair and balanced," and may not omit any "material fact or qualification if the omission, in light of the context of the material presented, would cause the communications to be misleading."[78] Firms are not permitted to make "any false, exaggerated, unwarranted, promissory or misleading statement or claim in any communication."[79] Further, communications must "provide balanced treatment of risks and potential benefits."[80] Additionally, firms must consider to whom they will be making the communication, and provide appropriate details and explanations.[81]

The rules do not make any differentiation for the method of delivery. Electronic communications are captured by each definition. Accordingly, communications that take place via social media web sites or through apps are subject to the requirements of the rule. FINRA understands that firms are utilizing different means of communication, including icons, illustrations, cartoons, animations, short videos, and pictograms.[82] FINRA recognizes that these new technologies can help investors understand the firm's products and services, while also delivering required disclosures.[83]

Regardless of how the firm communicates with the public, firms are still obligated to follow FINRA rules and ensure communications are fair and balanced and not misleading.[84] FINRA has provided some guidance as to what that means for non-promotional materials:

- **Brand communications:** Brand communications that only acquaint investors with a firm's name and the fact that it offers financial services generally require no additional information in order to be fair and balanced.
- **Educational communications:** FINRA encourages members to use educational communications that promote financial literacy. For example, a member might develop a website that explains different

78. FINRA, Rule 2210(d)(1)(A) (2019).

79. FINRA, Rule 2210(d)(1)(B) (2019).

80. FINRA, Rule 2210(d)(1)(D) (2019).

81. *See* FINRA, Rule 2210(d)(1)(E) (2019).

82. *See* FINRA, REGUL. NOTICE 19-31, ADVERTISING REGULATION (Sept. 19, 2019), https://www.finra.org/rules-guidance/notices/19-31.

83. *See id.*

84. *See id.*

types of securities and how markets work, but because it does not promote specific securities or services it may only require a simple statement noting that securities involve risks and an offer to provide additional information. Another example is educational content that only provides basic information about what mutual funds are and does not include information that relates to the desirability of a specific product; such a communication would not need to disclose the specific risks associated with a particular fund.

- **Reference resources:** Some members provide websites, apps or other reference resources that do not promote a specific product or service; instead, they provide information intended to assist investors with investment decisions. In general, investors must choose to access these resources and interact with them to find the information (e.g., by downloading an app or creating an online account on the firm's website). A resource that does not promote specific products or services might need little or no disclosure under FINRA rules.
- **Post-sale communications:** Once a sale has occurred, members may provide communications to investors that discuss the product, such as changes to its portfolio or information about how the product has responded to changes in market conditions. These subsequent communications typically do not require the same extent of disclosure as communications leading up to a sale. Of course, a post-sale communication that recommends additional purchases or another product would be a promotional communication.[85]

Promotional materials that discuss the benefits of a particular product, type of product, or service may require extensive disclosures, including a balanced discussion of the risks or drawbacks.[86]

FINRA has also provided specific guidance to firms communicating commission discounts. For example, FINRA has stated that the communications must recognize that stocks are not the only type of securities available, and discounts may vary depending on the product traded.[87] Firms

85. *Id.*

86. *See id.*

87. *See Guidance: Recommendations Concerning Advertising and Promotion of Commission Discounts*, FINRA, https://www.finra.org/rules-guidance/guidance/recommendations-concerning-advertising-and-promotion-commission-discounts.

must also acknowledge that certain products, such as mutual funds, may have sales charges that cannot be discounted.[88] Further, firms must include a description of any factors that would impact the discount, such as initial deposit requirements, minimum transaction size, or registration fee.[89] Firms must also disclose any services charges that are applicable, such as charges applicable to limit orders, safekeeping of securities, odd lot transactions, or research.[90]

Communications that recommend a particular security or investment strategy are subject to other rules and limitations.

Both FINRA and the SEC set standards of conduct that are applicable when a recommendation of a security or investment strategy is made to an investor. However, neither FINRA nor the SEC define the term "recommendation." When it enacted Reg. Best Interest, the SEC stated that it would define the term consistently with how it had been defined previously, specifically referencing FINRA's Suitability Rule and FINRA Notice to Members 01-23.[91]

FINRA Notice to Members 01-23, Online Suitability, discusses the obligations of firms when communicating with customers online.[92] FINRA explained that:

> [T]he "facts and circumstances" determination of whether a communication is a "recommendation" requires an analysis of the content, context, and presentation of the particular communication or set of communications. The determination of whether a "recommendation" has been made, moreover, is an objective rather than a subjective inquiry. An important factor in this regard is whether—given its content, context, and manner of presentation— a particular communication from a broker/dealer to a customer reasonably would be viewed as a "call to action," or suggestion that the customer engage in a securities transaction. Members should bear in mind that an analysis of the content, context, and manner of

88. *See id.*

89. *See id.*

90. *See id.*

91. *See* Regulation Best Interest: The Broker-Dealer Standard of Conduct, 84 Fed. Reg. 33,318, 33,335 (July 12, 2019) (hereinafter "Reg. Best Interest Adopting Release").

92. *See* FINRA, NOTICE TO MEMBERS 01-23, ONLINE SUITABILITY (Apr. 2001), https://www.finra.org/rules-guidance/notices/01-23.

> presentation of a communication requires examination of the underlying substantive information transmitted to the customer and consideration of any other facts and circumstances, such as any accompanying explanatory message from the broker/dealer. Another principle that members should keep in mind is that, in general, the more individually tailored the communication to a specific customer or a targeted group of customers about a security or group of securities, the greater likelihood that the communication may be viewed as a "recommendation.[93]

FINRA went on to provide examples of communications that would likely fall outside the definition, and communications that would generally fall within the definition of recommendation.[94] For example, the following types of communications are likely not recommendations:

- A website with an electronic library that contains research reports, news, quotes, and charts;
- A search tool that allows a customer to sort or filter information about securities, so long as the firm does not limit it to or prefer securities in which the firm makes a market or for which it has issued a "buy" recommendation; and
- An email or other electronic subscription service that alerts a customer to news affecting securities in the customer's portfolio or on the customer's "watch list."[95]

The following communications are more likely to be deemed recommendations:

