October 24, 2024

Vanessa A. Countryman
Secretary
U.S. Securities and Exchange Commission
100 F Street, NE
Washington, DC 20549-1090

Re: Cybersecurity Risk Management Rule for Broker-Dealers, Clearing Agencies, Major Security-Based Swap Participants, the Municipal Securities Rulemaking Board, National Securities Associations, National Securities Exchanges, Security-Based Swap Data Repositories, Security-Based Swap Dealers, and Transfer Agents (File No. S7-06-23, RIN 3235-AN15), 88 Fed. Reg. 20212 (Apr. 5, 2023); Cybersecurity Risk Management for Investment Advisers, Registered Investment Companies, and Business Development Companies (File No. S7-04-22, RIN 3235-AN08), 87 Fed. Reg. 13524 (Mar. 9, 2022).

Dear Ms. Countryman:

Better Markets[1] appreciates the opportunity to provide further comment on the above-captioned Proposed Rules.[2] Despite the threat that cybersecurity vulnerabilities pose to investors, no SEC rules currently require broker-dealers or investment advisers to have comprehensive cybersecurity programs. The Proposed Rules, among other things, would require broker-dealers and investment advisers to adopt policies and procedures governing cybersecurity.

We write to emphasize three points. First, the SEC has the authority to require that broker-dealers and investment advisers adopt policies and procedures governing cybersecurity. Second, the need for broker-dealers and investment advisers to adopt policies and procedures governing cybersecurity has only become more apparent since the SEC first proposed the Proposed Rules. Third, the SEC should finalize the Proposed Rules so that broker-dealers and investment advisers have programs to better insulate investors from the risks of cyberattacks.

I. The Commission has the authority to adopt the Proposed Rules.

There should be no question that the SEC has the authority to adopt the Proposed Rules. Section 15(b)(7) of the Securities Exchange Act of 1934 provides that no registered broker or dealer "shall effect any transaction in, or induce the purchase or sale of, any security unless such broker or dealer meets such standards of operational capability and . . . such standards of

---

[1] Better Markets is a non-profit, non-partisan, and independent organization founded in the wake of the 2008 financial crisis to promote the public interest in the financial markets, support the financial reform of Wall Street, and make our financial system work for all Americans again. Better Markets works with allies—including many in finance—to promote pro-market, pro-business, and pro-growth policies that help build a stronger, safer financial system that protects and promotes Americans' jobs, savings, retirements, and more.

[2] 88 Fed. Reg. 20,212 (Apr. 5, 2023) (Cybersecurity Risk Management Rule for Broker-Dealers); 87 Fed. Reg. 13,524 (Mar. 9, 2022) (Cybersecurity Risk Management for Investment Advisers).

training, experience, competence, and such other qualifications as the Commission finds necessary or appropriate in the public interest or for the protection of investors."[3] That section further provides that the Commission "shall establish such standards by rules and regulations."[4]

With respect to the proposed rule governing broker-dealers, the proposal states that a "cybersecurity program with a clear incident response plan designed to ensure continued operational capability, and the protection of, and access to, personal, confidential, or proprietary information and data . . . would assist in mitigating the effects of a cybersecurity incident."[5] The proposal state further that broker-dealers "generally should focus on operational capability in creating reasonably designed policies and procedures to ensure their continued operations in the event of a cybersecurity incident."[6] A rule requiring broker-dealers to have a cybersecurity program to ensure their operational capability in the event of a cyberattack is entirely consistent with Congress's directive that the SEC have the authority to adopt rules establishing standards of operational capability for broker-dealers in the public interest and for the protection of investors.

Section 223 of the Investment Advisers Act of 1940 provides that registered investment advisers "shall take such steps to safeguard client assets over which such adviser has custody . . . as the Commission may, by rule, prescribe."[7] With respect to the proposed rule governing investment advisers, the proposal recognizes that a "potential risk for an adviser's client stemming from the cybersecurity threats faced by the adviser is that a cybersecurity incident at the adviser could lead to the client's information being compromised or the loss of the client's assets."[8]

> Although protection provided by qualified custodians can mitigate risk to certain client assets to some extent, they cannot replace cybersecurity hygiene at the adviser level. As an adviser's "custody" of client assets implies a degree of control over those assets, compromise of adviser's systems—or the adviser's service provider's systems—could lead to unauthorized actions being taken with respect to those assets—including assets maintained with qualified custodians.[9]

The proposed rule would therefore impose explicit cybersecurity requirements on investment advisers to "enhance the Commission's ability to oversee and enforce rules designed to protect client and investor information and assets."[10] A rule imposing requirements to protect the loss of client assets from a cyberattack is entirely consistent with Congress's directive that the SEC have the authority to adopt rules prescribing steps that advisers must take to safeguard client assets.

---

3 15 U.S.C. § 78o(b)(7).
4 *Id.*
5 88 Fed. Reg. at 20,243.
6 *Id.*
7 15 U.S.C. 80b-18b.
8 87 Fed. Reg. at 13,546.
9 *Id.*
10 *Id.* at 13,550.

II. The need for broker-dealers and investment advisers to adopt cybersecurity programs has only become more apparent since the SEC issued the Proposed Rules.