- An email or pop-up to a targeted customer or targeted group of customers encouraging the purchase of a security;
- A list of stocks accompanied by a request that the customer purchase one or more stocks on the list;
- A portfolio analysis tool that provides a list of specific securities the customer could buy or sell to meet the investment goals the customer has inputted; and

93. *Id.*

94. *Id.*

95. *See id.*

- Sending or pushing specific investment suggestions following the firm's use of data mining technology to analyze a customer's financial or online activity.[96]

FINRA acknowledged that the examples provided were not all inclusive, and were based on then prevalent technologies.[97] It suggested that firms analyze each communication to determine whether it reasonably could be considered a "call to action," such that it would influence a customer to trade a particular security or group of securities.[98] Such analysis should take place regardless of whether the customer requested the information, or if it was a computer software program that determined the information should be sent.[99] FINRA also reminded firms that they cannot discharge or avoid their obligations by using disclaimers.[100]

FINRA also recognized that firms may communicate on social media. The fact that the communication is widely disseminated or limited to a select one or more individuals is not determinative of whether the firm has made a recommendation.[101] Firms must still consider the facts and circumstances of the communication.[102]

If the communication is deemed to be a recommendation, then firms must comply with FINRA Rule 2111, Suitability or Reg. Best Interest. FINRA Rule 2111 applies to all recommendations made to customers prior to June 30, 2020. For recommendations made on or after June 30, 2020 either FINRA Rule 2111 or Reg. Best Interest applies. Reg. Best Interest applies to recommendations made to retail investors, defined as natural persons and their legal representatives, seeking advice for personal, family, or household purposes.[103]

---

96. *See id.*

97. *See id.*

98. *See id.*

99. *See id.*

100. *See id.*

101. *See* FINRA, REGUL. NOTICE 10-06, SOCIAL MEDIA WEB SITES, GUIDANCE ON BLOGS AND SOCIAL NETWORKING WEB SITES (Jan. 2010), https://www.finra.org/rules-guidance/notices/10-06.

102. *See id.*

103. Reg. Best Interest Adopting Release, *supra* note 91 at 33,343.

FINRA Rule 2111 applies to any recommendations not covered by Reg. Best Interest.[104]

If FINRA Rule 2111 applies, firms must comply with the three suitability components, reasonable-basis suitability, customer-specific suitability, and quantitative suitability. Reasonable-basis suitability requires that a firm "have a reasonable basis to believe, based on reasonable diligence, that the recommendation is suitable for at least some investors."[105] This requires the firm to have an understanding of the recommendation's risks and rewards.[106]

The customer-specific obligation requires that a firm "have a reasonable basis to believe that the recommendation is suitable for a particular customer based on that customer's investment profile."[107] The customer's investment profile includes the customer's age, other investments, financial situation and needs, tax status, investment objectives, investment experience, investment time horizon, liquidity needs, and risk tolerance.[108]

Quantitative suitability requires that the firm "have a reasonable basis for believing that a series of recommended transactions, even if suitable when viewed in isolation, are not excessive and unsuitable for the customer when taken together in light of the customer's investment profile."[109]

If the recommendation is governed by Reg. Best Interest, the firm must comply with the Disclosure, Care, Conflict of Interest, and Compliance obligations.[110] The Care obligation, in many ways, mirrors FINRA Rule 2111. It also consists of reasonable-basis, customer-specific, and quantitative obligations. Pursuant to the reasonable-basis obligation, the firm must "[u]nderstand the potential risks, rewards, and costs associated with the recommendation, and have a reasonable basis to believe that the recommendation could be in the best interest of at least some retail customers."[111]

Under the customer-specific obligation, the firm must "[h]ave a reasonable basis to believe that the recommendation is in the best interest of a particular

---

104. *See* FINRA Rule 2111.08 (2020).

105. FINRA, Rule 2111.05(a) (2020).

106. *Id.*

107. FINRA, Rule 2111.05(b) (2020).

108. FINRA, Rule 2111(a) (2020).

109. FINRA, Rule 2111.05(c) (2020).

110. 17 C.F.R. § 240.15l-1(a)(2) (2021).

111. 17 C.F.R. § 240.15l-1(a)(2)(ii)(A) (2021).

retail customer based on that retail customer's investment profile and the potential risks, rewards, and costs associated with the recommendation and does not place the financial or other interest of the broker, dealer, or such natural person ahead of the interest of the retail customer."[112]

The quantitative obligation requires the firm to "[h]ave a reasonable basis to believe that a series of recommended transactions, even if in the retail customer's best interest when viewed in isolation, is not excessive and is in the retail customer's best interest when taken together in light of the retail customer's investment profile and does not place the financial or other interest of the broker, dealer, or such natural person making the series of recommendations ahead of the interest of the retail customer."[113]

As noted, neither FINRA nor the SEC have defined recommendation, and have not said whether they would deem gamification features to be recommendations. They have recognized that gamification or prompts that promote or encourage trading activity may be subject to Reg. Best Interest.[114]

Massachusetts filed an Administrative Complaint against Robinhood that sought to hold the firm responsible for violations of its newly enacted fiduciary regulation.[115] Like the Suitability Rule and Reg. Best Interest, the regulation imposes obligations on a firm when it makes recommendations. Massachusetts relied in part on Robinhood's communications, including push notifications of lists of stocks, in arguing that Robinhood was making recommendations.[116]

(ii) Options Communications

In addition to the general rules concerning communications, FINRA has enacted more specific rules with respect to options communications. With the increased prevelance of options trading in self-directed online accounts,

112. 17 C.F.R. § 240.15l-1(a)(2)(ii)(B) (2021).

113. 17 C.F.R. §240.15l-1(a)(2)(ii)(C) (2021).

114. *See* Cook, *supra* note 15; *see also* Gensler, *supra* note 18.

115. Robinhood Financial, LLC, *supra* note 15.

116. *See* Defendants' Opposition Memorandum to the Plaintiff's Motion for Preliminary Injuctive Relief, Robinhood Financial v. Glavin, Civil Action No. 2184 CV 00884 BLS (May 10, 2021), https://www.masscourts.org/eservices/search.page.3?x=OWxSoK9l0j0xQ3Ar*dLG8NbPCYo0lMb4t1lMmfgHt8auP6Hex0vgfqBaVPJtlWJxUQkEfkQwmkkRr8E-vtGLgpBP6K4fVmZatR75C65DUmXZIZN5iyDlMQ2Zh8eE2vda58aECDHXC*OQrPTkUElyysGq496D0FLvTZW1zXs8kfs.

FINRA and the SEC have both voiced concerns that investors may not fully appreciate the risks involved.[117] When communicating about options, firms must meet additional standards.

There are two different standards to which communications regarding standardized options, prior to the delivery of disclosure documents, must conform.[118] If the options are not exempt by Securities Act Rule 238, and the communication is taking place prior to the prospectus delivery that "meets the requirements of Section 10(a) of the Securities Act", then the communication must "conform to Securities Act Rule 134 or 134a, as applicable."[119] However, if the communications are about options that are exempt from by Securities Act Rule 238, and are made before the delivery of disclosure documents are made, then there are five rules that must be adhered to.[120] First, the options being discussed can only be generally described.[121] Second, the communication must include contact information to enable the readers to obtain the disclosure documents.[122] Third, the communication may not contain "recommendations or past or projected performance figures, including annualized rates of return, or names of specific securities."[123] However, the communication may include any statement required by state or administrative law.[124] Finally, the communication is allowed to contain advertising devices, such as borders, logos, and graphics, provided that such devices are not misleading.[125]

---

117. *See* Cook, *supra* note 15.

118. *See* FINRA, Rule 2220(d), Options Communications (2014).

119. FINRA, Rule 2220(d)(1)(B) (2014).

120. *See* FINRA, Rule 2220(d)(1)(A) (2014).

121. *See* FINRA, Rule 2220(d)(1)(A)(I) (2014) ("The text may also contain a brief description of options, including a statement that identifies registered clearing agencies for options and a brief description of the general attributes and method of operation of the exchanges on which such options are traded, including a discussion of how an option is priced.").

122. *See* FINRA, Rule 2220(d)(1)(A)(ii) (2014).

123. FINRA, Rule 2220(d)(1)(A)(iii) (2014).

124. *See* FINRA, Rule 2220(d)(1)(A)(iv) (2014).

125. *See* FINRA, Rule 2220(d)(1)(A)(v) (2014).

While FINRA Rule 2220(d)(1) deals with the substance of options communications, FINRA Rule 2220(d)(2) deals with communication standards that apply to firms. Firms are prohibited from including in their options communications any information that is false or misleading, or omits any materially relevant information.[126] Furthermore, firms may not make promises of results, nor make unwarranted claims or forecasts.[127] Firms are also prohibited from including opinions that lack any reasonable basis.[128] Additionally, if warnings or caveats are included in such communications, then they must be legible.[129] Such warnings may not be misleading or irrelevant.[130] These communications may not suggest that a secondary market for the options is available.[131] Finally, communications may not be made if they "would constitute a prospectus as that term is defined in the Securities Act, unless it meets the requirements of Section 10 of the Securities Act."[132]

Firms are further prohibited from using options communications that are deficient in certain ways. Communications must reflect the risks of options trading and the complexities of options as related to other investments.[133] The communication must contain a warning that options are not suitable for all investors.[134] Conversely, firms are prohibited from making a communication if it suggests that options are suitable to all.[135] Also, any communications must inform the reader that supporting documentation for all claims made is available upon request.[136] However, certain of these requirements do not apply

126. *See* FINRA, Rule 2220(d)(2)(A)(i) (2014).

127. *See* FINRA, Rule 2220(d)(2)(A)(ii) (2014).

128. *See id.*

129. *See* FINRA, Rule 2220(d)(2)(A)(iii) (2014).

130. *See id.*

131. *See* FINRA, Rule 2220(d)(2)(A)(v) (2014).

132. FINRA, Rule 2220(d)(2)(A)(iv) (2014).

133. *See* FINRA, Rule 2220(d)(2)(A)(vi) (2014).

134. *See* FINRA, Rule 2220(d)(2)(A)(vii) (2014).

135. *See id.*

136. *See* FINRA, Rule 2220(d)(2)(A)(viii) (2014) (such documentation includes "comparison, recommendations, statistics, or other technical data").

to institutional communications.[137] Finally, all communications must be equally balanced between the upside benefits with the attendant risks.[138] All such risk warnings must be as specific as the statement of opportunities.[139]

So long as certain conditions are met, projections may be included in options communications.[140] First, all such communications must include or follow the options disclosure document.[141] Furthermore, "no suggestion of certainty of future performance [may be] made."[142] Additionally, parameters must be given to accompany the projection figures,[143] along with "all relevant costs, including commissions, fees, and interest charges."[144] All projections must be plausible, intended to be used as a point of reference,[145] and all material assumptions for those projections must be identified.[146] The risks for the options transaction must be disclosed.[147] Finally, "in communications relating to annualized rates of return, that such returns are not based upon any less than a 60-day experience; any formulas used in making calculations are clearly displayed; and a statement is included to the effect that the annualized returns cited might be achieved only if the parameters described can be duplicated and that there is no certainty of doing so."[148]

Similarly, options communications may include statistics of past performance of recommendations, and transactions, provided that certain requirements are met.[149] First, the disclosure document must accompany or

---

137. *See* FINRA, Rule 2220(d)(2)(B) (2014); *see also* FINRA, Rule 2220(a)(1)(B) (2014) (stating institutional communications are defined by FINRA, Rule 2210(a)).

138. *See* FINRA, Rule 2220(d)(2)(C) (2014).

139. *See id.* ("[B]road generalities must be avoided.").

140. *See* FINRA, Rule 2220(d)(3) (2014).

141. *See* FINRA, Rule 2220(d)(3)(A) (2014).

142. FINRA, Rule 2220(d)(3)(B) (2014).

143. *See* FINRA, Rule 2220(d)(3)(C) (2014).

144. FINRA, Rule 2220(d)(3)(D) (2014).

145. *See* FINRA, Rule 2220(d)(3)(E) (2014).

146. *See* FINRA, Rule 2220(d)(3)(F) (2014).

147. *See* FINRA, Rule 2220(d)(3)(G) (2014).