With respect to cybersecurity attacks, the financial industry "is a high value target due to its vast sensitive customer data."[11] As a result, broker-dealers and registered investment advisers "have to be constantly vigilant for such data break-ins."[12] A few examples in the last year alone show the need for rules to ensure such vigilance by broker-dealers and investment advisers:

- In August 2024, Fidelity suffered a data breach when cybercriminals accessed the firm's computer network. The attack enabled access to customers' names, social security numbers, financial account information, and driver's license numbers. The breach impacted over 75,000 clients. A proposed class action lawsuit alleged that the company did not follow standard cybersecurity practices, such as encrypting client information and providing sufficient employee training. The complaint also accused Fidelity of not providing timely notice of the breach to customers, saying the firm did not disclose it for several weeks after it occurred.[13]

- In February 2024, Prudential experienced a cyberattack that compromised the personal information of clients of the firm. The hack involved social engineering—the manipulation of certain individuals such as company employees to act on behalf of unauthorized parties. The hackers obtained the names of Prudential clients and the serial numbers associated with identification records such as driver's licenses and non-driver identification cards. The data breach affected over 36,000 individuals. A proposed class action alleged that Prudential acted negligently in failing to protect its clients' personal information. The lawsuit also alleged that the firm failed to provide the affected individuals with timely notice of the breach.[14]

- In January 2024, Interactive Brokers discovered that an unauthorized party was able to gain access to an employee's email account. The incident resulted in the unauthorized party being able to access customers' sensitive information, including their names, social security numbers, financial account information, and driver's license numbers. The breach impacted about 600 clients of the firm.[15]

- In November 2023, a ransomware attack exposed the personal information of customers of Bank of America. The data breach compromised the name, address,

---

11 Madelein van der Hout, *Advisers need to keep pace with evolving cyber attacks*, FT Adviser (Sept. 18, 2024), https://www.ftadviser.com/regulation/2024/09/18/advisers-need-to-keep-pace-with-evolving-cyber-attacks/.

12 Bruce Kelly, *Interactive Brokers latest B-D to report data breach*, InvestmentNews (May 21, 2024), https://www.investmentnews.com/broker-dealers/interactive-brokers-latest-b-d-to-report-data-breach/253609.

13 Cassandre Coyer, *Fidelity Sued for Hack Exposing 77,000 Clients' Finance Data*, Bloomberg (Oct. 16, 2024), https://news.bloomberglaw.com/privacy-and-data-security/fidelity-investments-slapped-with-suit-over-hacked-client-data.

14 Emilie Ruscoe, *Prudential Financial Hit With Data Breach Suit in NJ*, Law360 (June 10, 2024), https://www.law360.com/articles/1845681/prudential-financial-hit-with-data-breach-suit-in-nj.

15 Melanie Waddell, *Interactive Brokers Notifies 600 Clients of Data Breach*, ThinkAdvisor (May 22, 2024), https://www.thinkadvisor.com/2024/05/22/interactive-brokers-notifies-600-clients-of-data-breach/.

data of birth, social security number, and other account information of the bank's deferred compensation customers. The hack affected over 57,000 accounts.[16]

- In October 2023, TIAA disclosed that a hack exposed the personal information of its customers. The data breach affected about 9,000 retail accounts.[17]

III. The SEC should finalize the Proposed Rules so that broker-dealers and investment advisers have programs to better insulate investors from the risks of cyberattacks.

These types of cybersecurity incidents have "prompt[ed] strict regulations" in Europe.[18] For example, in 2023 the European Union enacted the Digital Operational Resilience Act (DORA), which is designed to strengthen "the IT security of financial entities such as banks, insurance companies and investment firms."[19] DORA "requires financial entities to formulate a risk management system and put policies in place to identify exposure to cybercrimes and defend against them."[20] In the event of a data breach, financial entities must file a report within a specific time period.[21] There is no reason why similar rules should not apply in the United States.

The SEC's own Division of Examinations recognizes the importance of cybersecurity at broker-dealers and investment advisers. In its recently published priorities for 2025, the Division states that its "focus on cybersecurity practices by registrants remains vital to ensuring the safeguarding of customer records and information."[22] The fact that cybersecurity practices at broker-dealers and investment advisers are vital to the safeguarding of customer records and information is all the more reason for the SEC to adopt rules requiring that broker-dealers and investment advisers adopt and implement cybersecurity policies and procedures.

The Division also states that "[p]articular attention will be on firms' policies and procedures, governance practices, data loss prevention, access controls, account management, and responses to cyber-related incidents, including those related to ransomware attacks."[23] Again, the importance of these tools means that the SEC should require that broker-dealers and investment advisers have them. The Division's goal with its focus on cybersecurity is to "prevent interruptions to mission-critical services and to protect investor information, records, and assets"; the SEC would be best positioned to accomplish this goal by supplementing its exam program with rules imposing cybersecurity requirements on broker-dealers and investment advisers.

---

16 Carter Pape, Data breach affects 57,000 Bank of America accounts, American Banker (Feb. 13, 2024), https://www.americanbanker.com/news/data-breach-affects-57-000-bank-of-america-accounts.

17 Bruce Kelly, *TIAA latest big firm to report data breach and hack*, InvestmentNews (Oct. 2, 2024), https://www.investmentnews.com/industry-news/tiaa-latest-big-firm-to-report-data-breach-and-hack/257471.

18 van der Hout, supra note 11.

19 https://www.eiopa.europa.eu/digital-operational-resilience-act-dora_en.

20 Esen Esener, *Adaptive Governance for Blockchain Networks*, 7 Stan. J. Blockchain L. & Pol'y 76, 83 (2024).

21 *Id.*

22 Division of Examinations, U.S. Securities and Exchange Commission, Fiscal Year 2025 Examination Priorities, https://www.sec.gov/files/2025-exam-priorities.pdf, at 12.

23 *Id.*

Conclusion

We hope these comments are helpful as the Commission finalizes the Proposed Rules.

Sincerely,

Benjamin L. Schiffrin
Director of Securities Policy

Better Markets, Inc.
2000 Pennsylvania Avenue, NW
Suite 4008
Washington, DC 20006
(202) 618-6464

bschiffrin@bettermarkets.org
http://www.bettermarkets.org