148. FINRA, Rule 2220(d)(3)(H) (2014).

149. *See* FINRA, Rule 2220(d)(4) (2014).

precede any such information.[150] Next, the information must be presented in "a balanced manner."[151] Additionally, the statistics need to be "confined to a specific 'universe' that can be fully isolated and circumscribed and that covers at least the most recent 12-month period."[152] All recommendations or transactions must include: the initial date, the initial price at the initial date, and the "date and price of each recommendation or transaction at the end of the period or when liquidation was suggested or effected, whichever was earlier."[153] The performance must also include the relevant costs, inclusive of commissions, fees, and margin obligations.[154] If annualized rates of return are communicated, then all material assumptions used in those calculations must also be communicated.[155]

Furthermore, an overview of general market conditions during the covered periods must be made.[156] Any comparison made between the general state of the market and the performance record must be valid.[157] Also, there must be a specific warning that past performance does not guarantee future results.[158] Finally, the statistics or record must come with the initialed determination of a Registered Options Principal that they "fairly [re]present the status of the recommendations or transactions reported upon."[159]

---

150. *See* FINRA, Rule 2220(d)(4)(A) (2014).

151. FINRA Rule, 2220(d)(4)(B) (2014).

152. *Id.*

153. FINRA, Rule 2220(d)(4)(C) (2014). This is further limited as follows: "provided that if the communications are limited to summarized or averaged records or statistics, in lieu of the complete record there may be included the number of items recommended or transacted, the number that advanced and the number that declined, together with an offer to provide the complete record upon request.".

154. *See* FINRA, Rule 2220(d)(4)(D) (2014).

155. *See* FINRA, Rule 2220(d)(4)(E) (2014).

156. *See* FINRA, Rule 2220(d)(4)(F) (2014).

157. *See id*.

158. *See* FINRA, Rule 2220(d)(4)(G) (2014).

159. FINRA, Rule 2220(d)(4)(H) (2014).

Communications regarding an options program[160] must include "the cumulative history or unproven nature of the program and its underlying assumptions."[161] Finally, if a firm violates any other SEC or SIPC rule related to options communications, the firm will have also violated FINRA Rule 2220.[162]

(iii) Margin Disclosure Statement

Certain communications must be made if the firm makes a certain type of trading available, regardless of whether the investor has requested it. Before opening a margin account on behalf of a customer, a firm is obligated to provide the customer with a Margin Disclosure Statement.[163] If the firm offers margin accounts, the firm must also make the statement available on its website in a clear and conspicuous manner.[164]

The statement is intended to highlight many of the risks attendant with margin trading. FINRA sets forth the required content of the statement, which includes the following sections: "You can lose more funds than you deposit in the margin account;" "The firm can force the sale of securities or other assets in your account(s);" "The firm can sell your securities or other assets without contacting you;" "You are not entitled to choose which securities or other assets in your account(s) are liquidated or sold to meet a margin call;" "The firm can increase its 'house' maintenance margin requirements at any time and is not required to provide you advance written notice;" "You are not entitled to an extension of time on a margin call."[165] Each section contains a brief explanation. At least once a calendar year, the firm must also send to each customer with a margin account either the statement or a summary disclosure that includes each of the section headings.[166] Firms are permitted to customize

160. *See* FINRA, Rule 2220(d)(5) (2014) ("i.e., an investment plan employing the systematic use of one or more options strategies").

161. *Id.*

162. *See* FINRA, Rule 2220(d)(6) (2014).

163. *See* FINRA, Rule 2264(a), Margin Disclosure Statement (2011).

164. *See id.*

165. *Id.*

166. *See* FINRA, Rule 2264(b) (2011).

the disclosure so long as it is substantially similar to the content required by the rule.[167]

(iv) Day-Trading Disclosure Statement

If a firm promotes a day-trading strategy, whether directly or indirectly, it may not open an account for any customer unless it has provided the customer with the day-trading disclosure statement and posted the statement on its website in a clear and conspicuous manner.[168] FINRA does offer to review communications and provide guidance to firms as to whether the communication will be deemed to be "promoting a day-trading strategy."[169]

As with the Margin Disclosure Statement, the content of the statement is set forth by FINRA, and includes the following headings: "Day trading can be extremely risky;" "Be cautious of claims of large profits from day trading;" "Day trading requires knowledge of securities markets;" "Day trading requires knowledge of a firm's operations;" "Day trading will generate substantial commissions, even if the per trade cost is low;" "Day trading on margin or short selling may result in losses beyond your initial investment;" and "Potential Registration Requirements."[170]

C. Cybersecurity: Protection of Customer Information, Funds and Securities

The technology that has transformed the brokerage industry and driven the growth of online platforms and brokerage apps has also created supervisory challenges for financial firms. The use of cloud-based servers, remote access to trading platforms and customer data, email and electronic wire transfers, and even algorithms (or "bots") to open and monitor customer accounts, among other things, provide opportunities for malicious actors to steal confidential information and customer assets and to disrupt a firm's business operations.

---

167. *See* FINRA, Rule 2264(c) (2011).

168. *See* FINRA, Rule 2270(a), Day-Trading Risk Disclosure Statement (2013).

169. *See* FINRA, Rule 2270.01, Review by FINRA's Advertising Regulation Department (2013).

170. FINRA Rule 2270(a) (2013).

In a 2021 annual report on examinations and risk monitoring program, FINRA observed that cybersecurity "remains one of the principal operational risks facing broker-dealers" and that it expects firms "to develop reasonably designed cybersecurity programs and controls that are consistent with their risk profile, business model and scale of operations."[171]

The SEC and FINRA have increasingly focused on cybersecurity risks, issuing risk alerts and guidance to the industry about its obligations to protect confidential customer information under Rule 30 of the SEC's Regulation S-P, establish written procedures to identify and respond to "identity theft red flags" as required under Rule 201 of the SEC's Regulation S-ID, and protect against cybersecurity attacks that could result in disruption of operations and services to customer, implicating FINRA Rule 4370.

(i) SEC Regulation S-P Rule 30: The Safeguard Rule

The SEC's Rule 30 under the SEC's Regulation S-P, adopted in 2000 and known as "the Safeguard Rule," requires every broker-dealer to adopt and maintain "written policies and procedures that address administrative, technical, and physical safeguard for the protection of customer records and information."[172] The policies and procedures must be reasonably designed to "(1) insure the security and confidentiality of customer records and information; (2) protect against any anticipated threats or hazards to the

171. 2021 FINRA Report, *supra* note 16.

172. Privacy of Consumer Financial Information (Regulation S-P), 65 Fed. Reg. 40,334 (June 29, 2000) (codified at17 C.F.R. § 248.30(a)). The SEC promulgated Regulation S-P pursuant to Title V of the Gramm-Leach-Bliley Act ("GLBA"), passed in 1999, which directed federal agencies with oversight over financial institutions to establish standards for the protection of customer information. 15 U.S.C. § 6801(b) (2010). Title V governs imposed upon financial institutions "an affirmative and continuing obligation . . . to protect the security and confidentiality of [customer] nonpublic personal information." 15 U.S.C. § 6801(a) (2010). It further directed federal agencies with oversight over the financial industry to promulgate rules that "establish appropriate standards for the financial institutions subject to their jurisdiction relating to administrative, technical, and physical safeguards . . ." 15 U.S.C. § 6801(b) (2010). The SEC adopted amendments to the Safeguard Rule, effective January 2005, to require that the policies and procedures adopted be in writing. SEC. EXCH. COMM'N, REL. NOS. 34-50781, IA-2332, IC-26685, DISPOSAL OF CONSUMER REPORT INFORMATION (Dec. 2, 2004), https://www.sec.gov/rules/final/34-50781.htm.

security or integrity of customer records and information; and (3) protect against unauthorized access to or use of customer records or information that could result in substantial harm or inconvenience to any customer."[173]

After Regulation S-P Rule 30 was initially adopted, firms' security policies generally focused on administrative and physical risks to customers' personally identifiable information ("PII"), rather than risks related to changing technology.[174] FINRA Regulatory Notice 05-49 reminded firms that their policies and procedures to protect against unauthorized access to or use of customer records or PII that could result in substantial harm or inconvenience to customers should "adequately reflect changes" in technology or alternative work arrangements.[175]

FINRA acknowledged that there can be no "one-size-fits-all" policy or procedure, but stressed that members should consider at a minimum whether: (1) the firm's existing policy adequately addresses the technology it currently uses; (2) the firm has taken appropriate technological precautions to protect customer information; (3) the firm is providing training to its employees about its available technology, its use and the steps necessary to protect customer information; and (4) the firm is conducting periodic audits to detect vulnerabilities and ensure the systems are, in practice, protecting customer records and information from unauthorized access.[176]

Despite their increasing reliance on technology, many financial firms have not adequately adapted their written policies and procedures to new technology or have otherwise failed to address new vulnerabilities in their systems. In 2015, the SEC's Office of Compliance Examinations and Inspections ("OCIE") issued a risk alert after a cybersecurity examinations sweep found

---

173. 15 U.S.C. § 6801(b) (2010).

174. Jeffrey Taft, Matthew Bisanz, and Leslie Cruz, *The SEC's Regulation S-P in the Age of Cybersecurity*, THE INVESTMENT LAWYER, Vol. 9, No. 9 (Sept. 2019), https://www.mayerbrown.com/-/media/files/perspectives-events/publications/2019/09/il_0919_taftbisanzcruz.pdf (observing that when Regulation S-P was first adopted many safeguarding procedures "focused on administrative and physical safeguards, and to a lesser extent on technical safeguards").

175. FINRA, NOTICE TO MEMBERS 05-49, SAFEGUARDING CONFIDENTIAL CUSTOMER INFORMATION at 1 (July 2005), https://www.finra.org/rules-guidance/notices/05-49. Regarding the use of wireless networks, FINRA stressed the importance of using appropriate safeguards, such as encryption, to prevent unauthorized parties from accessing customer information, and the use of firewalls to mitigate risks of outside intrusion by hackers.

176. *Id.* at 4.

that while most of the firms examined had adopted written security policies and procedures, 88% of broker-dealers and 74% of registered investment advisers had experienced cyber-attacks (directly or through one or more of their vendors) or had security gaps.[177]

The SEC's early enforcement cases under Regulation S-P Rule 30 focused on administrative and physical risks to PII, such as handling customer information when winding down business operations.[178] More recently, the SEC has charged brokerage firms and investment advisers with violations of Regulation S-P Rule 30 for failures to adopt, implement or enforce written policies and procedures applicable to the firm's use of technology, including, the use of email addresses not affiliated with the firm's domain name to receive over 4,000 faxes containing customer PII (in violation of written policies),[179] storing customer PII on a third-party web server without adopting written policies and procedures regarding the security and confidentiality of that information and the protection of that information from threats or unauthorized access,[180] and failing to ensure the reasonable design and operation of two web-based applications on the firm's Intranet that organized customer data and PII, to limit access to the PII, or to conduct any audits or testing of its applications to guard against unauthorized access.[181]

---

177. *See* SEC. EXCH. COMM'N OFFICE OF COMPLIANCE INSPECTIONS AND EXAMINATIONS, NATIONAL EXAM PROGRAM RISK ALERT, CYBERSECURITY EXAMINATION SWEEP SUMMARY, at 2-3 (Feb. 3, 2015), https://www.sec.gov /about/offices/ocie/cybersecurity-examination-sweep-summary.pdf.

178. *See, e.g.,* David C. Levine, SEC. EXCH. COMM'N, REL. NO. 34-64222, 100 SEC Docket 3049, 2011 WL 1325568, *5 (Apr. 7, 2011) (finding brokerage firm violated, and its senior officer aided and abetted the firm's violations, of Rule 30(a) of Regulation S-P because firm failed to adopt policies and procedures to protect customer information while firm was winding down its business).

179. *See* Craig Scott Capital, LLC*,* SEC. EXCH. COMM'N, REL. NO. 34-77595 (Apr. 12, 2016) (ordering cease-and-desist and fining firm $100,000 penalty, and $10,000 penalties against individual associated persons who used personal emails in violation of written policies).

180. *See* R.T. Jones Capital Equities Management, Inc., SEC. EXCH. COMM'N, REL. NO. IA-4204 (Sept. 22, 2015) (the firm's third-party web server was hacked and the PII of more than 100,000 customers was rendered vulnerable to theft; firm fined $75,000).

181. *See* Morgan Stanley Smith Barney, SEC. EXCH. COMM'N, REL. NOS. 34-78021, IA-4415 (June 8, 2016) (for nearly three years one of the firm's associated persons exploited flaws in the applications to misappropriate data regarding 730,000

FINRA has brought enforcement actions against broker-dealers for violations of Regulation S-P Rule 30 in connection with similar security breaches due to firms' failure to adopt, implement and enforce written security policies to its current technology. A recurring problem is firms' use of third-party cloud services without adequately assessing and testing the third-party provider's security systems. FINRA charged Lincoln Financial Securities Corp. with violations of Regulation S-P Rule 30 because, commencing in 2011, one of the firm's branch offices started using a third-party cloud service provider to store records, including customer account applications that contained PII, without ensuring that the provider installed antivirus and encryption software.[182] Although hackers with foreign IP addresses had hacked into the server and gained access to PII for 4500 customers, the firm failed to implement a policy for months after the cyberattack, and failed to ensure its registered representatives and third-party vendor adequately applied the policy.[183] As a result of these supervisory failures, FINRA found that Lincoln Financial violated Regulation S-P Rule 30 and further violated FINRA's supervision rule and Rule 2010, censuring the firm and imposing a penalty of $650,000.[184]

(ii) SEC Regulation S-ID: The Identity Theft Red Flags Rule

The SEC's Rule 201 of Regulation S-ID, adopted in 2013 and known as the "Identity Theft Red Flags Rule,"[185] requires broker-dealers and investment

---

customer accounts; Morgan Stanley was ordered to cease-and-desist, censured, and fined $1,000,000).

182. *See* Letter of Acceptance, Waiver, and Consent, FINRA Dep't of Enforcement v. Lincoln Financial Securities Corp., Docket No. 2013035036601 (Nov. 14, 2016).

183. *See id.*

184. *See id.* at 2-3; 5. *See also* Letter of Acceptance, Waiver, and Consent, FINRA Dep't of Enforcement v. Oak Tree Securities, Inc., Docket No. 2015043455201 (Sept. 28, 2017) (finding that for nearly two years Oak Tree used third party vendors to create and host its public website, but did not create any policies or procedures to ensure that it maintained the confidentiality of customer PII, or ensure that its vendors had procedures to protect PII; on at least seven occasions an internet search engine was able to access PII for over 700 customers).

185. SEC. EXCH. COMM'N, REL. NOS. 34-69,359, IA-3582, IC-30,456, IDENTITY THEFT RED FLAGS RULES (Apr. 10, 2013; effective May 20, 2013) (codified at 17 C.F.R. § 248.201), https://www.sec.gov/rules/final/2013/34-69359.pdf. The SEC

advisers registered (or required to be registered) with the SEC to establish and implement a written Identity Theft Prevention Program that is designed to detect, prevent and mitigate identity theft[186] in connection with the opening of a covered account or any existing covered account.[187] The SEC has explained that an Identity Theft Prevention Program "must include reasonable policies and procedures to: identify relevant red flags for the covered accounts and incorporate them into the Identity Theft Prevention Program; detect the red flags hat have been incorporated into the Identity Theft Prevention Program; respond appropriately to any red flags that are detected pursuant to the Identity Theft Prevention Program; and ensure that the Identity Theft Prevention Program is updated periodically to reflect changes in risks to customers from identity theft."[188]

In 2018, the SEC brought its first enforcement case for violations of the Identity Theft Red Flags Rule against Voya Financial Advisors, Inc. ("VFA"), finding that VFA had failed to update its Identity Theft Prevention Program despite significant changes in external cybersecurity risks, and failed to respond to cybersecurity incidents.[189] VFA, a dually registered firm with a national network of independent contractor registered representatives, provided its contractors with access to its brokerage and advisory customer information through a proprietary web portal, VPro.[190] The portal was managed and serviced by VFA's parent company, Voya, which handled

---

promulgated the rule (jointly issued with the CFTC) to implement provisions of the Dodd-Frank Wall Street Reform and Consumer Protection Act, which amended section 615(e) of the Fair Credit Reporting Act, 15 U.S.C. § 1681, to add the SEC and CFTC to the list of entities required to promulgate rules to require financial institutions and creditors to implement identity theft protection programs. *See id.*

186. The rule defines "identity theft" as a fraud committed or attempted using the identifying information of another person without authority. 17 C.F.R. § 248.201(b)(9) (2021).

187. The rule defines a "covered account" to include an account that a broker-dealer or investment adviser offers or maintains, primarily for personal, family, or household purposes, that involves or is designed to permit multiple payments or transactions, such as a brokerage account with a broker-dealer. 17 C.F.R. § 248.201(b)(3) (2021).

188. Voya Financial Advisors, Inc., SEC. EXCH. COMM'N, REL. NOS. 34-84288, IA-5048, at 3-4 (Sept. 26, 2018).

189. *See id.*

190. *See id.* at 2.

VFA's cybersecurity functions, serviced support call centers, and responded to VFA's contractor representatives for assistance on VPro.[191]

The SEC found that during three days in April 2016, one or more persons impersonating VFA contractor representatives called the IT support team to reset their passwords, providing PII for the representatives; thereafter the callers were able to access to VPro and, thereby, gained access to the PII for approximately 5,600 customers.[192] The SEC found that VFA violated the Identity Theft Red Flags Rule by not updating its Identity Theft Prevention Program since 2009, by failing to conduct adequate identity theft training, and by failing to ensure that the Identity Theft Prevention Program included reasonable procedures designed to respond to and prevent red flags.[193]

In December 2020, FINRA charged a firm for Regulation S-ID Rule 201 violations in connection with security breaches. FINRA censured and fined Supreme Alliance $65,000 for failing to take action when the emails of its CEO (who was also the firm's chief compliance officer) was hacked.[194] The firm's CEO started receiving hundreds of notifications in his firm email account that his emails could not be delivered to certain external addresses, but he ignored the messages for four months.[195] When the CEO finally forwarded one of the notifications to the firm's outside email vendor, the vendor notified him that his email was likely compromised.[196] Despite learning this, the firm failed to implement any of the procedures of its written policies, or mitigate the risk of identity theft.[197] The AWC explained that at least 200 of the 17,000 emails

---

191. *See id.* at 4-5.

192. *See id.* at 7-8.

193. *See id.* at 7. During the relevant period, VFA had detected red flags prior to and after the April 2016 intrusion but did not reasonably respond to the red flags by changing security codes, or implementing other procedures to deny unauthorized persons access to VFA customer accounts. *See id.* The SEC also charged VFA with violations of the Safeguard Rule, Regulation S-P, Rule 30, because its policies and procedures were not reasonably designed to prevent and respond to cybersecurity risks. *See id.* at 3, 10.

194. *See* Letter of Acceptance, Waiver, and Consent, FINRA Dep't of Enforcement v. Supreme Alliance LLC, Docket No. 2019062898302 (Dec. 18, 2020).

195. *See id.* at 3.

196. *See id.*

197. *See id.*

blind copied to an external source contained customer PII.[198] FINRA found that Supreme Alliance did not have a program to address the identification and detection of red flags, or provide its registered representatives with any guidance in the event an identity theft had occurred; instead, the firm had written "generic policies and procedures not tailored to the firm's actual business model."[199] As a result, the firm violated Rule 201 of Regulation S-ID.[200]

(iii) Protecting Customer Funds

FINRA has long stressed the importance of implementing written policies and procedures governing the withdrawal and transmittal of customer funds and assets. In 2009, FINRA reminded firms to have written policies and procedures reasonably designed to review and monitor all instructions to transmit or withdraw assets from customer accounts.[201]

Concerns over the rising number of incidents of customer funds stolen as a result of compromised emails and fraudulent email instructions mailed to firms prompted FINRA to issue Regulatory Notice 12-05.[202] FINRA explained that a firm's supervisory control system must include policies and procedures reasonably designed to review and monitor the transmittal of funds or securities from customer accounts to third-party accounts (resulting in a change of beneficial ownership), to outside entities, to locations other than the customer's primary residence, and between customer accounts and registered

198. *See id.*

199. *Id.* at 2.

200. *See id.* at 3. By virtue of its violation of Regulation S-ID, the firm also violated FINRA Rule 2010. *Id.*

201. *See* FINRA, REGUL. NOTICE 09-64, CUSTOMER ASSETS, VERIFICATION OF INSTRUCTIONS TO TRANSMIT OR WITHDRAW ASSETS FROM CUSTOMER ACCOUNTS (Nov. 2009), https://www.finra.org/sites/default/files/NoticeDocument/p120372.pdf. The notice also highlighted questions for firms to consider in evaluating its policies and procedures for the transmittal of funds or securities.

202. *See* FINRA, REGUL. NOTICE 12-05, CUSTOMER ACCOUNT PROTECTION, VERIFICATION OF EMAILED INSTRUCTIONS TO TRANSMIT OR WITHDRAW ASSETS FROM CUSTOMER ACCOUNTS (Jan. 2012), https://www.finra.org/rules-guidance/notices/12-05.

representatives.[203] The procedures must consider the specific risks associated with each method the firm allows for transmittal.[204] When firms accept email or other electronic wire or transfer instructions, their policies and procedures should include a method for verifying that the email or instructions were in fact sent by the customer, and they should train their employees to follow these procedures.[205]

In December 2020, FINRA charged Lincoln Investment with supervisory failures in connection with its transmittal of customer funds to malicious actors, arising from the failure of the firm to implement policies and procedures to identify and respond to "red flags" or suspicious activity.[206] First, the firm received multiple phone calls from a woman impersonating a customer and requesting transfers of funds to a bank account that was not previously associated with the customer.[207] The firm transferred funds from the customer's account despite numerous red flags, including the imposter's failure to answer security questions correctly.[208] Additionally, the firm failed to follow its own written policy concerning third-party transfer requests, transferring $30,000 to a third-party after an associated person received an email from a customer's email account which had been compromised.[209] FINRA charged Lincoln with violations of Rule 3110(a) for its failure to establish, maintain and enforce policies and procedures to safeguard customer

---

203. *See id.* at 2.

204. *See id.*

205. *See id.* at 2-3. Moreover, the obligation to have supervisory procedures for the reviewing and monitoring of customer assets applies both to clearing and introducing firms, and while Rule 4311(c) permits firms to allocate responsibility for the performance of certain functions between the clearing and introducing firms when accounts are carried on a fully disclosed basis, the rule "expressly requires that the carrying firm be allocated the responsibility for the safeguarding of customer funds and securities." *Id.* at 3. For example, the introducing firm may have the responsibility to verify the customer's identity and that the instructions came from the customer and, therefore, have policies and procedures to ensure it carries out this function, but the clearing firm must still have adequate policies and procedures to review and monitor all disbursements it makes from the customer's account. *See id.*

206. *See* Letter of Acceptance, Waiver, and Consent, FINRA Dep't of Enforcement v. Lincoln Financial, Docket No. 2018056408401 (Dec. 10, 2020).

207. *See id.* at 2-3.

208. *See id.*

209. *See id.* at 4.

assets, which "includes the responsibility to identify and respond to red flags," censured the firm and imposed a $35,000 penalty.[210]

(iv) Increasing Cybersecurity Concerns in the Age of COVID-19

The COVID-19 pandemic profoundly affected many aspects of society and our daily lives, leading to millions of Americans working (and studying) from home, relying on technology to remotely access workplaces, classrooms, and other sites. The increased reliance on technology, combined with billions of stimulus checks sent to Americans, created new opportunities for financial fraud, prompting regulators to issue alerts about COVID-19 pandemic scams targeting consumers and investors.[211] According to one study, "[c]ybersecurity was the top near-term concern for independent broker-dealers" working from home or remote offices.[212]

FINRA has also issued several notices alerting members to the increased risk of fraudulent activity and the challenges for firms in safekeeping customer information and assets. On the heels of nationwide stay at home orders, FINRA reminded firms about their obligations under FINRA Rule 4370 and to consider pandemic-related business continuity plans,[213] and alerted them about

---

210. *Id.* at 2, 4. The AWC referenced FINRA Regulatory Notice 09-64 (Nov. 2009), which reminded members of their supervisory obligations to safeguard customer assets, which includes having policies and procedures governing the withdrawal or transmittal of funds or assets from customer accounts. *See id.* at 2.

211. *See Look Out for Coronavirus-Related Investment Scams*, SEC. EXCH. COMM'N (Feb. 4, 2020), https://www.investor.gov/introduction-investing/general-resources/news-alerts/alerts-bulletins/investor-alerts/look-out; *Fraud and Coronavirus (COVID-19)*, FINRA (Mar. 26, 2020), https://www.finra.org/investors/insights/fraud-and-coronavirus-covid-19.

212. Bruce Kelly, *Broker-dealers Brace for Cyberthreats*, INVESTMENTNEWS (Jan. 18, 2021), https://www.investmentnews.com/broke-dealers-brace-for-cyberthreats-201403.

213. *See* FINRA, REGUL. NOTICE 20-08, PANDEMIC-RELATED BUSINESS CONTINUITY PLANNING, GUIDANCE AND REGULATORY RELIEF (Mar. 9, 2020), https://www.finra.org/rules-guidance/notices/20-08. FINRA's 2021 Report explained that any cybersecurity breach that interrupts member operations or results in denials of service to customers also implicates Rule 4370 (Business Continuity Plans and Emergency Contact Information). *See* 2021 FINRA Report, *supra* note 16 at 8. Rule 4370 requires member firms to create and maintain a written business continuity plan identifying procedures relating to an emergency or significant business disruption,

addressing the increased vulnerability to cyberattacks and taking additional steps to protect customer information from being compromised on networks and mobile devices.[214]

In Regulatory Notice 20-08, which focused on providing firms with pandemic-related business continuity planning guidance, FINRA specifically addressed cybersecurity and advised firms to consider the increased risk of cyber events due to use of remote offices or telework.[215] FINRA stressed the importance that firms "remain vigilant in their surveillance against cyber threats and take steps to reduce the risk of cyber events."[216]

FINRA Regulatory Notice 20-13 outlined four common scams to which firms and their customers may be exposed during the COVID-19 pandemic.[217] First, FINRA observed the increase in new customer accounts and warned firms of an increase in fraudulent account openings and money transfers using synthetic or stolen customer identities, pointing firms to the importance of Customer Identification Programs, monitoring for fraud during the account opening process, and verifying transfers in selected circumstances – essentially the very same best practices FINRA has identified for a robust AML program.[218] Second, FINRA noted the increase of firm imposter scams, where fraudsters impersonate firms or associated persons in either communicating with customers or creating a fake online presence or website,

---

and update the plan in the event of any material change to the member's operations, structure, business or location. Rule 4370(a), (b). Although member firms have flexibility to design their business continuity plan, the plan must address the following elements relevant to cybersecurity risks: (1) data back-up and recovery (hard copy and electronic); (2) all mission critical systems; (3) financial and operational assessments; (4) alternative communications between customers and the member; (5) alternative communications between the member and its employees; (6) alternate physical location of employees; and (7) how the member will assure "customers' prompt access to their funds and securities in the event the member determines it is unable to continue its business." Rule 4370(c).

214. *See Cybersecurity Alert: Measures to Consider as Firms Respond to the Coronavirus Pandemic (COVID-19)*, FINRA (Mar. 26, 2020), https://www.finra.org/rules-guidance/notices/information-notice-032620.

215. *See* FINRA, REGUL. NOTICE 20-08, *supra* note 213.

216. *Id.*

217. *See* FINRA, REGUL. NOTICE 20-13, *supra* note 44.

218. *See id.* at 2-4; *see also* FINRA, REGUL. NOTICE 19-18, *supra* note 41.

and provided guidance on how firms could mitigate those risks.[219] Third, the notice explained that the use of remote working arrangements increased opportunities for IT Help Desk scams, where fraudster pose as associated persons, and contact the firm's IT Help Desk staff for a password reset, thereby giving the fraudster access to the firm's network, confidential information and customer assets.[220] The fourth common scam the notice identified was email compromise schemes, where fraudsters taking advantage of remote working arrangements send an email posing as firm leadership or manager to request funds or a transfer.[221]

In 2021, FINRA issued Regulatory Notice 21-18, stating that it had received an increasing number of reports regarding online customer account takeovers, involving bad actors using compromised customer information (i.e., username and password), to gain unauthorized access to customers' online brokerage accounts.[222] In order to assist firms in identifying, preventing and responding to such attacks, FINRA hosted a roundtable discussion with representatives of 20 member firms of various sizes and business models to discuss approaches to mitigating account takeover risks.[223] The notice identified the relevant regulatory obligations to protect customer information and assets, listed common challenges to protecting customer accounts, and

---

219. *See* FINRA, REGUL. NOTICE 20-13, *supra* note 44 at 5. FINRA specifically referred to its earlier Information Notice, *Imposter Websites Impacting Member Firms* (Apr. 29, 2019), which warned member firms about "imposter websites," where a malicious actor uses the names and/or photos of registered representatives to establish websites that look like the representatives' personal sites, and then directs the customers to enter personal information. *Id.* Several months after issuing Regulatory Notice 20-13, FINRA issued another notice warning firms and associated persons about imposter websites. *See* FINRA, REGUL. NOTICE 20-30, FRAUDSTERS USING REGISTERED REPRESENTATIVES NAMES TO ESTABLISH IMPOSTER WEBSITES (Aug. 20, 2020), https://www.finra.org/rules-guidance/notices/20-30. FINRA explained that firms could take steps to identify these pages by periodically searching the web for the names of its registered representatives or create alerts that automatically search for defined terms. *See id.* at 2.

220. *See* FINRA, REGUL. NOTICE 20-13, *supra* note 44 at 6. Another variant of the scheme is a fraudster posing as an IT Help Desk staffer who contacts the associated person to harvest his or her credentials or introduce malware. *See id.*

221. *See id.* at 7.

222. *See* FINRA, REGUL. NOTICE 21-18, CYBERSECURITY (May 12, 2021), https://www.finra.org/rules-guidance/notices/21-18.

223. *See id.* at 1.

provided a list of best practices and approaches to authenticating customer identities, monitoring accounts, implementing automated threat detection, and procedures to respond to potential or reported account takeovers.[224]

II. CONCLUSION

Technology has evolved the way investors interact with brokerage firms. These changes raise challenges for firms determining how to comply with the existing regulations in light of their new business models. However, the challenges firms face today mirror those in the early stages of online trading. While some things have changed, some have not.

Online platforms and mobile trading apps have increased the ability of investors to access the markets. Although the changes to technology have led more investors to be self-directed, they are still entitled to the protections of FINRA and SEC rules. Firms must still comply with the rules governing opening and approving accounts. Firms must confirm customer identies, even though they are only dealing with the investor virtually. Firms must comply with the communications rules, ensuring all communications are fair and balanced. And finally, firms must safeguard customer information, funds, and securities.

224. *See id.* at 4-7.